中央警察大學犯罪防治研究所

碩士論文

指導教授:賴擁連 博士

Lai, Yung-Lien Ph.D.

網路詐欺犯罪被害之性別差異—以網路日常活動與自我控制理論分析

Gender differences in cyber fraud victimization: An analysis based on the theories of Cyber Routine Activity and Self-Control

研 究 生:方呈祥

Fang, Cheng-Hsiang

中華民國 109 年 6 月

謝誌

時光荏苒，在警大研究所就讀的兩年美好時光，眼見著即將畫下完美的句點。歷經兩年磨練及通過重重考驗後，終於到了撰寫謝誌的時刻，此刻的內心雖然滿懷順利取得碩士學位的歡喜，但同時夾雜即將與犯防所師長及研中這個溫暖大家庭道別的不捨之情。一本碩士論文的付梓，更著實感謝在撰寫過程中許多人的支持、指導及鼓勵，以下僅以此謝誌，致上最誠摯的感謝之意。

首先，這本論文的完成，最大的功臣莫過於我的啟蒙恩師–擁連老師。有幸能成為老師門下的學生，對我而言，實是莫大的榮耀與肯定，在跟隨老師將近兩年的學習歷程中，不論是在議題發想、研究方向及統計方法上，老師總提供許多意見、鼓勵與支持，老師強大的邏輯思維及思辨能力，更讓我在學術汪洋中迷茫時，得以尋覓正確的航向。此外，老師對於學術的堅持、熱愛及未來研究憧憬的學者風範，更深刻烙印於我腦海中。

其次，在警大研究所的兩年期間，感謝研究生中隊的師長、朋友，以及陪伴我兩年，共同度過歡笑與淚水的 462 室友們—政桐、建河、博裕及傳浩，在這段就學的歷程中，慶幸與大家經歷生活大小事務，也因為彼此的相互砥礪及陪伴，讓這兩年的時光變成我人生中最美好的一段回憶。此外，感謝 106 年班學長姐及警專好友兼研究所學長—季珈，從預備教育、入學後的大小考試、課業及論文方面皆提供許多協助，不勝感激。

再者，犯防所除了是警察學術的最高殿堂外，亦是一個溫暖的大家庭。在這大家庭中，充滿著師長的關愛、鼓勵與支持，感謝田木主任、玉書老師、文勇老師、文彥老師、煌發老師、勝昂老師、怡宏老師及碧翠老師在學期間的指導及照顧，以及美麗的文瑜助教，讓我們遇到各種大小困難時都能迎刃而解，學生均銘記於心。此外，本論文的完成，除感謝所有填答問卷的受訪者外，亦十分感謝不辭辛勞給予學生指導的兩位口試委員—許春金老師、鄧煌發老師，感謝老師們提供的寶貴意見，讓學生的論文更臻完善。

最後，特別感謝一直以來無條件支持我的家人們，總讓我能在無憂無慮的環境下，能專心致力於準備各項大小考試及學術領域的研究，謹將此論文獻給您們。

方呈祥 謹誌

2020 年 6 月

摘要

近年來，隨著網路蓬勃發展，網路犯罪數量及型態日趨增加，其中，網路詐欺犯罪所造成的被害損失更嚴重影響著公眾社會之生活秩序。此外，有鑑於過往對於網路詐欺被害研究鮮少深入探究兩性被害之差異，故本研究基於過往研究基礎，除以文獻探討法外，亦採網路問卷調查法，以網路日常活動及自我控制理論為研究框架，蒐集網路使用者網路詐欺被害經驗及網路詐欺被害因素，並彌補兩性網路詐欺被害差異研究之不足。本研究於 2019 年 11 月至 2020 年 1 月，進行正式問卷調查。首先，以配額抽樣方式擇定受試對象，輔以對照網路使用人口母群體之特性，控制「性別」及「年齡」，計算出受試者配額人數，視為配額抽樣，共收取網路問卷 870 份，並依此進行後續分析。

經多變量分析後發現，在全體樣本中，男性、年齡較低、無業者(含退休者、家管、學生)、收入較高、教育程度較低，每次上網時數及每周上網次數較高、平(假)日深夜時段上網，從事較多網路風險職業活動、具有較高網路負面誘因、衝動性、冒險性及投機性特質者，並缺乏社會監控者，其網路詐欺被害可能性較高，而性別、網路風險休閒活動、物理監控、網路負面誘因及投機性，皆係網路詐欺被害與重複被害次數之重要預測因子。在兩性網路詐欺被害影響因素中，男性樣本以年齡較低、無業者、每次上網時數及每周上網次數較高、在平(假)日深夜時段上網，從事較多網路風險職業活動、具有較高網路負面誘因、衝動性及冒險性特質者，從事較少網路休閒與職業活動、缺乏有效社會監控者，其網路詐欺被害可能性較高。在女性樣本中，無業者、收入較高、在平(假)日深夜時段上網，從事較多網路風險職業活動、具有較高網路負面誘因、衝動性及投機性特質者，並從事較少網路休閒活動者，其網路詐欺被害可能性較高。

最後，本研究根據前述研究發現，具體轉化為九項未來可行之政策建議，並劃分為標的物(被害者)、情境(場域)及潛在犯罪者等三大面向，以供有關單位參酌。首先，在標的物(被害者)部分，應降低網路依賴、減少高風險網路行為、增加網路風險認知意識。其次，情境(場域)部分，應訂立明確法令規範、落實網路分級管理、減少網路負面誘因。最後，潛在犯罪者部分，應強化網路監控、提升道德倫理，並抑制個人網路偏差動機。

關鍵字:性別、網路詐欺犯罪被害、網路日常活動理論、自我控制理論、重複被害

Abstract

In recent years, with the rapidly growing of internet prevalence, the numbers and types of cybercrime have dramatically increased in Taiwan. Specifically, a huge loss resulted from cyber fraud crime seriously impacted citizens' lives, as well as financial order and market in Taiwan Island. Meanwhile, the gender difference issue has been largely overlooked in this regard while the cyber fraud victimization has been paid attention recently in academic field. Drawn from the research framework developed in the western societies, the thesis aims to explore the influential factors on cyber fraud victimization. To be specific, the differences of differential factors in gender have been explored and analyzed in advance.

The cyber routine activity and self-control theories have been integrated as the research framework to develop the online questionnaire inquiring online users' routine activities, low self-control ability, and cyber fraud victimization experiences to fill the void of the gender differences in cyber-fraud victimization. Before an official survey, two-time pretests have been conducted in October, 2019 to make sure if the instrument was appropriate. After deleting and revising some not appropriate items, the official online questionnaire survey has been done during the period from November 2019 to January 2020. Also, based on the statistics form TWNIC, two demographical characteristics, "gender" and "age" have been controlled to make sure if the distribution of the collected online respondents is equal to the distribution of the online user population. As a result, a total of 925 anonymous online questionnaires has been recruited. After deleing some repeated respondents and some questionnaires with substantial missing values, 870 questionnaires have been employed to analyze in final.

The results from bivariate analyses (e.g., chi-square, t-test, and one-way ANOVA, Pearson's r) and multivariate analyses (e.g., Poisson regression and Negative binominal regression) showed that gender is an important factor in the explanation of cyber fraud

victimization, suggesting males had more fraud victimization experiences compared to their counterparts, females. Moreover, the results also indicated that males are significantly different from females in the frequency of online lifestyle, level of self-control, and the probability of being victimized situations/opportunities. Among those personal characteristics, the occupation was also an important factor in explaining cyber fraud victimization. After synthesizing the above research results, among those demographic characteristics, male, young people, the unemployed, the wealth and the less educated were more likely to be victims of cyber fraud. In term of cyber routine activity and self-control variables, those who surfed the Internet late at night, engaged in high-risk cyber vocational activities, received more negative incentives from the Internet, and were more impulsive, have a higher probability of being victimized in cyber fraud. Finally, this study also identified that gender, cyber risky leisure activities, physical guardianship, online negative incentives were successfully predicting those repeated victims in cyber fraud.

Overall, based on those findings, this study offers several policy implications and breaks them down to three major aspects: The suitable targets (the victim), the situation, and the potential offenders. First of all, as the suitable targets, we suggest that personal network dependence should be reduced, high-risk online lifestyle should be reduced, and the awareness of network risks should be raised. Secondly, in the situation, it is recommended to formulate definite laws and regulations, implement hierarchical management of the network, and reduce negative incentives on the internet. Finally, as the potential offenders, it is recommended that network monitoring should be strengthened, moral ethics should be enhanced, and personal motivations for network deviation should be suppressed.

Keywords: gender, cyber-fraud victimization, cyber routine activity theory, self control theory, repeated victimization

目錄

表目錄

圖目錄

第一章 緒論

本章共分為三節，第一節係研究問題背景及重要性、第二節則列述研究動機及目的，第三節為相關名詞詮釋，以下分次說明各節內容:

第一節 研究問題背景及重要性

一、研究問題背景

2019 年 3 月，長期研究網路趨勢分析研究機構 Pew Research Center 發表一份有關他們自 2000 年迄今對美國成人長期網路使用行為之觀察分析。據內容指出，隨著網路發展，美國網路的成人使用者自 2000 年至 2018 年止，從總人口數的 52%上升至總人口數的 89%，同時，報告顯示大約 4 分之 1 的美國成年人表示他們「幾乎每天經常」上網。

根據 Insight-Xplorer 創市際市場研究顧問 2020 年臺灣上網率追蹤調查(如圖 1-1-1 所示)，自 2005 年 6 月至 2019 年 6 月，我國整體上網率從 50.8%成長至 89.6%，整體上網率成長近 2 倍。另根據財團法人臺灣網路資訊中心於 2020 年所公佈「2019 年臺灣寬頻網路使用調查報告」，推估全國 12 歲以上上網人數達 1,898 萬人；而全國上網人數更首次突破 2,000 萬人，高達 2,020 萬，相較於 1996 年全國僅 40 萬用戶，在這 20 年期間內成長了 50 倍之多。眾多的網路使用人口及網路普及率的提升均顯示網際網路已與我們生活密不可分，同時，網路的迅速發展亦增加不同年齡層接觸網際網路的機會。

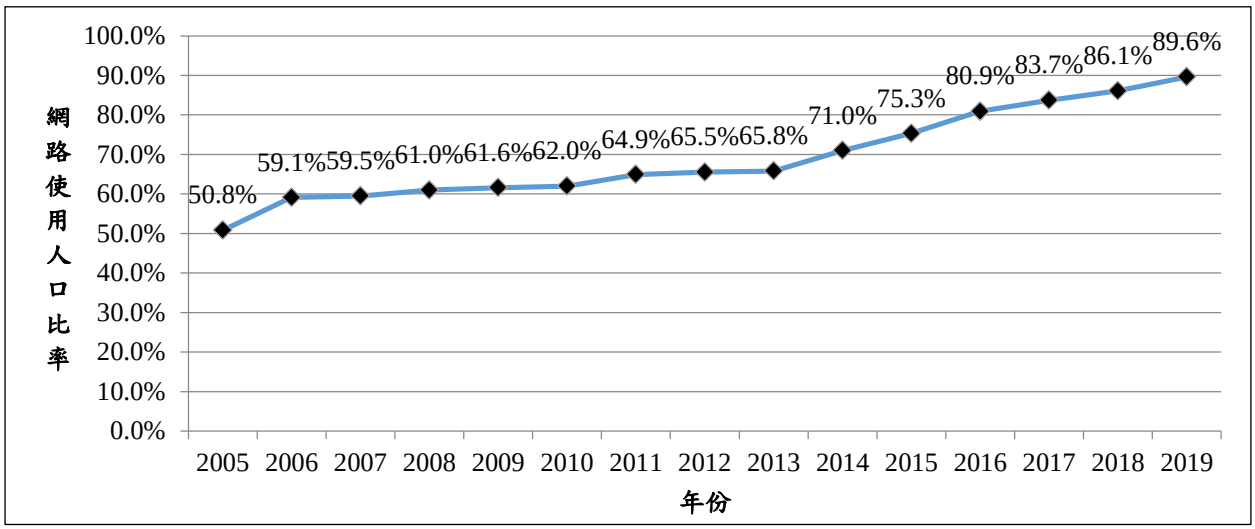

圖 1-1-1 2005-2019 年臺灣地區 12 歲以上民眾網路使用人口比例

（資料來源：整理自 Insight-Xplorer 創市際市場研究顧問臺灣網路使用行為基礎調查）

Cohen 和 Felson(1979)指出，通訊技術的變化將使社會結構產生改變，並因此滲透進入人們的日常生活中，進而改變人們日常生活中的各種接觸型態。隨著網路使用率持續上升，消費者可以在網路上進行許多不同的日常活動（例如使用網路銀行交易、網路通訊及網路購物）及各種網路行為。根據資策會產業情報研究所(MIC)於 2019 年 6 月份針對消費者網路購物行為進行的一項調查發現，臺灣網友網購習慣持續加深，全臺具有網路購物經驗的網路使用者高達 8 成，在日常購物頻率方面，臺灣網路使用者於日常購物頻率中，整體網路購物的頻率已相當接近實體購物（網路購物已達 45%），亦即每 10 次購物行為中，約有 4.5 次是透過網路購物的管道，其中，21~45 歲族群的網路購物頻率又高於整體平均，顯見臺灣網路購物的高普及率。

根據亞太知名網路高科技行業諮詢機構——灼識諮詢有限公司（China Insights Consultancy，以下簡稱 CIC）2019 年 3 月份所發表的最新報告指出，2015 至 2018 年臺灣網路購物人數的複合年均增長率為 3.5%，達到 1,500 萬人（約占 87%的網路使用人口）。不僅網購人數增加，每個人的網路購物花費也越來越高，平均每人每年在網路購物的支出從 2015 年的 24,700 元增加至 2018 年的 29,400 元，根據 CIC 報告顯示，從 2018 至 2022 年，複合年均增長率為 3.0%，預計在 2022 年每人網購花費將達到 49,900 元。上述數據顯示隨著網路的普及化，使人們的消費習慣產生改變，網路購物用戶數、線上訂單及每筆消費金額亦持續增加，而網路購物行為的增加也使網路使用者經常透過網路管道以傳送個人的私人資訊或財務訊息(Newman & Clarke, 2003)。

網際網路的迅速發展及日新月異雖隨時提供我們多樣且豐富的資訊、提升了生活的便利性，但同時也產生了許多新型態的犯罪類型、犯罪手法與不同的犯罪管道。犯罪者透過網路開創新的犯罪管道，使網路成為犯罪的媒介，提供了更多元的「場域」與「機會」（陳玉書、曾百川，2007；張耀中，2009）。資安大廠賽門鐵克(Symantec)旗下諾頓公司(Norton)於 2018 年發布最新「網路安全調查報告」，報告指出 2017 年，近 400 萬名臺灣人曾是網路犯罪的被害者，因網路犯罪造成的總損失超過新台幣 346 億元，平均每位被害者的損失為 8,886 元（中央社，2018），具體揭示網路犯罪被害之嚴重性。

蔡佳瑜(2010)認為，犯罪經常是依附於日常合法活動所建構之社會體系中。Flanagin、Hocevar 和 Samahito(2014)指出，多數美國網路使用者每天都在搜尋網路產品資訊並進行網路購物行為。雖然網路購物向消費者提供直接購物的渠道，提供成本和時間效率的選擇，但相對而言，可能將會對網路詐欺行為產生無人監控的風險。網路環境不同於傳統的實體環境，是個非地域化、虛擬化的環境，故缺乏許多傳統物理環境中所能辨識的訊息，使理性決策者無法根據這些環境訊息做出正確決定，而匿名的網路環境更使網路使用者很難辨別出具詐欺性的探測，從而使個人遭受網路詐欺被害之風險增加(溫怡婷，2008 ; Bay, Cook, Grubisic, & Nikitkov, 2014)。網路詐欺目的在於以各種不同的詐騙手段使被害者交付個人財物，犯罪者以多樣的手段竊取個人私人資訊，並進一步誘使被害者以各種方式交付其財物，進而達到其詐欺目的(蔡田木、周文勇、陳玉書，2009 ; Buchanan & Whitty, 2014; Pratt, Holtfreter, & Reisig, 2010; Reyns, 2013; Vahdati & Yasini, 2015)。

Cohen 和 Felson(1979)指出，通訊技術的變化可能會影響個人犯罪被害暴露程度。網際網路的普及化從根本上改變了消費者的消費型態，並同時擴大了網路詐欺犯罪者鎖定網路消費者的機會，使網路詐欺犯罪及被害案件上升。據內政部警政署刑事警察局(2020)統計(如表 1-1-1 所示)，網路詐欺案件自 2014 年至 2019 年間，每年大約發生 3,000 至 5,000 件，平均每日有 10 位國人受騙，具體地揭示網路詐欺犯罪之嚴重性。

表 1-1-1 2014 年至 2019 年網路犯罪案件發生概況表

年度		發生數(件)						破獲數(件)	破獲率(%)
			所占比例(%)	詐欺	妨害電腦使用	侵害智慧財產權	妨害名譽(信用)		
2014年		18,725	90.52	5,714	7,555	2,280	1,401	7,674	40.98
2015年		12,586	81.81	3,979	2,854	1,981	1,482	8,920	70.87
2016年		13,362	81.99	4,521	2,325	2,243	1,866	9,578	71.68
2017年		14,997	72.17	4,274	2,066	2,162	2,322	11,854	79.04
2018年		13,714	75.90	4,093	1,735	1,999	2,582	10,963	79.25
2019年		12,844	76.16	3,871	1,692	1,593	2,626	10,353	80.61
較2018年	增減%	-1,005	(0.07)	-260	-119	-412	35	- 622	(1.36)
	增減%	- 7.26	—	- 6.29	- 6.57	- 20.55	1.35	- 5.67	—

(資料來源:內政部警政署刑事警察局，2020)

Reyns(2013)認為，隨著網路的發展，人們所參與的日常活動並不僅限於某一特定物理位置或一天中的某些特定時間，而網路上的犯罪模式也因此而生重大變化。Newman 和 Clarke(2003)指出，社會結構的變化以及其所衍生出的犯罪模式變化，可歸因於科技技術與網際網路的進步，而網路接觸者的匿名性、網路搜尋個人訊息的便利性、易於傳送詐欺訊息以及缺乏強而有力的法律監控，則有助於增加犯罪活動。Holt 和 Bossler (2009)、Savona 和 Mignone(2004)認為網路上的犯罪模式正在發生巨大轉變，網路犯罪者可以在任何時間、地點，以低成本卻高效率的網路管道與大量潛在被害者進行接觸，使得傳統物理空間中加害者與被害者時空上之聚合要素越來越不受限制。

綜上所述，隨著網路科技之進步與普及，不同於傳統犯罪類型之網路犯罪漸漸出現，成為大眾所關注的重要議題。在這些網路犯罪類型中，尤其以「網路詐欺犯罪」案件占最多的比例。根據內政部警政署刑事警察局(2020)針對 2019 年網路犯罪發生案件進行統計（如圖 1-1-2 所示），2019 年網路犯罪發生數 1 萬 2,844 件，較上年減少 1,005 件(-7.26%)。網路犯罪案類中主要以「詐欺」3,871 件（占 30.14%）最多，「妨害名譽（信用）」2,626 件（占 20.45%）次之，「妨害電腦使用」1,692 件（占 13.17%）居第 3，三者合計共 63.74%（內政部警政署刑事警察局，2020）。

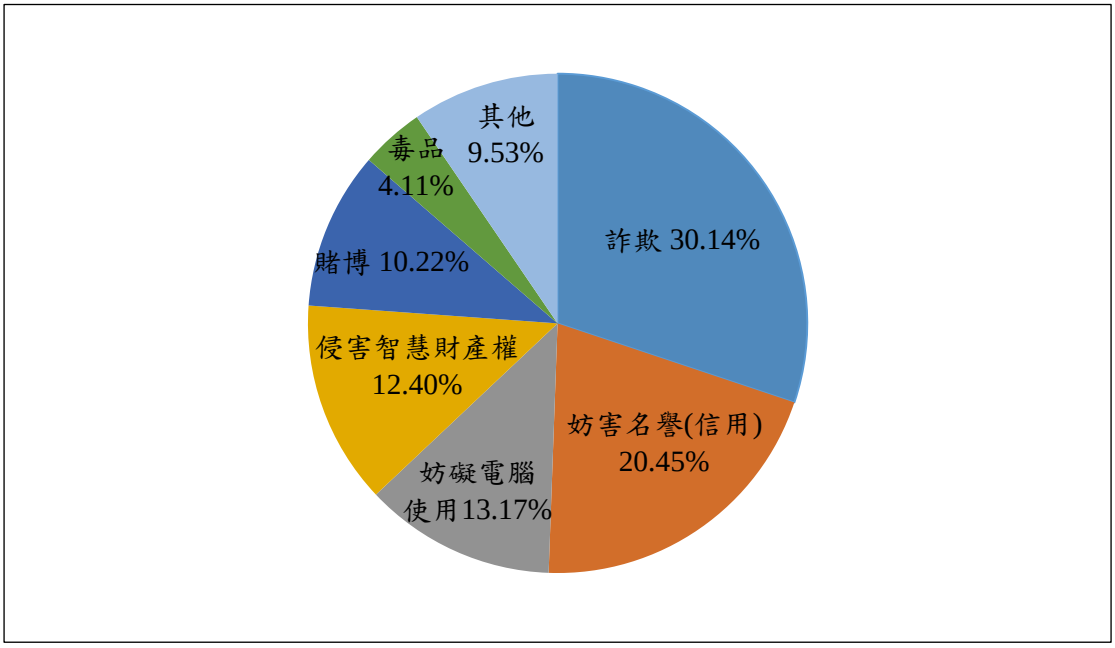

圖 1-1-2 2019 年網路犯罪類型

（資料來源:內政部警政署刑事警察局，2020）

一直以來，在犯罪學研究的範疇中，性別皆為預測犯罪或被害程度的一個重要指標。許多研究指出，男性與女性無論是在生活型態、日常生活、想法思考或是行為舉止方面均有所差異，這樣的差異直接或間接地影響了兩性之間犯罪或被害的程度。根據內政部警政署(2020)對於 2012 年至 2019 年網路詐欺犯罪被害人口進行性別差異分析(如下圖 1-1-3 所示)顯示，近 8 年來，兩性在網路詐欺犯罪被害方面，均持續具有差異，且男性被害人口比率均大於女性，顯見兩性在網路詐欺犯罪被害差異之特殊性。

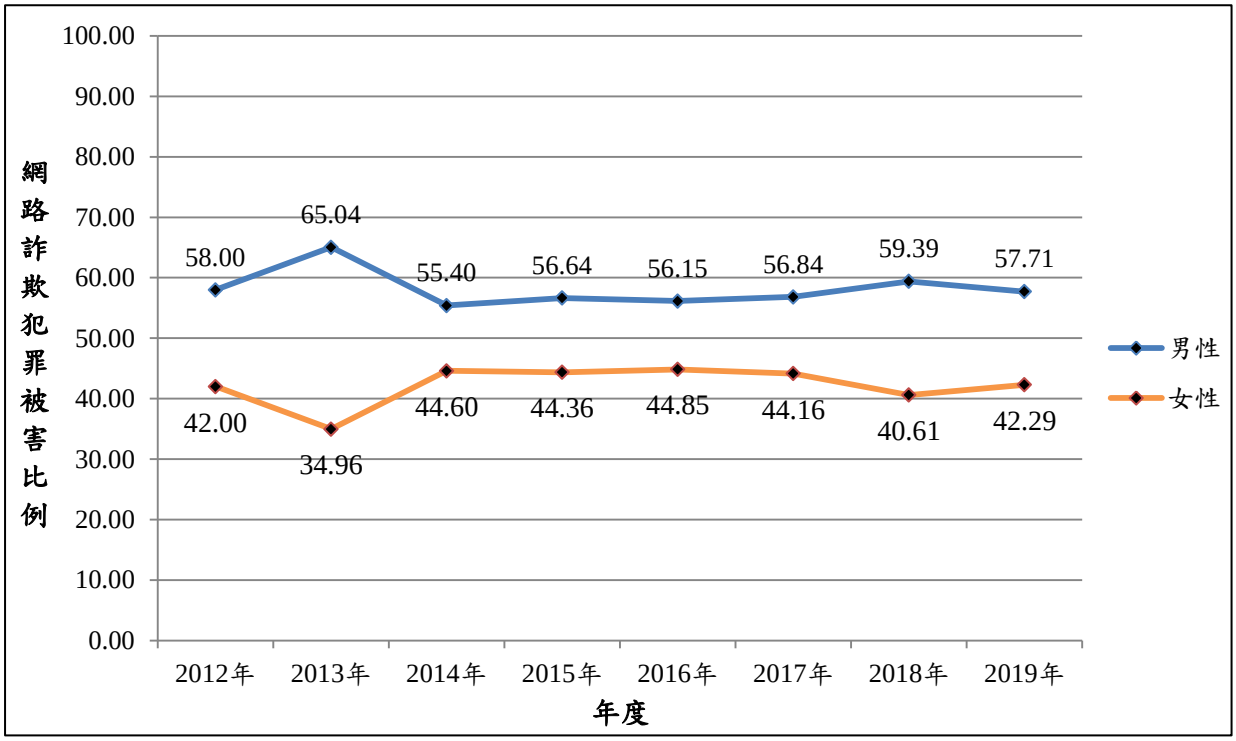

圖 1-1-3 2012-2019 年網路詐欺犯罪被害性別比例統計

（資料來源:整理自內政部警政署，2020）

綜上所述，隨著科技日新月異及網路使用率持續上升，世界各國的網路犯罪情況亦日益嚴重。在各種網路犯罪的類型中，尤其以網路詐欺犯罪為現今網路犯罪與被害的主要類型，近年來的被害人數及損失金額也屢創新高。此外，從上圖 1-1-3 可知，歷年來兩性在網路詐欺被害方面持續具有差異存在，因此，除了必須對於現今普遍存在的網路詐欺被害現象進行深入瞭解外，更需正視兩性之間的被害差異情形，了解其被害現況、深入探究其行為歷程及被害原因，並建立解釋兩性網路詐欺被害差異之理論模式，以期防患於未然。

二、研究重要性

（一）「網路詐欺」已成為現今網路犯罪與被害的主要類型

資安大廠賽門鐵克(Symantec)旗下諾頓公司(Norton)於 2019 年全球性網路犯罪研究發現，全球平均網路犯罪被害者比例大約佔總人口數的 3 分之 2，在美國、巴西、中國則分別有 73%、76%及 83%的人曾經歷網路犯罪被害。網路的快速發展使得人們的日常生活以網路為重心，網路虛擬世界更成為人們的重要生活場域，有鑑於未來網路使用率持續上升，網路犯罪必然成為犯罪主流。在眾多網路犯罪類型中，尤其以網路詐欺犯罪最為盛行，也成為現今網路犯罪與被害的主要類型。

臺灣曾因廣泛且嚴重的詐騙犯罪行為而被世界各國稱為「詐騙之島」，許多國內外學者亦針對臺灣廣泛的詐騙犯罪現象進行深度探討。經警政署刑事警察局(2020)統計，自 2012 年至 2014 年，網路詐欺犯罪發生率一直居於我國網路犯罪之第二位，然而，自 2015 年起迄今，網路詐欺犯罪的發生率卻超越其他網路犯罪類型而高居首位。從上述資料可知，我國網路詐欺犯罪近年來案件迅速增加之嚴重趨勢，因此有關網路詐欺犯罪之被害研究儼然成為刻不容緩的重要議題，故強化對於不同性別間網路詐欺犯罪被害之了解，不僅具有研究之急迫性，亦具有犯罪預防之重要性。

（二）網路詐欺犯罪案件潛在被害者眾多

根據內政部警政署刑事警察局(2020)統計，網路犯罪的比例從 1997 年佔全般刑案之 0.7%，截至 2019 年已佔全般刑案之 5.11%。2001 年刑事警察局全年度所破獲的網路詐欺案件尚未達百件，但從 2016 年開始，全年度網路詐欺案件報案數已超越 4,000 件，這個數據顯示，網路詐欺犯罪案件數在 16 年內成長了近 40 倍之多。

根據學者研究發現，官方所登載的網路詐欺案件數量雖逐年升高，但仍有許多人在網路被害後因為損失金額不大、已向公司申訴，或是覺得丟臉等因素而認為不用報警（鄭佳虹，2006），也因此，實際上向官方機構報案者，往往僅佔實際犯罪案件的 3 至 4 成（吳怡靜，2005）。

此外，日本學者 Taisuke Kanayama(2017)對日本國內網路犯罪被害情形進行全國性

調查，除了發現網路詐欺案件數量的持續攀升及巨大的損失金額外，亦發現網路犯罪被害者實際向警察等官方機構報案的比例僅佔 32%，換言之，大約 3 分之 2 的網路犯罪被害者未向官方機構報告其犯罪被害。英國學者 Goucher(2010)對於英國網路犯罪被害者的一項研究中發現，被害者中僅有 34%曾向警方報案。透過上述數據顯示，隨著網路使用人口日益增加，網路詐欺犯罪的實際數量可能遠高於官方所登載之犯罪統計數據，故網路詐欺犯罪之潛在被害者數量實不容小覷。因此，透過強化對網路詐欺犯罪之了解，除有助發掘潛在之被害者外，更有利於提升犯罪偵查技巧及擬定相關防制策略。

（三）網路詐欺被害特性有別於一般傳統犯罪

在傳統犯罪學及被害者學領域中，大多數理論被運用於解釋暴力或財產等犯罪行為，但網路詐欺與傳統犯罪型態不同，係一種新興之犯罪型態，此種新型態的犯罪類型透過網路的創建和擴展，使犯罪者與潛在被害者間的接觸不受時間與空間之限制(Newman & Clarke, 2003; Wall, 2007; Yar, 2005)。

傳統的詐欺犯罪必須透過犯罪者與被害人面對面直接地接觸與互動而遂行其犯罪行為，但有鑑於網路技術的進步，人與人之間的交流已不須透過傳統直接接觸，而是透過各種不同的網路管道以進行虛擬世界的互動。此外，匿名性的網路環境也使網路使用者難以辨別出這種具詐欺性的探測(Bay et al., 2014)，故若仍以傳統的理論觀點來分析網路犯罪行為，將難以完整了解及精確掌握犯罪現象。

Newman 和 Clarke(2003)指出，網路行為（尤其是網路購物），為詐欺目標和被害提供了多種的機會，雖然我們對網路詐欺犯罪被害情形的理解有所增加，但對於針對特定犯罪目標之進一步了解，將有助於提升犯罪預防工作。未來預估因網路的普及率與國人網路使用習慣之提升，網路詐欺被害的案件數將會不斷攀升，而網路詐欺犯罪類型正如變形蟲一般，報章媒體的宣導永遠都只能見招拆招，無法防患於未然（葉雲宏，2008）。綜上所述，透過對於不同性別網路詐欺被害者之個人特性及網路生活型態進行分析，將有助於對網路詐欺犯罪與被害間潛在的因果機制之深入了解、增加被害原因解釋之基礎，並有助於形塑網路詐欺被害理論架構，以制定合宜且有效的犯罪預防策略。

第二節 研究問題動機及目的

一、研究動機

首先，根據內政部警政署 2019 年統計顯示，網路詐欺已蔚為網路犯罪主流，網路使用者中大多為年輕族群，網路詐欺案件「犯罪者」及「被害者」之主要年齡層集中於 18 到 39 歲，分別占將近 74%及 60%，形成了所謂「年輕人騙年輕人」的犯罪型態（自由時報，2020）。根據內政部警政署 2020 年統計（如下表 1-2-1 所示），歷年來兩性在網路詐欺被害上持續具有差異，在 2019 年，男性被害人數為 2,234 人（佔總人數 57.71%）、女性被害人數為 1,637（佔總人數 42.29%），兩者比例相差近 20%，而警政署 2019 年 7 月發布之「警政統計通報」亦指出，2019 年 1 至 6 月以 LINE 通訊軟體實施網路詐欺的案件中，被害人共有 585 人，其中以男性 364 人（占 62.22%）居多，女性在網路詐欺被害案件中卻僅占 38.78%，兩者在被害數據上之差異高達 23.44%，亦有所差異。

雖然上述官方統計數據顯示兩性在網路詐欺被害方面具有差異，但依據國家通訊傳播委員會(NCC)於 2020 年 1 月所發表之「2019 年寬頻使用調查結果摘要報告」中指出，就網路使用人口的性別分析部分，男性及女性網路使用率分別為 51.2%及 48.8%，並未有顯著差異。就上述網路詐欺被害及網路使用的數據而言，兩性在網路使用的情形上雖未有太大的差異，但在被害數據上卻呈現出明顯的差異。

表 1-2-1 2012 年至 2019 年網路詐欺犯罪被害性別比例差異概況表

年(月)別	男性		女性		合計	
	人數	百分比	人數	百分比	人數	百分比
2012 年	2,018	58.00	1,432	42.00	3,480	100.00
2013 年	1,043	65.04	560	34.96	1,603	100.00
2014 年	3,135	55.40	2,524	44.60	5,659	100.00
2015 年	2,275	56.64	1,741	44.36	4,016	100.00
2016 年	2,578	56.15	2,013	44.85	4,591	100.00
2017 年	2,224	56.84	1,688	44.16	3,912	100.00
2018 年	2,412	59.39	1,605	40.61	4,017	100.00
2019 年	2,234	57.71	1,637	42.29	3,871	100.00

（資料來源:整理自內政部警政署，2020）

此外，綜觀國內外有關網路犯罪與一般詐欺犯罪文獻相當豐富，對於網路詐欺犯罪與被害之實證研究亦不在少數。然而，有關深入探究不同性別間網路生活方式所造成的被害風險差異及兩者間是否有特殊關連性之研究卻付之闕如，而經上述數據分析後發現，兩性在網路使用時間並未有明顯差異，但在網路詐欺被害比例上卻有所差異，因此，不同性別被害者是否具有某些特性而容易成為加害者鎖定的對象，值得深入分析與探究。本研究嘗試以量化研究之方式彌補國內有關兩性間網路詐欺被害差異研究之不足，藉由深入探討網路詐欺被害之性別差異，並擬以網路日常活動及自我控制理論為研究架構，除可以對不同性別間網路使用行為及網路詐欺被害差異現象有更全面地了解，亦能發掘易成為網路詐欺被害的對象，期能研擬必要之早期預防措施，此為**本研究動機之一**。

其次，2019 年澳大利亞消費者委員會(ACCC)所發布之報告指出，2018 年因網路詐欺造成的總損失價值超過 9,000 萬美元，報告指出，網路詐欺是一項代價昂貴的破壞性犯罪，而美國國際商業機器公司（International Business Machines Corporation，簡稱 IBM）於 2006 年的調查發現，大約 70%的網路用戶表示他們認為自己更可能成為網路犯罪的被害者而非實體犯罪被害者，大量的網路使用者認為他們在網路上所進行之各項交易行為的風險遠超過其收益(Criminal Law Reporter, 2006)。Anderson(2004)在美國實施的一項全國性調查報告指出，有近 9 分之 1 的人報告他們是網路詐欺的被害者。美國司法部(U.S. Department of Justice)於 2008 年依據上述百分比推算，將 2.21 億網路使用者轉化為近 2,500 萬詐欺受害者後發現，這個人數大約是謀殺、性侵、武裝搶劫和加重襲擊犯罪之被害者總數的 18 倍。此外，更有研究表明，網路詐欺被害人數和因網路詐欺而造成的社會成本遠超過嚴重街頭犯罪所致的數字(Moore & Mills, 1990; Titus, 1995)。

在我國，依據內政部警政署刑事警察局(2020)指出，在現今網路世代中，網路詐欺犯罪已蔚為網路犯罪主流，雖網路詐欺案件破獲率日漸升高，但 2019 年國內整體網路詐欺案件發生數仍多達 3,871 件，較 5 年前案件數增加兩成；其中因網路購物所延伸而來的電信、網路詐欺案件就占了 45%。此外，根據官方資料統計，雖然 2019 年警察機關攔阻民眾被害款項總計 12 億 2 千多萬餘元，但國人遭詐騙損失金額仍高達 37 億 3 千 7 百多萬元，整體詐騙金額相當可觀。另外，資策會於 2011 年的調查發現，臺灣地

區大約每 3 個詐欺犯罪的被害者，就有一位是透過網路管道而被詐騙，若將因故未報案者計入統計數據中，則網路詐欺犯罪之潛在被害人數實不容小覷，而網路詐欺犯罪所造成的被害損失亦因報案率低而無法準確估計。

Anderson(2013)認為，網路詐欺犯罪所造成直接與間接之社會損失不容易準確估計，但其對個人、組織、刑事司法系統及整個社會之影響卻十分巨大。多數學者更指出，由於許多網路詐欺被害者並未向官方機構報告，網路被害者之實際財務影響狀況可能更高，以及多數被害者未意識到其遭受詐欺被害，導致網路詐欺所造成之實際被害損失因無法被量化數據精準估計而被低估(Button et al., 2014; Button, Lewis, & Tapley, 2009; Chang, 2008; Cross, Smith, & Richards, 2014; Standler, 2002)。綜上所述，許多數據均一再顯示，網路詐欺犯罪除已蔚為現今網路犯罪主流，成為網路犯罪與被害之主要類型外，網路詐欺犯罪所造成之巨大財務損失及其破壞金融秩序，嚴重影響公眾生活與社會安定，因此，網路詐欺被害不僅有其研究之急迫性，亦有研究之必要性，此為**本研究動機之二**。

最後，在多數犯罪類型中，少數被害者經歷了多次被害行為，係所謂「重複被害者」。在網路詐欺犯害中，英國 2016 年官方統計發現，有 16%的詐欺被害者在過去一年中是所謂的重複被害者，而多數學者指出，由於網路詐欺重複被害者經常受到財務及心理上之傷害，因此，對於網路詐欺重複被害者之研究確實有其必要性(Button, Lewis & Tapley, 2014; Whitty, 2015; Whitty & Buchanan, 2016; Whitty, 2019)。此外，多數學者亦均指出，重複被害研究無論在犯罪學、犯罪分析及犯罪統計上，皆具有實質且重要的貢獻(Averdijk, 2011; Averdijk & Loeber, 2012; Farrell & Pease, 1993; Farrell & Grove, 2012; Ignatans & Pease, 2018; Whitty, 2015;Whitty, 2019)，在犯罪預防領域中，重複被害研究不僅有助於提前辨識高風險重複被害族群、減少犯罪所產生之高度重複性與集中性現象外，亦能透過將有限之犯罪預防與刑事司法體系的資源挹注於少數的重複被害者中，使整體犯罪預防成效大幅上升。

有鑑於長期以來，多數國內外學者對於重複被害現象之關注，以及重複被害研究在犯罪學、犯罪預防及犯罪分析領域中之重要性，本研究將對於網路詐欺被害者進一步進行分析，期望建構網路詐欺之重複被害指標，此為**本研究動機之三**。

二、研究目的

詐欺犯罪具有多種型態，近年來詐欺犯罪者更加頻繁地以網路為媒介來吸引合適的目標(Newman & Clarke, 2003; Wall, 2007; Yar, 2005)。網路詐欺犯罪係有組織、訓練，利用他人通信，具專業性之團體，並具有成本低、風險低、量刑低及獲利高、隱匿性高之「三低二高」的犯罪特性（陳永鎮，2007）。網路詐欺犯罪者大多接受過專業化訓練，並多為集團化、分工化的犯罪模式，且虛擬網路空間中通常缺乏監控者(Anderson, 2004; Burns, Whitworth, & Thompson, 2004)，因此，即便政府設立許多法令，但由於網路詐欺案件複雜的區域管轄特性，以致於在犯罪偵查及案件追訴、定罪方面均有一定困難度。

當網路詐欺犯罪成功實行時，被害者通常已遭受財物上之損害，而犯罪者也早已透過各種匿名、虛擬的網路渠道消失無蹤，政府機關因而難以實行犯罪之偵查及追訴。此外，在虛擬的網路空間中，潛在的犯罪者無法直接觀察個人的特性，故網路犯罪者常在其日常從事網路活動的期間鎖定被害者。有鑑於網路詐欺犯罪偵查及起訴之不易，對於事前能早期確認、辨識網路詐欺犯罪高被害族群及高風險環境也就成為非常重要的關鍵，本研究期望藉由相關犯罪學理論架構，對於網路詐欺被害有更深入地了解，研擬必要之防治措施，以防患於未然、有效減少網路詐欺被害行為之產生。

基於上述研究動機，本研究擬以網路日常活動理論、自我控制理論為理論分析架構，深入探討不同性別間網路詐欺被害者之相關特性及被害成因，相關研究目的分述如下:

(一)瞭解不同性別網路使用者之被害原因、被害型態及被害損失之分布情形。

(二)藉由分析不同性別網路使用者之個人基本特性、低自我控制、網路生活型態及被害情境與機會，以瞭解其被害差異。

(三)分析經常暴露於網路詐欺被害情境下之個人特性及網路生活型態，以作為網路詐欺被害理論對於被害行為之檢驗，並檢視自我控制及網路日常活動理論對於性別被害差異之理論解釋力及預測力，以提前發掘可能遭受網路詐欺被害之族群。

(四)分析網路詐欺重複被害者特質、低自我控制、網路生活型態及被害情境與機會，以建構網路詐欺重複被害之高風險指標。

(五)根據研究結果，提供具體防治網路詐欺被害建議並作為未來研究參考。

第三節 相關名詞詮釋

本研究相關名詞定義之詮釋，包括網路詐欺犯罪、網路生活型態(網路休閒活動、網路職業活動、網路風險休閒活動、網路風險職業活動)、被害情境與機會(網路安全監控、網路負面誘因、網路偏差動機)及重複被害，以下就各名詞定義分別敘述如下：

一、網路詐欺犯罪

所謂網路犯罪，是電腦犯罪之延伸，故性質上為電腦犯罪之一種，顧名思義，即是透過電腦網際網路設備所遂行之犯罪行為（林宜隆，2000；陳靜慧，2015）。所謂網路詐欺犯罪，蔡田木(2015)指出，網路詐欺犯罪係於網路詐騙型態與預防之道中，透過網路之方式，利用各種人性之弱點，向民眾進行詐騙使其陷入認知錯誤之行為。

本研究將網路詐欺犯罪(Internet Fraud)界定為行為人利用網際網路特性作為工具或手段，於網路拍賣及各購物網、網路聊天室、電子郵件、網路遊戲或網頁等虛擬世界中，以詐騙的方式，傳達虛偽不實的資訊，使被害者陷於錯誤進而交付財物（包括現金、虛擬貨幣等），因而獲取不法利益之犯罪行為（曾百川，2006）。

二、網路生活型態

本研究所稱之「網路生活型態」概念，根據 Choi(2008)研究概念及探索性因素分析所萃取出之因素構面，其中包括「網路休閒活動」、「網路職業活動」、「網路風險休閒活動」及「網路風險職業活動」四個重要概念，茲將其概念及操作性定義分述如下:

(一)網路休閒活動

在網路休閒活動與網路職業活動部分，Choi(2008)網路日常活動理論之研究概念，所建構之指標為網路職業與休閒活動，但本研究依據探索式因素分析結果，將該構面進一步區分為「網路休閒活動」與「網路職業活動」。所謂「網路休閒活動」概念，係指網路使用者日常使用網路時與休閒有關之行為，本研究將網路休閒活動之操作性定義界定為受訪者在「網路生活型態量表」中「網路休閒活動」構面之得分情形，在量表加總後總得分越高，代表個人以網路從事其休閒活動的機會也越高。

(二)網路職業活動

所謂「網路職業活動」概念，係指網路使用者日常使用網路時的各種與職業有關之行為，本研究將網路職業活動之操作性定義界定為受訪者在「網路生活型態量表」中「網路職業活動」構面之得分情形，在量表加總後的總得分越高，代表個人以網路從事其職業活動的機會也越高。

(三)網路風險休閒活動

所謂「網路風險休閒活動」概念，係指網路使用者日常使用網路中從事具有風險性的休閒活動行為。本研究將網路風險休閒活動之操作性定義界定為受訪者在「網路生活型態量表」中「網路風險休閒活動」構面之得分情形，在量表加總後的總得分越高，代表個人以網路從事具風險性休閒活動的機會越高。

(四)網路風險職業活動

所謂「網路風險職業活動」概念，係指網路使用者日常使用網路中從事具有風險性的職業活動行為。本研究將網路風險職業活動之操作性定義界定為受訪者在「網路生活型態量表」中「網路風險職業活動」構面之得分情形，在量表加總後的總得分越高，代表個人以網路從事具風險性職業活動的機會越高。

三、被害情境與機會

本研究所稱之「被害情境與機會」概念，係指犯罪被害發生的情境及其機會，係以個人上網時有無外在社會或物理監控以遏止其網路詐欺犯罪被害發生、個人在網路使用過程中是否接收負面誘因訊息及個人上網時是否有曾有網路偏差動機等四個因素加以探討，綜合探討網路被害情境與機會之影響力。以下就上述概念之操作性定義界定如下:

(一)網路安全監控

所謂「網路安全監控」，係由 Choi(2008)研究中的「數位監控」(Digital Guardianship)概念所轉化而來，本研究之「網路安全監控」係指有能力監控個人從事網路行為的相關人、事、物，抑或是阻礙具有犯罪動機犯罪者從事傷害、攻擊或獲得標的物的能力。

「網路安全監控」概念，係依據 Cohen 和 Felson(1979)將有能力的監控者分為「社會監控」(social guardianship)及「物理監控」(physical guardianship)兩個概念。

「社會監控」係指除了個人以外，有能力遏止個人免予遭受被害之第三人。「物理監控」是指被害者本身所採取降低風險發生的基本預防措施，透過增加個人的危機意識及防護措施可以有效地減少個人被害機會之發生。本研究將「物理監控」及「社會監控」之操作性定義界定為受訪者在「物理監控」及「社會監控」構面之得分情形，在量表加總後的總得分越高，代表個人在網路使用時的物理或社會監控程度越高。

(二)網路負面誘因

本研究所稱之「網路負面誘因」，係指網路使用者在使用網路的過程中，曾經接收、看到非法或偏差誘因訊息的機會，進而提供機會而造成網路偏差行為的發生。本研究將其操作性定義界定為受訪者在「網路負面誘因構面」之得分情形，在量表加總後的總得分越高，代表個人在網路使用過程中所接收到的負面誘因越多。

(三)網路偏差動機

本研究所謂「網路偏差動機」，係指網路使用者在網路使用過程中，曾經出現網路偏差動機之情形。本研究將其操作性定義界定為受訪者在「網路偏差動機構面」之得分情形，量表加總後總得分越高，代表個人在網路使用過程中有越高的網路偏差動機。

四、重複被害

所謂重複被害，包括在某特定時間或地點遭受相同犯罪類型被害之反覆被害(Repeated Victimization)，及在某特定期間或地點遭受 2 種以上的被害類型之多重被害(Multiple Victimization)兩個意義。Chang 等人(2003)則將重複被害界定為，個人在過去 1 年(12 個月)內遭到 2 次以上之被害行為。Doerner 與 Lab(1998)將重複被害定義為，重複發生於同一人或同一地點之被害現象。

本研究綜合上述學者定義，將重複被害(Repeated Victimization)界定為在過去 1 年(12 個月)內，遭受 2 次以上網路詐欺被害之行為。

第二章 文獻探討

本章依據前述研究動機與目的，可分為兩大探討內涵，首先是探討虛擬網路空間中情境與機會要素之相關理論、其次則為探討個人自我控制程度之相關理論。因此，本章共分為六節，第一節為探討情境、機會與網路詐欺被害之相關理論、第二節為探討自我控制與網路詐欺被害之相關理論、第三節為探討日常活動與自我控制間之關聯性、第四節為探討性別差異與被害行為、第五節為探討網路詐欺犯罪被害之相關實證研究，最後一節則是根據前述文獻與研究所導引出之綜合評述。

第一節 情境、機會與網路詐欺被害相關理論

一、生活型態理論

20 世紀末葉後，犯罪學者關注的焦點逐漸從「犯罪原因」和「犯罪動機」轉移至犯罪發生的「情境」和「機會」因素，進而發展所謂的「環境犯罪學」(Environmental Criminology)。環境犯罪學著重於犯罪事件發生之情境與機會，認為犯罪係植基於行為者的日常活動、平日的生活交集，以及他們與周圍社會和物理結構的相互作用，並透過這些因素的聚合為犯罪創造了機會，並形成了在時間和空間上分佈不均的犯罪模式。

生活方式理論(Lifestyle Theory)，或稱為生活型態—暴露理論(Lifestyle/Exposure theory of Personal Victimization)，係由 Hindelang、Gottfredson 及 Garofalo 於 1978 年依據犯罪被害調查後所提出之環境犯罪學理論，主要探討個人為何會成為犯罪被害者之重要因素。Hindelang 等人於 1976 年對於美國八個城市進行犯罪被害調查，發現犯罪被害者的人口特性並非隨機分佈，並將探討重點置於個人的「生活方式」，而「生活方式」係指個人日常生活的各項活動，包括個人的職業及休閒活動兩個層面。理論認為個人的犯罪被害程度係取決於其生活型態，個人成為犯罪被害者，係因其生活型態增加了與犯罪者互動的機會，因此犯罪被害的風險與個人特性或生活型態有關（許春金，2013）。

Hindelang 等人(1978)認為個人的「職業和休閒活動」是生活方式中最重要的組成要素，直接影響個人被害風險的程度，所謂「職業活動」包括工作與求學，而「休閒活動」則包括個人日常從事的各項休閒娛樂活動。因此，個人的職業和休閒活動影響其生活方

式，而生活方式又影響著個人的犯罪被害風險。

此外，個人的預期社會角色和社會結構亦影響其生活方式，並有助於個人決定參與某些風險活動。所謂「預期社會角色」，或稱為社會角色期待，係指大眾依據個人在社會結構中的地位而對個人產生的角色期望，而「社會結構」即是社會上各種既定的制度（例如:家庭、教育、經濟、法律等）。個人在社會結構中的地位決定了社會大眾對他的角色期待，社會結構則限制了個人行為的選擇，進而產生了適應生活的行為模式，並表現於個人的職業及休閒活動兩個方面，而每個人在特定的時間、特定的地點與特定的人接觸，自然會有不同的機率成為被害者，因此被害的情形並非隨機分布（林和男，2004）。

生活方式暴露理論認為犯罪並非隨機分布，犯罪者與被害者的生活型態具有關聯性，並認為兩者具有相同的生活方式及人口特性，亦即不同基本背景之個人，因社會期待、社會結構及生活調適之不同，而形成不同之生活型態，使個人面臨不同程度的被害風險(Hindelang, Gottfredson, & Garafalo, 1978)。因此，當個人的生活型態與犯罪者接觸的機會越高，其暴露於危險情境的機會越多，個人被害的可能性也就越高。

Hindelang 等人(1978)指出，個人的生活方式建構其被害的機會，並提出八項重要的具體命題，藉以進一步說明「生活方式」、「人口變項」與犯罪被害間關聯性之連帶關係（黃富源，2002）：

命題一:個人被害可能性與其暴露於公共場所時間多寡成正比，特別是夜晚公共場所。

命題二:個人置身公共場所可能性隨其生活方式不同而有所差異，尤其夜晚較為明顯。

命題三:具有類似的生活方式，彼此間接觸互動之機會較多。

命題四:個人被害之可能性，端視其是否具有與加害者相類似之基本特性。

命題五:個人與其家人以外成員接觸時間之多寡，隨其生活方式之不同而所有差異。

命題六:個人被害之可能性，隨其與非家人接觸時間之多寡而定，尤其是竊盜罪。

命題七:生活方式之不同與個人阻絕和具有犯罪特性之人接觸能力之差異有關，即個人愈常與有犯罪特性之人接觸，其被害可能性也就愈大。

命題八:生活方式之差異與一個人成為被害之方便性(convenience)、誘發性 (desirability)及易於侵害性(vulnerability)之差異有關。

二、日常活動理論

日常活動理論係由美國犯罪學者 Cohen 和 Felson 於 1979 年提出，理論認為犯罪率的變化並非社會的病態因素，而是涉及人們日常生活的改變，並認為犯罪與合法行為兩者並非獨立事件，而是共同存在於人們的日常生活當中。大多數犯罪學理論，著重於解釋犯罪者的行為動機與原因，但 Cohen 和 Felson 認為以加害人為主要核心研究對象的傳統犯罪學理論，並無法有效解釋 1960 年代美國犯罪率持續攀升的現象及原因，故將理論探討重心置於社會變遷對於犯罪現象的結構性影響。在犯罪行為的探討方面，理論認為加害者本就具有犯罪之傾向，個人在從事犯罪行為前會先經過理性選擇思考、判斷犯罪的成功機率後才會實行。此外，日常活動理論認為個人的日常生活模式以及他們所涉及的「日常活動」會影響這些因素在時間和空間上的聚合因而產生犯罪的可能性。

日常活動理論是種犯罪因果論，將犯罪行為與人們日常生活聯繫在一起，認為隨著日常活動方式的不同(改變)，就有可能改變犯罪發生的可能性(周愫嫻、曹立群，2007)。Cohen 和 Felson(1979)認為犯罪和被害事件是時空因素聚合下的結果，並進一步提出，當具有動機的犯罪者和合適的標的物（被害者、財物），在缺乏具有能力或有效監控的環境中聚合時，就會產生被害的機會，這也代表著當被害者和犯罪者同時聚集在同一個缺乏監控的環境時，就可能產生犯罪。

近年來，許多學者將日常活動理論應用於解釋虛擬網路世界之犯罪行為。Grabosky (2001)認為傳統用以解釋實體物理環境犯罪之日常活動理論，亦可以用以解釋虛擬網路環境中所發生的犯罪行為，藉以建立虛擬網路和實體場域犯罪行為間理論架構之一致性。Yar(2005)則提出了關於日常活動理論是否可用以解釋網路犯罪的系統性理論反思，對於日常活動理論中的犯罪三要素是否能有效解釋虛擬世界中的網路犯罪則主張，有動機的犯罪者無論是在現實物理環境或虛擬網路世界，皆能相互對應，因此，有能力監控者的概念適合運用於虛擬世界中，並認為這些概念與傳統犯罪僅為程度上而非本質上的差異，故理論在網路犯罪方面仍然具有高度解釋力。Clarke(2004)亦認為網路有助於在缺乏監控的系統或場域中使有動機的犯罪者和合適的目標聚合，從而創造有利於被害的環境。

雖然多數學者皆認為以往用以解釋物理環境的日常活動理論可適用於虛擬網路場域的解釋，但仍有部分學者對此提出質疑。Capeller(2001)認為，網路是一個不同於傳統物理環境的虛擬場域，在此無實體、無物質的場域中，時間與空間的聚合並不受到限制，故對於此虛擬網路世界必須要修改相關哲學、歷史及社會性的假設，對於虛擬網路空間的研究亦應修改原有的理論架構與假設。此外，雖然 Yar(2005)認為日常活動理論可適用於解釋虛擬網路空間，但他認為實體物理環境與虛擬網路空間確實有其差異，故進一步提出並非日常活動理論之所有要素皆可轉化成為網路變項（例如，慣性/可移動性很難以直接轉換至虛擬網路環境）。除了探討日常活動理論各要素對虛擬環境的可轉換性之外，Yar(2005)還進一步發展了他所謂的「網路空間的生態學」(Ecology of Cyberspace)。他認為日常活動理論是犯罪因果關係的一種生態方法，取決於在時空條件下對犯罪者和標的物進行聚合的能力，在虛擬網路空間中，時間與空間並未受到限制，因此，無論人或物之間的距離、時間為何，三要素之間的聚合都是立即共存的。

近年來，日常活動理論逐漸成為犯罪被害者學領域中重要的理論，並被作為不同犯罪被害類型之解釋。隨著網路的發展與進步，以往用以預測整體街頭犯罪率的日常活動理論也被用以解釋許多與網路相關之犯罪被害行為(Bossler & Holt, 2007; Choi, 2008; Grabosky & Smith, 2001; Holt & Bossler, 2009; Holtfreter et al., 2008; Hutchings & Hayes, 2009; Marcum, Higgins, & Ricketts, 2010; Newman & Clarke, 2003; Ngo & Paternoster, 2011; Pratt et al., 2010; Van, 2013; Yar, 2005)。儘管將日常活動理論應用於與傳統物理場域不同的虛擬網路犯罪仍舊存在爭議，但許多實證研究已支持日常活動理論確實能有效預測虛擬網路場域中路被害行為(Bossler & Holt, 2007; Choi, 2008; Holt & Bossler, 2009; Hutchings & Hayes, 2009; Ngo & Paternoster, 2011; Pratt et al., 2010; Pease, 2001; Turanovic & Pratt, 2012; Van, 2013; Yar, 2005)。

日常活動理論認為，網際網路使人們的生活型態產生變化，而日常生活型態的改變、犯罪標的物及監控型態的變化，正反映了「日常活動的變化」（許春金，2006）。此外，根據日常活動理論，網路詐欺犯罪的發生必須在時空因素上由以下三個要素所共同聚合而成：

(一)有動機且具有犯罪能力者

日常活動理論將具有動機的犯罪者視為前提,認為標的物的變化及監控型態的變化反應了犯罪率之變化,此外,在機會允許的情況下,有能力的犯罪者必須是願意犯罪者(Akers & Sellers, 2004)。當整體合法機會結構的改變,會在缺乏有能力監控者的情況下增加具有動機之犯罪者和合適標的物之間的聚合(Pratt et al., 2010)。簡言之,網際網路造成了社會變遷,社會變遷影響了犯罪的型態、管道與機會,擴大了網路詐欺犯罪者鎖定網路使用者的機會。

(二)合適的標的物

所謂合適的標的物,係指犯罪者想要得到或控制的任何人或財物(Felson, 2001)。Felson(1998)指出,犯罪者對於標的物的考量通常基於四個要素,並將四個要素加以縮寫,以 VIVA 簡稱之,其中包括標的物的價值(Value)、標的物的慣性/可移動性(Inertia)、標的物的可見性(Visibility)及標的物的可接近性(Access),以下就四個要素分述如後:

首先,標的物的價值(Value),以網路詐欺犯罪為例,標的物的價值係根源於被害者對於網路交易的需求性,當被害人欲透過網路進行高風險或高投機性之交易時,就容易成為加害人鎖定的高價值之標的物。

其次,標的物的慣性(Inertia),係指其可移動性,Cohen 和 Felson(1979)將可移動性簡要地描述為物品的物理特性以及物體攜帶的容易性程度,但 Yar(2005)指出,文件和技術規範亦可被視為一種可移動性的形式,因為它們決定了目標可能提供的阻力程度,從而影響其理論適用性。

再者,標的物的可見性(Visibility),係指犯罪者如何在其可見的範圍內,去尋找合適的被害者,換言之,係指犯罪者希望竊取或控制物體顯而易見之程度。被害者的網路可見性高低影響個人是否成為合適目標的程度。由於個人長時間的網路活動,使其暴露於被害者可見性及被害情境的機會更高,故當被害人使用網路的時間、頻率越高時,其可見性越高,越有可能成為犯罪者鎖定的對象。

最後,標的物可接近性(Access),指的是加害者如何以最省力與最不暴露自身危險

的方式，在其可見的範圍中，去尋找合適的被害者，遂行其犯罪行為（陳怡儒，2010）。在實體世界中，可接近性包括社區內的分布、商品是否在易於接近的位置及日常生活的其他特徵，這都使得犯罪者更容易與標的物接觸，但在虛擬的網路世界中，網路犯罪者需要操作系統和網頁瀏覽器等軟體與網路使用者加以接觸。

(三)有能力的監控者不在場

所謂監控，係指個人或標的物防止犯罪發生的能力(Cohen & Felson, 1979; Garofalo & Clark, 1992; Meier & Miethe, 1993; Tseloni et al., 2004)，而有能力的監控者，係指能保護標的物或是抑制犯罪行為發生者，除了外在的行為者外，亦包括技術、個人或安全防護措施。當缺乏有能力的監控者在場時，犯罪者便減少受到阻礙之機會，並能直接接觸標的物，從而容易遂行其犯罪行為。此外，日常活動理論將有能力的監控者區分為「物理監控」及「社會監控」等兩個類型(Cohen & Felson, 1979; Mustaine & Tewksbury, 2002)。

首先，「物理監控」(Physical guardianship)係指透過物理環境及物理安全設備（例如：加裝防盜警報器、汽機車安全鎖或其他安全措施）的強化以阻礙犯罪者的犯罪行為，藉由強化外在物理環境的安全性，可有效減少犯罪者直接接觸標的物的機會。此外，物理監控也包括個人的風險意識程度（網路風險技術知識）及其採取降低風險發生的預防措施，當個人具有高度網路技術知識或被害意識時，他們在網路上所面臨的風險就會更低，且能比其他網路使用者更早預測到被害的可能性，從而減少其成為被害者的風險。

其次，「社會監控」(Social guardianship)係指除了個人之外的第三方監控者是否存在現場，此時的旁觀者可以作為有能力的監控者並發揮重要作用，透過社會監控者的存在或與其他鄰居、友人之接觸，能有效減少並遏止加害者從事犯罪行為。

網路場域中通常缺乏上述兩個不同類型的有能力監控者，係因網路是一個虛擬的社群，而非一個實體、物理的場域，且網路行為是一種具有隱私性的私人行為，即使人們身處同一環境，彼此相互約束或干涉的能力也不高，因此通常缺乏社會監控，若此時個人危機意識不足或未採取有效的防範措施，導致缺乏個人監控時，就容易成為網路詐欺犯罪之被害者，這也解釋了網路詐欺犯罪的高被害率。此外，當犯罪過程中缺乏有能力

的物理或社會監控者時，便有利於潛在犯罪者遂行犯罪行為，在犯罪的過程中，被害者大多缺乏被害意識、無法採取有效的防護措施，因此，當被害人察覺其被害之結果後，犯罪行為大都已實施完成，而犯罪者亦早已透過不同的網路渠道消失無蹤。

日常活動理論將具有動機及能力的犯罪者視為前提，以「合適的標的物」、「有能力的監控者」來解釋犯罪行為之發生，認為當人們生活方式發生變化時便會使「合適的標的物」、「有能力的監控者」產生變化，進而影響犯罪率的變化及犯罪行為的發生。由此可知，隨著科技技術的進步及網路的普及化，增加了個人上網之機會，造成消費者改變其日常生活及消費型態，並從根本上改變了社會的互動結構，而透過這種「合法技術的進步」會影響被害者的特質及監控者的型態(Cohen & Felson, 1979)。

綜上所述，在虛擬網路世界中，通常缺乏有能力的監控者，並增加具有犯罪動機的潛在犯罪者，此時若有合適的標的物（財物、被害者），則犯罪行為極有可能會發生。網際網路改變了網路使用者的消費習慣、擴大了網路詐欺犯罪者鎖定網路使用者的機會，因而使得網路使用者之被害機會增加，因此，理論之主張符合以網路互動所進行之詐欺犯罪，當一個具有犯罪傾向且有犯罪能力的網路詐欺潛在犯罪者，在缺乏正式或非正式的物理及社會監控下，發現合適的標的物，從而遂行網路詐欺犯罪行為。有關日常活動理論三要素與網路詐欺犯罪(被害)之間的互動關係，如下圖 2-1-1 所示。

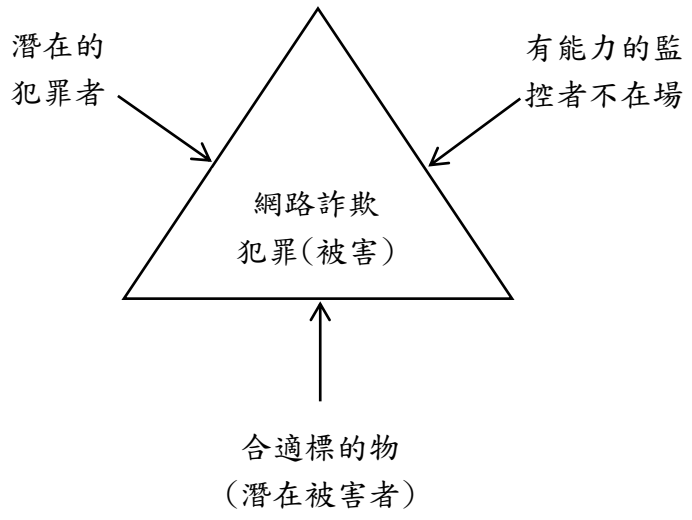

圖 2-1-1 日常活動理論三要素與網路詐欺被害之關聯性

（引自陳玉書、曾百川，2007）

三、網路日常活動理論

一直以來，生活方式暴露理論及日常活動理論大多用以解釋傳統物理環境犯罪被害行為之發生，但近年來多數學者則逐漸將原本用以解釋實體物理環境之二個被害理論，適用於虛擬網路環境中犯罪被害行為之解釋。在理論解釋之轉化過程中，部分學者認為傳統理論的內涵適用於解釋虛擬的網路犯罪被害行為(Bossler & Holt, 2008; Clarke, 2004; Grabosky, 2001; Holt & Bossler, 2009; Holtfreter et al., 2008; Pratt et al., 2010; Turanovic & Pratt, 2012; Van, 2013)，但亦有學者認為虛擬網路世界有其場域之限制，故虛擬場域中的網路犯罪行為並無法透過傳統理論的各個變項加以解釋(Capeller, 2001; Yar, 2005)。有鑑於傳統被害者理論在解釋網路被害行為之爭議性及侷限性，Choi(2008)將上述兩個理論加以整合，結合其中重要概念，據以發展出以網路場域為解釋中心之整合性理論—「網路日常活動理論」(Cyber-Routine Activities Theory，簡稱 Cyber-RAT)，藉以為網路犯罪被害研究帶來更準確的診斷及預測。

在理論重新概念化之過程中，Choi(2008)認為日常活動理論與生活方式暴露理論兩者並非相互獨立的理論，彼此具有相容性，而日常活動理論僅為生活方式暴露理論之擴展，兩者均以微觀層面的角度解釋個人的日常活動、個人與他人的互動及社會結構如何影響犯罪機會之程度。在兩者理論內涵中均有共同的重要原則—生活方式(Lifestyle)。生活方式暴露理論認為，不同的生活方式會使個人暴露於不同程度的被害風險中，一個人的個人特性與生活方式影響其被害風險，並認為個人成為犯罪被害者係因其生活方式增加了與犯罪者互動的機會。日常活動理論亦認為個人的生活方式會影響其日常生活，並將生活方式暴露理論中所強調的「個人職業與休閒活動」的重要概念納入合適標的物的評斷準則中，進而轉化為 Felson(1998)提出四個用以評估標的物合適性的重要指標—VIVA。此外，在日常活動理論中，除了將生活方式的重要概念納入其理論內涵外，亦增加了影響犯罪在時空條件下所必須聚合的其他二個要素，即「具有動機的犯罪者」及「有能力的監控者」。

Choi(2008)擷取生活方式暴露理論及日常活動理論中共同的重要變項—生活方式(Lifestyle)，作為其理論的重要構成要素，並重新將理論再概念化(Reconceptualization)，據而提出網路日常活動理論（Cyber-Routine Activities Theory，簡稱 Cyber-RAT）。網路日常活動理論的核心概念在於，缺乏數位監控及經常從事高風險的網路生活方式會直接影響並增加個人成為網路犯罪被害者的可能性，理論認為導致網路犯罪被害的兩個重要因素包括:「網路生活型態」(Online Lifestyle)以及「數位監控」(Digital Guardianship)，例如:網路安全防護措施，並認為個人的網路生活型態及數位監控在很大程度上解釋了個人的網路犯罪被害行為。

Choi 在其 2008 年的研究中以結構方程式模型（Structural Equation Modeling，簡稱 SEM），對於網路使用者的個人數位監控能力和網路生活型態，是否直接或間接地影響網路犯罪被害進行研究。在其建構之網路日常活動理論架構中，以「網路生活型態」及「數位監控」作為自變項，以「網路犯罪被害」為依變項，探討兩者間的關聯性，有關其研究架構各變項內容分述如後。

首先，在網路生活型態變項中，係由三個不同的觀察變項所建構而成，其中包括:網路職業與休閒活動(Online Vocational and Leisure Activities)、網路風險休閒活動(Cyber Risky Leisure Activities)及網路風險職業活動(Cyber Risky Vocational Activities)。「網路職業與休閒活動」變項係根據 Hindelang 等人(1978)生活方式暴露理論中「個人的職業和休閒活動」概念延伸而來，認為個人的網路職業與休閒活動使個人暴露於不同程度的犯罪被害風險，而「網路風險休閒活動」及「網路風險職業活動」兩個變項則是 Cohen 和 Felson (1979)日常活動理論中用以評估合適標的物的兩個重要風險測量指標，透過這三個變項可有效評估個人網路生活型態的被害風險暴露程度。

其次，在「數位監控」的變項中，則包括網路安全防護數量(Number of Security)以及網路安全防護持續之時間(Duration of Having Security)兩個變項，透過這兩個變項可以了解網路使用者是否採行適當的網路防護措施及採行該措施持續的時間，以了解個人在數位監控上的防護程度。

最後，依變項「網路犯罪被害」部分，係由三個不同觀察變項所組成，其中則包括被電腦病毒感染之頻率(Frequency of Virus Infection)、被害財物之損失(Monetary Loss)及損失時間(Hour Loss)等三個項目。有關 Choi(2008)提出之網路日常活動理論架構，如下圖 2-1-2 所示:

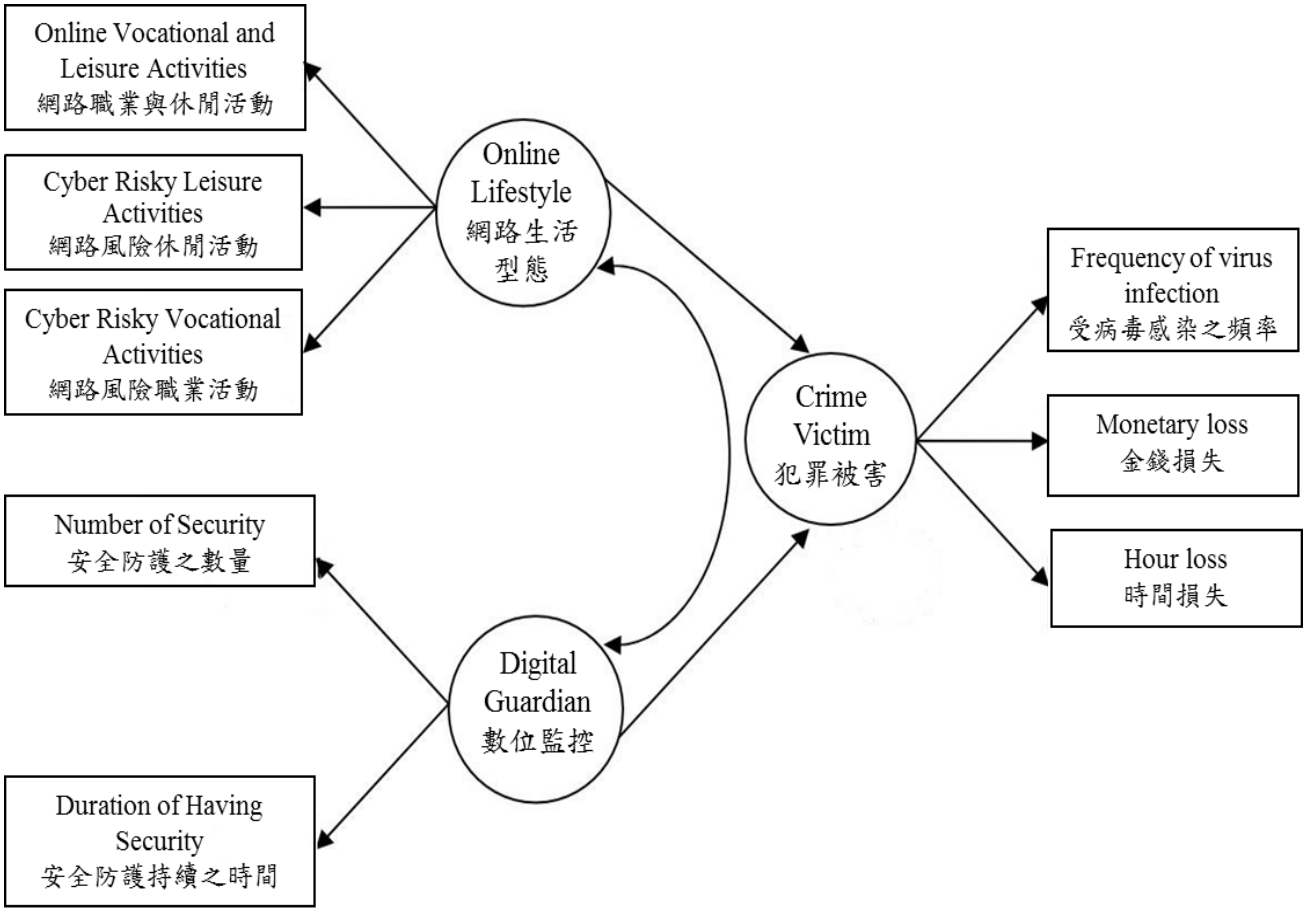

圖 2-1-2 網路日常活動理論架構

資料來源：Choi(2008).Computer crime victimization and integrated theory: An empirical assessment.

第二節 自我控制理論與網路詐欺被害

美國犯罪學家 Michael Gottfredson 與 Travis Hirschi 於 1990 年共同提出自我控制理論(Self-Control Theory)，又可稱為一般化犯罪理論或犯罪共通性理論(A General Theory of Crime)，理論主張犯罪者具有較低的自我控制傾向。自我控制理論係一種強調「自我控制」的控制理論，理論認為人們是理性及欲望的行為者，犯罪動機在所有個體中都是恆久不變的，人們會權衡其行為的成本及利益後，進而採取相應的行動，而犯罪便是一種追求立即利益及滿足的簡單行為。自我控制理論認為人們都具有犯罪的動機及驅力，因此，犯罪者及非犯罪者最大的區別在於個人的自我控制程度，自我控制程度較低者，行為通常較為輕率、缺乏毅力並經常從事尋求當下立即享樂、刺激冒險之行為，著重於當下所見之立即利益而不考慮其行為之長遠後果，因而易於從事犯罪行為。

Gottfredson 和 Hirschi(1990)將古典犯罪學派強調的犯罪行為(Crime Act)與實證犯罪學派強調的犯罪性(Criminality)兩者分別闡述。在其理論定義中，所謂「犯罪」(Crime)係為追求、滿足自我利益所採取的力量或詐欺行為，是在特定時間、空間的點所發生的一個事件或行為，其特徵為短暫的、簡單立即的、令人興奮滿足的且不需要太多技術。「犯罪性」(Criminality)，係指個人追求立即享樂而無視於長遠後果之傾向或趨勢，其最大特徵為「低自我控制」，一般而言，個人的自我控制能力形成於 8-10 歲，一旦形成將影響個人終身且難以改變，而低自我控制形成原因係家庭或學校不良育兒技術所致。

根據 Gottfredson 和 Hirschi(1990)對於犯罪採取之定義—犯罪係為追求自身利益所採行的力量或詐欺行為，說明自我控制理論可適用於解釋與詐欺有關之犯罪行為，故許多實證研究皆以自我控制理論來解釋與詐欺有關之犯罪行為。自我控制理論以共通性的概念解釋犯罪，主張任何犯罪都是「低自我控制」和「適宜機會」結合下的產物。此外，Gottfredson 和 Hirschi(1990)認為並非所有低自我控制者均會從事犯罪行為，犯罪的發生除了需要低自我控制特性外，尚須外在犯罪機會，故援引機會理論及日常活動理論加以闡述。在理論探討後，可以發現「犯罪機會」在網路詐欺中扮演非常重要的角色，主要原因在於網路規範不足，是一個缺乏正式「社會控制」的體系（王秋惠，2007）。

Beaver、Barnes 和 Boutwell (2014)指出，自我控制是指一個人控制、調節自我情緒，行為和慾望的能力。根據 Gottfredson 和 Hirschi(1990)的觀點，缺乏自我控制能力者是衝動地且不關心他們行為的長期後果，一旦有外在的犯罪機會，低自我控制能力者便很有可能參與能夠立即滿足而無需付出任何努力的活動，並經常從事尋求刺激冒險的行為。一般而言，人們的智力和個人背景（如教育程度和早年經驗），決定其自我控制能力(Halpern-Felsher et al., 2001; Hare, Camerer, & Rangel, 2009; Ommundsen, 2003)。

Gottfredson 和 Hirschi(1990)認為，低自我控制也會導致更嚴重的詐欺類型，Holtfreter 等人(2008)認為低自我控制特性顯著增加了個人詐欺被害的可能性，而 Chen 等人(2017)亦指出，自我控制與網路詐欺被害有關，自我控制程度較低者較易成為網路詐欺被害者。綜觀多數研究文獻均指出，個人的低自我控制特質是詐欺被害風險的強力預測因素(Benson & Moore, 1992; Holtfreter et al., 2008; Holtfreter et al., 2010; Langton, Piquero, & Hollinger, 2006; Pratt & Cullen, 2000; Reisig et al., 2009; Simpson & Piquero, 2002)。

長期以來，有關自我控制理論之研究皆側重於犯罪行為之探討，較少關注於被害者之特性。雖然 Gottfredson 和 Hirschi(1990)認為自我控制理論是犯罪的一般性理論，著重於解釋影響犯罪和偏差行為可能性的因素，而非探討犯罪被害的理論，但他們認為犯罪與被害之間具有高度關聯性，兩者皆係因自我控制程度不足所導致。

Gottfredson 和 Hirschi(1990)的理論中蘊含著缺乏自我控制者會選擇進入危險情境的概念。在犯罪環境中，低自我控制者無法準確衡量從事行為的潛在負面後果(Beaver, Wright, & DeLisi, 2007; McGloin, Pratt, & Maahs, 2004)，因此，當個人暴露於危險環境後，低自我控制能力者也將面臨更大的被害風險。此外，低自我控制者通常缺乏同情心，且很難與他人接觸，導致個人外在社會關係弱化，同時也因為缺乏良好的語言溝通能力，故經常誤解他人意圖(Gottfredson & Hirschi, 1990; Schreck, 1999; Pratt, Turanovic, Fox, & Wright, 2014; Reisig et al., 2009)，這種缺乏良好社會關係及低語言協調能力的狀況不僅將使個人的社會支持減少，進而增加其被害的可能性，在虛擬網路環境中更可能因無法準確評估他人意圖，進而處於劣勢的狀況(Herring, 1999; Holtfreter et al., 2010; Schreck, 1999; Wall, 2001)。

Schreck(1999)將自我控制理論重新塑造為一種被害性理論，認為低自我控制者尋求立即享樂感且往往短視近利，因此，他們較可能尋求具刺激、冒險或參與各種具風險性的活動，但卻很少採取必要的防護措施來避免個人的財產被害，從而導致其面臨更大的詐欺被害風險，此外，研究更進一步指出，低自我控制是犯罪被害的強力預測因子。

自 Schreck 於 1999 年的研究後，多數學者便逐漸將自我控制理論應用於犯罪被害的範疇中，以各種不同犯罪類型研究自我控制和個人被害間的關係，經多數研究顯示，低自我控制者較容易做出衝動性的決定，從而增加個人的脆弱性及接觸犯罪者的機會，並增加個人被害的風險(Forde & Kennedy, 1997; Holtfreter et al., 2008; Piquero et al., 2005; Schreck et al., 2002; Schreck et al., 2006; Stewart et al., 2004; Tillyer et al., 2011)。

Gottfredson 和 Hirschi(1990)主張「犯罪」係追求自身利益所採取之力量或詐欺行為。葉雲宏(2008)指出，以網路詐欺犯罪者而言，網路詐欺之行為因為具有立即性、刺激性，故可使他們以最簡單、迅速的方式來滿足個人享樂。以網路詐欺被害者而言，被害者大多與現實社會互動不佳，而低自我控制能力者不僅認為詐欺行為更具吸引力，亦更有可能使自己面臨詐欺被害的風險。此外，低自我控制者在網路所從事的各項交易行為也滿足了個人被害特徵，具低自我控制特質者無法有效抑制個人從事網路交易的衝動，經常尋求短暫且快速達到利益的手段，並期望透過很少的努力或投資而立即獲得大量利益的機會（例如，網路交易免手續費、可獲得折扣等），因而更容易成為網路詐欺被害者。

此外，近期有關自我控制理論之研究得到重要發現。研究指出，自我控制對非直接接觸被害者的影響遠大於直接接觸被害者，換言之，低自我控制在網路被害而非實體物理被害中具有更高的解釋力，研究顯示，低自我控制與網路犯罪被害間存在顯著關聯性，自我控制係網路被害的正向預測因子(Holt & Bossler, 2016; Pratt et al., 2014)。

綜上所述，自我控制理論預測犯罪和被害暴露都是由於個人忽視制定決策長期後果之習慣傾向，多數低自我控制者較為衝動且缺乏未來規劃，他們認為從事詐欺活動具有吸引力，且更有可能採取具風險性的行動，從而使他們容易成為詐欺行為的被害者，故低自我控制能力者的生活中應該普遍存在詐欺和被害行為的共同經驗。

第三節 日常活動理論與自我控制理論之關聯性

自我控制理論與日常活動理論經常被用以解釋被害現象，近期的研究也逐漸將兩者加以結合，以更完整地瞭解被害者的自我控制與情境因素之關聯性(Chen et al., 2017; Holt, Wilsem, Weijer, & Leukfeldt, 2018; Holtfreter et al., 2010; Pratt et al., 2006; Schreck, 1999; Schreck et al., 2002; Schreck & Fisher, 2004; Turanovic, Reisig, & Pratt, 2015)。

自我控制理論將偏差與被害行為相互連結，認為低自我控制特質使被害者處於高風險環境或從事偏差行為。Schreck(1999)因此將自我控制理論應用於被害者之研究，認為被害者與犯罪者相同，均具有相類似之之「低自我控制特質」，這種特質使被害者參與短期、高風險的行為，且很少考慮到長期且往往是嚴重的後果，同時也不會採取必要之防護措施以避免其被害，因而增加其財產的脆弱性，從而提升其成為犯罪目標的吸引力。此外，研究更進一步指出，低自我控制早於個人日常活動，導致個人參與高風險活動，並進一步增加其被害情境風險(Schreck, 1999; Schreck et al., 2002)。

有關自我控制與網路偏差之研究，大多顯示兩者間存在顯著關係(Buzzell, Foss, & Middleton, 2006; Franklin, 2011; Higgins et al., 2006; Higgins & Makin, 2004; Higgins & Wilson, 2006)。在網路環境中，犯罪者根據目標物的可見性指標選擇潛在被害者(Clarke, 1995; Tibbetts & Gibson, 2002; Wright, Logie, & Decker, 1995)，而低自我控制者之表現，較常從事偏差行為，從而成為顯而易見標的物，增加了被害機會(Stewart et al., 2004)。

有關自我控制與與接觸偏差同儕之研究顯示，低自我控制者較可能與偏差同儕交往，這不僅增加其從事偏差行為的可能性，也會受偏差同儕的影響而增加其網路被害風險(Franklin, 2011; Gibson & Wright, 2001; Higgins et al., 2006; Jensen & Brownfield, 1986; Lauritsen, Sampson, & Laub, 1991; Longshore, Chang, Hsieh, & Messina, 2004; Stewart et al., 2004)。當低自我控制者與偏差同儕接觸時，會增加個人與潛在犯罪者接觸之機會，使個人缺乏有效的社會監控，故無法抑制被害行為之發生，並成為犯罪者鎖定的目標(Holt & Bossler, 2009; Holt et al., 2018; Pratt, Turanovic, Fox, & Wright, 2014; Schreck & Fisher, 2004; Schreck et al., 2002; Wilcox & Cullen, 2017)。

多數學者將探討個人自我控制的自我控制理論與探討情境要素之日常活動理論加以結合，從而形塑出犯罪被害之概念架構(Chen et al., 2017; Franklin et al., 2015; Pratt et al., 2014; Schreck et al., 2002)。透過該概念架構可以發現，低自我控制對個人被害具有直接和間接的影響。首先，直接影響方面，低自我控制特性者所做出具衝動性、冒險性之決定增加了個人的脆弱性，且其風險認知的程度較低，故其被害機會較高。其次，在間接影響方面，低自我控制者更有可能將自己置於高風險的環境中，並增加與潛在犯罪者接觸之機會(Leukfeldt & Yar, 2016)。Stewart 等人(2004)、Turanovic 和 Pratt(2012)指出，低自我控制特性顯著地增加個人與有動機犯罪者的接觸、從事高風險的生活方式，而偏差生活方式更中介了自我控制對重複被害的影響。Holtfreter 等人(2008)指出，自我控制能力較差者其自陳網路購物的參與頻率較高，而這可能會增加個人遭受網路詐欺的機會。Mesch 和 Dodel(2018)、Yu(2014)研究自我控制、網路日常活動及個人訊息揭露之間的關聯性發現，個人成為詐欺目標的風險程度與其自我控制及網路日常活動有關，低自我控制者更有可能在網路上揭露個人信息，從而容易成為網路詐欺被害者。

經過多數實證研究後，進一步證實日常活動確實中介了自我控制對個人被害的影響，低自我控制者較易做出衝動、冒險性的決定，而將個人置於高風險情境中，從而增加詐欺被害;即便處於低風險的情境下，低自我控制者也因缺乏防護或監控的能力而更可能成為被害者(Holtfreter et al., 2008; Ren, He, Zhao & Zhang, 2016; Schreck et al., 2002)。在網路被害方面，研究顯示，低自我控制者更可能接觸從事網路犯罪的同儕，且更容易受到偏差同儕的影響進而成為網路被害者(Franklin, 2011; Pratt et al., 2014; Schreck et al., 2006; Turanovic & Pratt, 2014)。此外，低自我控制者不僅增加了與潛在犯罪者的接觸，也較少採取有效的預防措施以避免其財產或個人資訊受到侵害(Holt & Bossler, 2009)。

綜上所述，自我控制理論與日常活動理論在被害現象的解釋上，不僅具有相容性，更具有互補性。低自我控制特性以直接或間接的方式影響個人日常活動之情境因素，而使個人容易陷入高風險的環境中，增加其被害可能性。因此，即便是預測個體被害層面的自我控制因子，亦能與解釋情境因素之日常活動因素相互結合，共同適用於不同被害行為之解釋。

第四節 性別差異與被害行為

一、性別在解釋被害現象之重要性

一直以來，犯罪學家們對於性別如何影響犯罪被害現象有著極大的研究興趣。部分學者皆認為性別是影響被害風險的一項重要預測因子(Lauritsen & Carbone-Lopez, 2011)，許多研究亦著重於探討性別如何影響被害風險、不同性別間經歷的被害類型以及其他關鍵性的性別影響因素。

有關性別與被害間關聯性之研究，傳統女性主義所提出之理論大多側重於犯罪行為之探討，但近年來以女性為解釋主體或以女性主義觀點來探究被害行為發生成因之文獻也越來越豐富。迄今為止，有關性別與被害關聯性之研究大致上可分為兩類，一類係以性別為主要觀察變項，再依據不同犯罪類型，對於不同性別間所經歷的被害行為進行研究;另一類則將性別視為控制變項，以探討不同性別間之被害差異。

儘管過去數十年的研究指出，性別是被害行為的重要預測因素，但多數性別與被害關連性之研究卻未將性別列為主要觀察變項，進行深入探討，而僅將其作為控制變項或基本人口背景變項，著重於性別如何在整體上影響被害行為，然後再具體依據不同的犯罪類型進行分析研究(Crittenden & Policastro, 2018)，也因此，對於解釋這些性別上之被害差異及不同性別間被害因素是否相同之研究也相對較少(Lauritsen & Carbone-Lopez, 2011; Zaykowski & Gunter, 2013)。雖然有關探討性別如何直接影響被害的研究相對較少，但卻可從不同犯罪被害類型之性別差異影響因素進行歸納、分析及整理。

在性別與眾多被害類型之研究中，以暴力被害現象之性別差異受到最多實證研究的測試及探討。多數學者對於性別與暴力被害差異現象進行探討(Fitzpatrick, 1999; Lauritsen & Quinet, 1995; Lauritsen & Carbone-Lopez, 2011; Ruback et al., 2011; Schreck et al., 2003; Taylor et al., 2008; Tillyer et al., 2011; Zaykowski & Guntner, 2012)，在性別與被害差異方面，研究發現，在各項犯罪之統計數據中，多數需使用較多武力或力量的親密關係暴力或性侵害犯罪被害現象，男性犯罪率均普遍大於女性。此外，在暴力被害方面，

女性遭受暴力被害的可能性較高(Craven, 1997; Felson, 2002; Kruttschnitt et al., 2004; Lauritsen & Heimer, 2008; Rand, 2008)。

有關性別與被害之部分研究發現，性別係區分被害者與犯罪者兩者間的重要因素。Schreck 等人(2008)研究暴力被害之性別差異發現，性別是將暴力被害者和犯罪者區分為不同群體的關鍵因素。Pizarro 等人(2011)研究殺人犯罪者與被害者之間的重疊現象發現，殺人被害者與犯罪者之間的關鍵性區分因素可由性別加以詮釋。

在被害者學研究範疇中，多數學者認為不應將犯罪者與被害者兩者分開考量，他們認為，被害者與犯罪者在許多人口特質上皆有相似之處，許多被害者本身經常從事犯罪或是偏差行為(Jennings, Park, Tomsich, Gover, & Akers, 2011; Lauritsen, Sampson, & Laub, 1991; Maldonado-Molina, Jennings, Tobler, & Canino, 2010; Piquero et al., 2005; Sampson & Lauritsen, 1990; Lauritsen & Laub, 2007; Schreck et al., 2002; Schreck, Stewart, & Osgood, 2008)。根據上述相關研究可以發現，男性的犯罪率高於女性，故男性從事偏差活動或犯罪的可能性也高於女性，因此，相對而言也更有可能成為各類型的被害者。

此外，當多數研究發現男性比女性具有更大的被害風險，且可能成為犯罪被害者時，通常會發現包括性別與被害之間的潛在中介變項，例如:男性具有較高風險或偏差的生活方式因素、與偏差同儕接觸之可能性較高、與父母或家庭的依附程度較低，或是自我控制能力較低等因素(Jensen & Brownfield, 1986; Kennedy & Ford, 1990; Lauritsen et al., 1991; Miethe, Stafford, & Long, 1987; Sampson & Wooldredge, 1987; Schreck et al., 2008)。因此，多數研究皆認為，決定性別與被害風險可能性之差異因素中，可能存在許多中介因子，故在評估性別對被害影響的因素中，應該要將許多中介因素納入研究之評估中，才能完整了解性別對於被害行為之影響性。

綜上所述，雖然性別是影響被害風險及解釋被害差異的重要因子，但有關性別對於被害行為之直接影響卻仍舊存在許多爭議，因此，本研究擬以性別為主要觀察變項，嘗試探究不同性別間自我控制、情境機會及被害間的相互作用關係，以更深入地了解影響性別與被害之中介因子，並對於不同性別的網路詐欺被害差異有更全面性地理解。

二、網路犯罪被害之性別差異

近年來，隨著科技日新月異及網路的普及化，網路犯罪案件也節節攀升，因網路犯罪所衍生出的被害問題亦逐漸成為犯罪學研究的重要議題。犯罪學研究者對於網路被害(Cyber-victimization，簡稱 CV)之關注，不僅係因網路犯罪成因的抽象性及複雜性，更在於網路犯罪對於網路犯罪被害者所造成的各種生理、心理上的創傷及負面影響。此外，在以往犯罪學研究的範疇中，性別皆為預測或解釋被害現象的重要變項。在網路犯罪之被害研究中，性別同樣扮演著不可或缺的詮釋角色，因此，有關網路被害之性別差異，儼然成為網路被害研究範疇中的重要議題。

在網路被害之性別差異的研究領域中，較常遇到的問題通常可以分為概念、測量、設計和分析(Sun & Fan, 2018)。由於許多網路犯罪與傳統犯罪不同，係為新型態的犯罪類型，不僅在犯罪手法上與傳統犯罪有所差異，在犯罪成因、犯罪歷程及犯罪被害造成的影響方面也有所差異。此外，在研究的過程中，不同的研究者對於網路犯罪的概念及操作性定義不僅有所差異，不同受試者對於網路犯罪的概念及認知，亦有所不同，因此，即使對於同一網路犯罪類型，不同研究之測量及分析結果亦有所差異。

在眾多性別與網路被害類型差異之研究中，以網路霸凌被害的性別差異現象受到最多實證研究及探討。Sun、Fan 和 Du(2016)、Barlett 和 Coyne(2014)及 Kowalski、Giumetti、Schroeder 和 Lattanner(2014)蒐集歷年來有關網路霸凌被害性別差異之相關文獻後進行後設分析(Meta-Analysis)，在文獻之系統性回顧後，發現性別在網絡霸凌被害中的作用並不一致。多數研究顯示，性別在統計上係網路霸凌的顯著預測因素，但對於實際遭受霸凌被害之性別則未有一致性定論，部分研究發現男性較容易成為網路霸凌之被害者(Barlett & Coyne, 2014; Forssell, 2016; Huang & Chou, 2010; Wang et al., 2009)，但部分研究則發現女性較易成為網路霸凌被害者(Dehue, Bolman, & Völlink, 2008; Kaltiala-Heino & Rimpelä; Kowalski & Limber, 2007; Mark & Ratliffe, 2011)。雖然多數研究認為性別是影響網路霸凌被害差異之重要因素，但部分研究卻指出，網路霸凌並未有性別上的顯著差異(Balakrishnan, 2015; Beckman, Hagquist & Hellström, 2012; Bonanno & Hymel, 2013;

Smith et al., 2008)，而上述相互矛盾的研究結果同時也顯示，網路霸凌被害研究領域中存在的文化差異、研究設計、研究背景等，存在相關的潛在問題(Sun & Fan, 2018)。

綜觀多數網路被害類型中，性別差異的研究結果並不一致，部分研究認為女性較易受到網路攻擊，也更容易成為網路犯罪的被害者(Ackers, 2012; Craig et al., 2009)，其中，在網路跟蹤及網路騷擾這兩個被害類型中，有研究指出，這兩個犯罪類型係基於性別因素所產生的被害差異行為，並發現女性顯著地更容易受到這兩個犯罪類型的被害行為(Duggan, 2014; Hunt, 2016; Reyns, Henson, & Fisher, 2011; Moriarty & Freiberger, 2008)。雖然有關網路被害之性別差異，多數研究顯示女性較易成為網路犯罪的被害者，但部分研究並未認同此觀點(Huang & Chou, 2010; Popovic-Citic et al., 2011; Tokunaga, 2010)。

Fan 和 Sun(2015)、Sun 和 Fan(2018)對於性別與網路被害之相關文獻進行後設分析(Meta-analysis)，在系統性回顧歷年有關性別與各類型網路犯罪被害之實證研究後，綜合歸納出性別在網路被害現象之差異與影響因素，研究發現，女性的網路被害程度較男性高。此外，研究顯示，亞洲男性比女性遭受網路被害可能性更高，但在北美和歐洲樣本中的性別差異現象則正好相反，因此，他們認為，在網路被害之性別差異中，文化是影響不同性別網路被害可能性的重要因素，同時亦認為該研究為網路被害中性別差異的跨文化模式，提供了支持，可以解釋網路被害中性別差異不一致的現象。

此外，在性別與傳統被害之解釋上有所謂「女性被害主義」，該主義以女性為解釋主體，進而加以探究女性的被害因素。在網路被害的領域中，亦有所謂「網路女權主義」(Navarro & Jasinski, 2013)，網路女權主義者對於網路場域中女性被害現象之詮釋，主要分為兩個觀點，其中一個觀點認為網路場域是女性的解放區域，因此在網路被害中，女性被害率增加係因女性主動參與了這些導致個人被害的行為;另一種觀點則認為女性因為在網路上和社會中處於不利地位，所以遭受更多網路被害(Navarro & Jasinski, 2013)。

Brown、Demaray 和 Secord(2014)指出，網路犯罪被害中性別差異研究之不一致的現象可能是由多種因素造成的，當中可能包括:不同的研究樣本、研究文化背景、測量參考時間段以及不同的抽樣方法，因此，雖然性別在網路被害研究中仍舊存在爭議性，但確仍有其研究之必要性及重要性。

三、情境、機會在被害行為性別差異之解釋

環境犯罪學將探討重點置於被害者的「情境」與「機會」要素，認為一個人從事犯罪或被害行為時所受到的影響可由這兩個要素加以闡釋。在環境犯罪學的眾多理論中，尤其以生活型態理論與日常活動理論最具代表性。生活型態理論認為，個人從事之各項職業與休閒行為和持續的時間會影響個人與有動機犯罪者接觸之程度，並認為被害者和犯罪者具有相似的個人基本特性;理論更進一步指出，男性、青年、低收入和少數民族者成為被害者和犯罪者的風險更大(Hindelang et al., 1978)。日常活動理論則將生活方式暴露理論之概念加以延伸，認為犯罪或被害行為，係在時空條件下，在缺乏有能力監控者的情況下，由合適標的物和具有動機的犯罪者聚合所產生(Cohen & Felson, 1979; Meier & Miethe, 1993)。綜合上述兩個有關情境和機會的理論觀點可得知，被害是由個人與潛在犯罪者的接觸程度、被害行為的監控程度以及標的物的吸引程度而加以決定(Cohen & Felson, 1979; Cohen et al., 1981; Meithe & Meier, 1990)。

Jensen 和 Brownfield(1986)認為，犯罪或被害皆可以被視為是一種生活方式或日常活動，而經常從事偏差的生活方式將使個人容易處於危險的情境之中。因此，Jensen 和 Brownfield(1986)進一步提出重要概念，認為藉由觀察及分析不同性別間的生活方式，可了解不同性別的被害風險差異，進而對不同犯罪類型的性別被害差異現象加以詮釋。經過研究後發現，由於男性更有可能從事偏差的生活型態、增加與犯罪者的接觸，進而增加其被害風險之可能性;換言之，相較於女性而言，男性較容易成為各種犯罪類型的被害者。此外，研究更進一步指出，男性比女性在各類型的犯罪被害可能性上高了 49%，因此，他們認為在風險因素的判斷上，也應該要注意於不同性別間的偏差生活型態。

有鑑於 Jensen 和 Brownfield(1986)提出以生活方式來檢視並分析不同性別間的被害風險差異概念，部分學者開始研究不同性別生活方式及其被害差異之關聯性。國外學者 Zaykowski 和 Gunter(2013)研究偏差生活方式的參與是否增加男性和女性重複被害風險，研究發現，從事偏差行為與個人被害風險程度成高度正相關，多數被害者本身經常從事偏差或犯罪行為。國內許淑華(2002)研究性別、機會及自我控制對少年犯罪行為之影響，

發現男性少年與女性少年在自我控制、機會及犯罪與偏差行為上均具有顯著差異存在。江旭麗(2004)研究社會控制、自我控制與少女偏差行為之關聯性，研究亦指出，在少女偏差行為方面，以生活型態與機會要素最具有解釋力，並認為由於少女經常在外與朋友遊蕩或玩樂，因而增加其發生偏差與犯罪行為的機會。

有關性別與網路生活方式之相關研究，部分研究顯示，女性在網路上所花費的時間較男性少(Allen, 2001; Bartel-Sheehan, 1999; Kehoe et al., 1998; Pastore, 2000)，且女性對於使用網路之興趣及程度顯著低於男性(Allen, 2001; Alreck & Settle, 2002; Roper, 1998)。此外，部分研究亦指出，女性在網路購物或從事各項網路活動的可能性顯著低於男性(Allen, 2001; Alreck & Settle, 2002; Briones, 1998; Bartel-Sheehan, 1999; Pastore, 2000b)，有關男性及女性網路使用及網路購物之差異分析後發現，女性對於網路購物的風險認知顯著高於男性(Bartel-Sheehan, 1999; Garbarino & Strahilevitz, 2004; Kehoe et al., 1998)，故女性較少從事網路購物行為，更有研究指出，即使女性從事網路購物行為，也比男性採取更多能規避風險的防範措施(Bajtelsmit et al., 1997; Byrnes et al., 1999; Garbarino & Strahilevitz, 2004; Hersch, 1997)，因而大大地降低其受網路詐欺被害的可能性。

雖然部分實證研究指出，女性相對於男性，具有較高的風險認知，故較不容易成為網路詐欺被害者，但Zaykowski和Gunter(2013)研究不同性別對於網路購物的風險認知、從友人推薦的購物網站及成為網路詐欺被害者的風險可能性發現，女性在網路購物方面的被害風險顯著高於男性。此外，研究指出，女性認為朋友所推薦的購物網站不僅大大降低了其對網路購物的認知風險，更會使其購買之意願大幅提升。

因此，在解釋被害風險中的性別差異時，更重要的是評估不同性別間的生活方式。多數研究指出，偏差生活方式影響著被害風險，而評估不同性別間的生活方式則有助於對性別被害差異現象之解釋。綜合上述研究可以發現，兩性不僅在網路使用行為上有所差異，在網路風險認知及採取各項防範措施等面向上亦具有差異，因此，本研究將性別納入主要觀察變項，藉以了解不同性別間的網路使用型態及個人認知差異，並對兩性之網路詐欺被害差異，做更深入且更全面性地分析與詮釋。

四、性別、低自我控制在被害行為性別差異之解釋

Gottfredson 和 Hirschi(1990)提出之一般化犯罪理論認為，低自我控制是犯罪的主要原因，一旦低自我控制特質者獲得外在的犯罪機會，便容易從事犯罪或偏差行為。此外，一般化犯罪理論認為，自我控制通常是在童年時期(約 8 至 10 歲)所形成，父母對孩子的自我控制則負有重要責任，並認為低自我控制係因兒童早期家庭或學校育兒技術不良而致，一旦孩童形成低自我控制之特性，將在其生命歷程中保持恆久、穩定性地發展且影響個人終身，難以改變。

雖然自我控制理論係解釋犯罪行為的理論，但 Schreck(1999)將自我控制理論應用於被害者，認為低自我控制係為個人被害的主要原因。Schreck(1999)指出，低自我控制因素將導致具衝動性特質者經常從事尋求立即滿足感的行為，因此，低自我控制將增加個人作為潛在標的物的吸引力和脆弱性，從而使他們容易處於高被害風險的情境之中。此外，Schreck(1999)之研究中，更進一步延伸 Gottfredson 和 Hirschi(1990)的一般化犯罪理論，認為男性和女性之間的自我控制差異可以解釋被害者中的性別差異。

由於男性和女性在社會化的過程中，受到父母或學校的教育方式存在差異，故理論學者們預測兩性之間將存在「實質性的自我控制差異」(Gottfredson & Hirschi, 1990)。一般而言，多數人認為女性較男性易受到犯罪之侵害，故對於女性的行為有較多的監控及關注。此外，在傳統性別社會化角色中，女性被要求遵從更高程度的道德規範、受到更多的監督與控制，致使其行為受到社會高度地檢視與控制，因此，當女性實行犯罪或偏差行為時，也較容易受到社會的制裁或人們的譴責，從而比男性付出更多的社會代價。綜上所述，女性因傳統價值與社會化角色之關係，不僅具有較高的社會化程度，同時也受到更多的監督與控制，因此相對於男性而言，有較高的自我控制能力。

有關男性與女性自我控制程度差異之相關研究，多數研究皆發現，男性之自我控制程度較低，因此，性別變項無論是在兩性之態度或是行為上皆能精準地評估個人的自我控制程度(Burton , Cullen , Evans, Alarid, & Dunaway, 1998; Gibson, Ward, Wright, Beaver, & Delisi, 2010; Keane, Maxim, & Teevan, 1993; LaGrange & Silverman, 1999; Tittle, Ward,

& Grasmick, 2003; Ward, Gibson, Boman, & Leite, 2010)。上述實證研究之發現亦進一步證實了 Gottfredson 和 Hirschi(1990)的理論邏輯與預測，即一般人在自我控制方面確實存在實質性的性別差異，而根據一般化犯罪理論之觀點，這些差異係由早期男性和女性之社會化經歷的變化所導致。

有鑑於自我控制理論的邏輯概念，Schreck(1999)提出了一項重要的理論概念，認為自我控制中的性別差異是女性被害風險顯著低於男性的一個重要原因。在 Schreck(1999)研究中，以自我控制、性別和家庭收入等因素來探討這些變項間如何相互影響被害行為。在其研究後發現，性別與被害程度具有顯著相關，與女性相比，男性被害的可能性增加50%，此外，研究更指出，低自我控制與更高的被害機率呈現顯著正相關。

自 Schreck(1999)提出自我控制程度係影響被害性別差異的重要因素後，自我控制就經常被認為在性別與被害之關係中發揮了重要的中介作用。多數學者將自我控制特性置於中介變項，探討性別與不同犯罪被害類型間的關聯性。

有關性別、自我控制與被害間的相關研究，國外學者 Tittle、Ward 和 Grasmick(2003)研究指出，性別確實是自我控制程度的重要預測因子，研究發現，男性的自我控制顯著低於女性，故自我控制程度之差異可解釋犯罪或被害中的性別差異。Fox、Gover 和 Kaukinen(2009)研究亦指出，女性比男性更易成為跟蹤行為的被害者，而低自我控制是女性跟蹤被害的重要預測因素。Gover、Park、Tomsich 和 Jennings(2010)研究不同性別、自我控制與暴力被害間之關聯性後發現，對於女性而言，自我控制對暴力被害的影響性顯著高於男性。國內學者許淑華(2002)、江旭麗(2004)研究亦均指出，影響男、女少年偏差行為之主要原因係低自我控制與機會要素。

綜上所述，以往對男性和女性進行調查的各項研究中，性別通常被視為是統計分析中的控制變項而非主要探討的變項，因此，有關性別、自我控制與被害間關聯性之研究相對較少。此外，雖然很少有研究直接探討性別和自我控制如何與影響被害者相互作用，但綜觀上述實證研究後仍可發現，不同性別間之自我控制程度確實有所差異，而這樣的差異亦顯現於兩性被害之行為中，這也顯示性別可能透過低自我控制的中介作用，從而影響不同類型的被害行為。

第五節 相關實證研究

一、個人基本特性

(一)性別

有關性別與詐欺被害間關聯性之相關實證研究，多數學者對於性別及詐欺被害之間關聯性加以分析後，發現兩者具有顯著關聯性。部分研究顯示，男性詐欺被害人數普遍多於女性詐欺被害人數（張耀中，2003；張隆興，2006；陳佳玉，2007；黃珮如，2010；蔡田木，2009；Holtfreter et al., 2008），但部分學者研究則未發現性別與詐欺犯罪被害間有顯著差異（王文生，2005；江志慶，2003；吳柏鏢，2005；林清榮，2006；溫怡婷，2008; Holtfreter et al., 2010; Titus & Boyle, 1995; Van & Mason, 2001）。

近年來，國內有關性別與網路詐欺被害之實證研究，大多發現網路詐欺男性被害者人數顯著多於女性被害者（王秋惠，2007；黃祥益，2006；葉雲宏，2008；蔡田木，2009; 蔡佳瑜，2010；蔡其芳，2006）。其中，蔡田木(2009)對於詐騙犯罪被害者之屬性進行研究發現，性別差異確實會影響詐騙內容及被害機會，但國內廖釗頡(2010)研究卻發現性別並非影響網路釣魚被害之因素。國外學者 Reyns(2015)對於網路犯罪被害者之分析研究，發現女性網路詐欺被害者顯著高於男性，而 Mesch 和 Dodel(2018)之研究亦發現性別具有統計上的重要意義，研究指出，女性較不太可能成為電子郵件詐欺的被害者。此外，部分國外學者針對上述兩者進行研究則未發現兩者具有顯著差異(Leukfeldt & Yar, 2016; Louderback & Antonaccio, 2017; Ngo & Paternoster, 2011; Pratt et al., 2010)。

綜觀上述國內外對於性別與網路詐欺被害影響因素之研究，顯著及不顯著之結果皆有，因此，有關性別與網路詐欺犯罪被害之關聯性值得深入探討，故本研究將性別納入主要觀察變項，以深入探討影響不同性別網路詐欺被害之影響因素。

(二)年齡

有關年齡與詐欺犯罪間關聯性之實證研究，大多發現兩者間具有關聯性。國內學者對於詐欺被害者之分析研究發現，詐欺被害者大多介於 20 至 29 歲之間（江志慶，2003；張隆興，2005；溫怡婷，2008；蔡田木，2009）。王文生(2005)對於新興詐欺犯罪被害

者進行研究發現，被害者年齡以 20 至 39 歲最多。吳柏鏢(2005)對於電話詐欺被害者特性進行研究發現，被害者年齡以 19 至 55 歲之間最多，未成年和 60 歲以上的老年人遭受詐欺被害的機會較小。陳佳玉(2007)通訊金融詐欺犯罪被害特性及歷程之分析研究發現，年齡在 30 歲以下者有較高的被害比率。黃珮如(2010)研究發現，電話詐欺被害者年齡以 31 歲以上至 40 歲以下最多。蔡田木(2009)對於年齡與詐騙手法之關聯性分析發現，年齡在通訊詐欺手法被害上有顯著差異，詐欺被害者年齡以 19 歲以下佔最高比例。

國外學者 Titus 和 Boyle(1995)對於詐欺犯罪之個人被害特性進行研究發現，年齡與詐欺被害經驗有顯著關聯性，年紀輕者較易遭受詐欺被害。學者 Van 和 Mason (2001)對於消費詐欺被害者之弱點因素和報案行為進行調查，亦發現兩者間具有顯著關聯性，在詐欺被害者樣本中，以 18-24 歲之被害機率佔 77%最高。此外，部分研究對於年齡與詐欺犯罪被害進行分析，發現兩者並無顯著關聯（林清榮，2006；張隆興，2006; Holtfreter, Reisig, & Blomberg, 2006; Lee & Soberon-Ferrer, 1997）。

國內有關年齡及網路詐欺被害之實證研究，大多顯示兩者之間具有關聯性（王秋惠，2006；黃祥益，2006；廖釗頡，2010；葉雲宏，2008；蔡佳瑜，2010；蔡其芳，2006），但對於實際被害年齡之分布卻未有一致性定論。王秋惠(2006)研究發現，網路詐欺被害者以 29 歲以下者居多。黃祥益(2006)對於台灣地區少年網路犯罪與被害特性之研究發現，19-50 歲之間普遍以詐欺和妨害電腦使用被害者最多。葉雲宏(2008)網路詐欺被害影響因素之研究發現，網路詐欺犯罪被害者在年齡分布上，無被害經驗較有被害經驗者年紀年長。蔡佳瑜(2010)少年網路詐欺被害歷程之研究發現，網路詐欺犯罪被害者年齡以 16、17 歲者最多。蔡其芳(2006)研究發現，被害者以 21-25 歲所佔的被害比例最高。

國外學者對於上述兩個變項之研究則較不一致，Leukfeldt 和 Yar(2016)研究發現，年紀較輕的網路使用者，遭受網路詐欺的機率愈大。Ross 和 Smith(2011)研究指出，年齡是唯一持續被發現在網路詐欺被害方面具有一定預測價值之人口統計學變項，研究發現，年齡介於 18 至 24 歲、35 至 44 歲之間，最可能成為網路詐欺被害者。Whitty(2019)研究網路詐欺被害者之特徵發現，無論是單次被害或重複被害者，年齡均較未被害者高。Mesch 和 Dodel(2018)研究低自我控制、個人訊息揭露與網路詐欺被害之間的關聯性，

研究指出，年齡與個人訊息揭露呈現負相關，但卻與網路詐欺目標風險之間存在正相關，研究顯示，受訪者年齡越大，收到的詐欺電子郵件數量就越多，故成為網路詐欺被害者的機會也越高，部分學者研究亦發現年齡與是否被害間具有顯著關聯性(Jorna, 2016; Pratt et al., 2010; Reyns, 2013; Reyns, 2015)，但卻有研究卻發現兩者間並不具顯著關聯性(Leukfeldt & Yar, 2016; Louderback & Antonaccio, 2017; Ngo & Paternoster, 2011)。

(三)職業

綜觀國內外有關職業與詐欺被害間之實證研究，尚未有一致性定論。國內張隆興(2006)以 2005 年 1 至 6 月警方受理詐欺犯罪被害報案之官方統計資料，對於詐欺重複被害者進行研究後發現，詐欺重複被害者之職業分布以無業、工礦、商或金融佔多數。陳佳玉(2007)以 2007 年 165 反詐騙諮詢專線報案民眾為研究對象，進行通訊金融詐欺犯罪被害特性及歷程之分析發現，職業為學生者有較高的被害比率。然而，國外學者 Titus 和 Boyle(1995)、Van 和 Mason(2001)之相關研究卻均未發現兩者有顯著差異。

有關職業與網路詐欺被害間關聯性之實證研究則較為一致，國內王秋惠(2007)對於網路詐欺被害特性及被害歷程進行研究，在次級資料分析後發現，學生或無職業之樣本中，場所被害之比率明顯高於就業者樣本。黃祥益(2006)台灣地區少年網路犯罪與被害特性之研究發現，在被害者職業部分，以體力工、非技術工及服務業為最大宗之類型。廖釗頡(2010)研究網路釣魚被害之成因發現，網路釣魚被害者之職業分布以學生居多。蔡其芳(2006)以線上遊戲竊盜被害特徵進行研究發現，被害者多以學生、工、無業最多。蔡佳瑜(2010)少年網路詐欺被害研究發現，網路詐欺被害者之職業大多以學生、工人及無業者居多。

國外學者 Kigerl(2012)選取 132 個不同國家的代表性樣本加以分析後發現，失業率較高的國家有較多的網路犯罪行為。Leukfeldt 和 Yar(2016)對於六項不同網路犯罪類型進行被害調查後發現，其中，在網路消費者詐欺被害類型中，研究指出，無業者之網路詐欺被害風險較高。但部分國外學者對於上述兩個變項之研究則發現，職業與網路詐欺被害間並無顯著關聯性(Ngo & Paternoster, 2011; Reyns, 2013)。

(四)收入

有關收入與詐欺被害間關聯性之國內外實證研究，尚未有一致性定論。國內學者周愫嫻(2002)對於倒會詐欺被害者進行研究發現，被害者之收入大多皆在 5 萬元以下。陳佳玉(2007)通訊金融詐欺犯罪被害特性及歷程之之研究則發現,收入在 2 萬元以下者,容易透過行動電話接收詐騙訊息進而成為詐欺被害者。但國外學者 Titus 和 Boyle(1995)透過電話調查的方式，對於詐欺案件的被害者進行研究，則發現兩者並無顯著差異，而學者 Van 和 Mason(2001)調查消費詐欺被害行為,於各項人口特性上（包括年齡、性別、種族、教育程度和家庭收入）進行比較分析後，亦未發現兩者有顯著差異。

綜觀國內外學者對於收入與網路詐欺被害間關聯性之實證研究並未有一致性定論。廖釗頡(2010)研究網路釣魚被害類型及其成因發現，網路釣魚被害者的特徵為收入較低。國外 Reisig 等人(2009)研究發現，具有較高社會經濟地位者，其網路被害之風險較低，Ross 和 Smith(2011)研究指出，個人經歷的詐欺被害類型與收入程度間具有統計上之顯著關係，研究顯示，收入低於 20,000 美元者更有可能成為網路交易詐欺的被害者，而部分研究亦顯示兩者具有顯著差異,並顯示網路詐欺被害者之收入以五萬元以下佔多數（蔡其芳，2006 ; Kigerl, 2012; Pratt et al., 2010）。此外，Leukfeldt 和 Yar(2016)之研究則顯示個人的財務及收入狀況與其是否成為網路詐欺被害者並無顯著關聯性,研究指出，無論個人收入高低和擁有多少金融資產，其成為網路詐欺被害者的機會均相等。

(五)教育程度

綜觀國內有關教育程度與詐欺被害關聯性之實證研究,大多發現兩者具有關聯性。多數研究顯示，詐欺被害者之教育程度多以中等教育程度、高中以上至大學／專科以下佔多數（江志慶，2003； 吳柏鏢，2005； 張隆興，2006； 黃珮如，2010），但陳佳玉(2007)對於通訊金融詐欺犯罪被害特性之研究則發現,詐欺被害者之教育程度多為研究所以上。國外 Titus 和 Boyle(1995)對於詐欺被害者進行研究發現，教育與詐欺經驗有顯著差異，教育程度的極端表現(如沒有受過教育或受到研究所以上教育者)均較容易受到詐騙。Van 和 Mason (2001)以詐欺被害者之弱點因素進行調查，並對於各項人口特性進行分析後，亦發現教育程度對詐欺犯罪被害具有顯著差異，研究顯示，教育程度及社會化程度

較高者較易成為消費詐欺被害者。此外，林清榮(2006)以信用貸款詐欺為例，對於新興詐欺犯罪被害歷程進行研究發現，被害者教育程度之高低與詐欺被害間並無直接關係。

有關教育程度與網路詐欺被害間關聯性之研究，大多顯示兩者具有顯著關聯性，但對於實際被害之教育程度則尚未有一致性定論。部分研究顯示，網路詐欺被害者之教育程度多為中等教育程度、高中至大學（王秋惠，2007；蔡佳瑜，2010；蔡其芳，2006）。黃祥益(2006)少年網路被害特性之研究發現，學歷愈高者，其網路詐欺被害之比例愈高。廖釗頡(2010)網路釣魚被害成因之研究亦發現，網路釣魚被害者其教育程度相對較低。葉雲宏(2008)針對網路詐欺被害影響因素進行研究，發現未被害者有較高的教育程度。國外 Leukfeldt 和 Yar(2016)對於不同網路犯罪類型進行調查後發現，在網路消費者詐欺的犯罪被害類型中，教育程度之高低顯著影響個人是否成為被害者，研究更進一步指出，受教育程度較低者其受網路詐欺被害的風險較高。Pratt 等人(2010)網路詐欺被害之研究發現，受過更多教育者更可能成為網路詐欺之被害目標，研究更發現，網路詐欺被害者之教育程度大多介於高中（職）至大學間。雖然多數研究指出兩者間具有顯著關聯，但 Mesch 和 Dodel(2018)研究卻發現教育程度與網路詐欺被害可能性間並未有顯著差異。

(六)婚姻狀況

國內外有關婚姻狀況與詐欺被害之相關實證研究具有高度歧異性，國內研究大多顯示兩者間具有顯著差異（周愫嫻，2002；張隆興，2006；陳佳玉，2007；黃珮如，2010），且未婚者、單身者較容易成為詐欺之被害者。國外學者對於上述兩個變項之研究，則大多未發現兩者間有顯著差異(Holtfreter, 2008; Titus & Boyle, 1995; Van & Mason, 2001)。

有關婚姻狀況與網路詐欺被害之研究，國內葉雲宏(2008)、蔡其芳(2006)研究發現，網路詐欺被害者之婚姻狀況多以未婚、單身者居多。劉品秀(2007)研究發現，網路交友詐欺被害者多以年輕未婚的女性佔多數。此外，綜觀國外多數研究，雖大多未發現兩者間具有顯著差異(Ngo & Paternoster, 2011; Pratt et al., 2010; Reyns, 2013; Reyns, 2015)，但 Ross 和 Smith (2011)、Shadel、Pak 和 Sauer(2014)之研究卻發現，婚姻與網路詐欺被害存在顯著相關性，曾經歷負面生活事件者，其網路詐欺被害比例較高。

二、低自我控制特性

Gottfredson 和 Hirschi(1990)認為，缺乏自我控制者傾向於做出具衝動性的決定並參與負面生活有關之風險行為。因此，他們更有可能採取風險性行動，只需很少的努力或投資，並致力於獲得立即的刺激或報酬。Schreck(1999)將自我控制理論擴展至被害者，認為低自我控制是預測被害的有力因素，並認為被害者和犯罪者具有相類似的人格特質，他們皆有參與短期、高風險行為之傾向，這種行為會產生立即滿足感且很少考慮到長期、嚴重之行為後果。多數學者亦逐漸將自我控制理論擴展到不同形式被害類型之研究，如暴力犯罪(Piquero et al., 2005; Schreck, 1999; Schreck et al., 2002; Schreck, Fisher, & Miller, 2006; Stewart et al., 2004)、財產犯罪(Schreck, 1999; Schreck et al., 2006; Smith, 2004)以及詐欺犯罪(Benson & Moore, 1992; Holtfreter et al., 2008; Smith, 2004; Titus, 2001)等類型，而多數研究後發現，低自我控制程度與個人是否成為被害者具有顯著關聯性。

許多實證研究在各種犯罪和被害情境中，以低自我控制特性解釋犯罪被害情形，而多數研究亦發現，低自我控制特性會顯著增加犯罪被害風險(Bossler & Holt, 2009; Holt & Bossler, 2009; Holtfreter et al., 2008; Marenin & Reisig, 1995; Peker, 2017; Piquero et al., 2005; Schreck, 1999; Schreck et al., 2002; Stewart et al., 2004)。此外，在各類型犯罪被害行為中，低自我控制者不僅具有更高的被害風險，同時亦增加了其可能從事犯罪的機會(Fagan & Mazerolle, 1992; Jensen & Brownfield, 1986; Lauritsen, Sampson, & Laub, 1991; Schreck et al., 2002)。Holtfreter 等人(2008)研究更指出，低自我控制是有效解釋詐欺犯罪環境中犯罪者和被害者暴露兩者重疊(Overlapping)的關鍵因素。

Schreck(1999)在對 Gottfredson 和 Hirschi(1990)一般化犯罪理論的延伸概念中指出，男性和女性之間的自我控制差異可以解釋被害者中的性別差異。國內鄭文鐸(2018)對於男性與女性電信詐欺犯罪者自我控制與同理心進行研究後發現，在性別差異上，男性詐欺犯罪者不論在自我控制或同理心程度，皆顯著低於女性犯罪者，此外，研究更進一步指出，在詐欺犯罪者之低自我控制與同理心程度的預測上，性別為最主要之影響因子。多數國外對於自我控制是否存在性別差異之研究亦發現，大多數男性具低自我控制特性，

並從事較多犯罪行為(Elliott, 1994; Nagel & Hagan, 1983; Perrone, Sullivan, & Margaryan, 2004; Steffensmeier, Allan, & Streifel, 1989; Steffensmeier & Allan, 2000; Unnever, Cullen, & Pratt, 2003)，此外，部分國外實證亦指出，男性和女性之自我控制程度因性別不同而有所差異(Burton, Cullen, Evans, Alarid, & Gregory, 1998; Keane, Paul, & James, 1993; LaGrange & Silverman, 1999)。

近年來，隨著網路犯罪案件漸增，有關自我控制理論在解釋網路犯罪被害之研究亦越來越廣泛(Bossler & Holt, 2009; Buzzell et al., 2006; Higgins & Makin, 2004; Higgins, 2005; Higgins et al., 2006; Higgins, Wolfe, & Marcum, 2008; Holt & Bossler, 2009; Holt & Bossler, 2013)，而低自我控制特性對於網路詐欺犯罪被害之研究也越來越多元(王秋惠，2007；葉雲宏，2008；Ashalan, 2006; Bossler & Holt, 2010; Choi, 2008; Holt & Bossler, 2010; Holtfreter et al., 2008; Vazsonyi, Machackova, Sevcikova, Smahel, & Cerna, 2012)。以下就本研究中有關自我控制要素中重要變項之相關實證研究分述如下:

(一)衝動性(Impulsivity)

國內學者范國勇、張平吾、蔡田木、劉擇昌(2004)對於 ATM 轉帳詐欺犯罪進行之質性研究中發現，詐欺被害者之認知多為「心存貪念」、「防備心低」、「社會經驗不足」、「執迷不悟」及「身不由己」。葉雲宏(2008)對於網路詐欺被害影響因素之研究指出，在被害原因部分，以疏忽大意最多(32.7%)，其次為自己太笨(25.5%)，再次之則是過於相信別人(21.8%)，最後則為貪小便宜(12.7%)，多數人認為網路詐欺被害是可以避免的。

國外學者 Baumeister(2002)、Romal 和 Kaplan(1995)之研究發現，未能有效地進行自我控制係為衝動性購物的重要原因，而衝動、不謹慎的消費決策亦根源於低自我控制。Holtfreter 等人(2008)研究發現，在個人網路購物決策歷程中，衝動性的網路購物消費者較不在乎營業銷售人員的擔保和產品的聲譽。Reisig 等人(2009)研究發現，即使受訪者認為信用卡竊盜的風險相對較高，具衝動性的消費者仍不會改變他們的網路購物行為。Reisig 等人(2010)研究指出，衝動性的非理性消費者比理性消費者從事網路購物的頻率高出 45%，這也使他們更容易成為網路詐欺犯罪者的合適目標。Titus 和 Gover(2001)就

詐欺被害者之心理特質進行研究發現，詐欺被害者多為貪心、衝動、輕信他人及粗心。Wilsem(2001)對於荷蘭 6,210 名網路詐欺被害者進行研究發現，低自我控制者面對網路詐欺之回應與一般人不同，低自我控制者的回應方式使其具有較高之網路詐欺被害風險。Whitty(2019)研究發現，網路詐欺被害者在衝動性得分上較未被害者高，這也使其網路詐欺被害機率增加。此外，有關低自我控制與個人衝動性消費之研究發現，低自我控制者較易從事衝動性的消費活動，而較少從事需要長遠規劃、投資及儲蓄的穩定金融行為(Baumeister, 2002; Romal & Kaplan, 1995; Tangney, Baumeister, & Boone, 2004)。

綜上所述，國內外有關個人衝動性與是否被害之研究發現，具衝動性特質者，較難抵抗某些誘惑，且往往在未充分考慮後果的情況下從事衝動性的行為，增加個人暴露於犯罪情境或機會之可能，進而增加其被害風險（王秋惠，2007；溫怡婷，2008；葉雲宏，2008 ; Bossler & Holt, 2009; Forde & Kennedy, 1997; Holtfreter et al., 2008; Holt & Bossler, 2009; Norvilitis et al., 2006; Reisig et al., 2009; Schreck,1999; Schreck et al., 2002）。

（二）冒險性(Risk Seeking)

Schreck(1999)指出，低自我控制者著重於當下、立即的享樂，並經常從事具冒險性的行為、尋求快速致富的機會，因此經常被視為是尋求刺激、冒險者，而低自我控制者為尋求快速致富的機會，因此容易受到詐欺者計劃的影響，並經常從事具冒險性的投資，這種行為不僅降低了個人財產的安全性，也同時增加其被害的可能性。

Holtfreter 等人(2008)研究指出，低自我控制與消費者的詐欺被害有關，低自我控制者從事具風險性的投資行為反映了他們對於立即滿足的渴望，並使自己更可能面臨詐欺被害的風險。Holtfreter 等人(2010)研究發現，詐欺被害行為與低自我控制程度顯著相關，由於個人評估風險嚴重程度和脆弱性的能力有限，低自我控制者經常參與冒險性的活動。Wilsem(2013)對於不同網路犯罪被害類型進行研究後發現，低自我控制是網路犯罪被害的風險預測因素，而低自我控制者往往成為網路詐欺被害者之原因有二，首先，低自我控制導致不同類型的網路犯罪被害者經歷較高程度的網路被害風險。其次，由於低自我控制者對網路詐欺的風險評估能力有限，故經常成為網路詐欺的主要目標。

Chen 等人(2017)以低自我控制之指標（風險投資意願）評估網路使用者從事高風險投資之可能性後發現，風險投資意願與個人是否成為網路詐欺被害者間具有顯著關聯性，藉由評估個人是否經常從事高風險的投資行為，可預測未來是否成為網路詐欺被害者，研究亦指出，風險投資者重視潛在的經濟利潤，但卻很少評估因風險投資所造成的損失，因此，當個人面對各項風險投資計畫時，支持風險投資者更容易成為網路詐欺被害者。Reisig 等人(2009)對於網路消費者信用卡竊盜被害風險評估，以及個人風險認知是否與網路生活方式有關之研究發現，經濟衝動的非理性消費者通常於比理性消費者更頻繁地進行網路購物，且未採取有效的風險降低策略，而風險較低的消費者在網路上所花費的時間明顯較少、從網路上購買物品的次數亦顯著降低。Titus 和 Gover(2001)詐欺被害者之心理特質研究發現，詐欺被害者心理特質為粗心、易遭受恐嚇、且經常從事冒險行為。Van 和 Mason (2001)對於消費者詐欺被害脆弱性進行調查發現，年輕人比老年人更容易受到消費型詐欺被害，係因年輕人比老年人有較多的風險性經濟投資行為，研究亦發現，大多數詐欺被害者願意承擔較高的財務風險。

國內王秋惠(2006)網路詐欺被害特性與被害歷程之研究發現，網路詐欺被害者大多認為自己不會被害、過於自信，且因自身疏忽、貪念而過於相信別人，這些屬於被害的原因，也就是被害者本身的弱點因素。溫怡婷(2008)詐欺犯罪重複被害特性之質性訪談研究中發現，詐欺被害者大多具有較多的風險性理財行為，且多數詐欺被害者中，具有剛愎自用、堅信不疑、缺乏警覺、疏忽大意；心急如焚、當局者迷等特質。

綜合上述國內外實證研究可知，低自我控制者為追求立即享樂與個人滿足，而傾向從事具有高風險的投資行為，這些行為不僅增加個人暴露於風險的機會，亦增加其暴露於有動機犯罪者之程度，從而增加其網路詐欺被害之可能性，因此，網路使用者從事具冒險性金融投資行為的程度，通常被視為低自我控制程度的重要預測指標（王秋惠，2006；溫怡婷，2008; Bossler & Holt, 2009; Chen et al., 2017; Higgins & Makin, 2004; Higgins et al., 2006; Holtfreter et al., 2009; Holtfreter et al., 2010; Reisig et al., 2009; Schreck et al., 2002; Taylor, Davis, & Jillapalli, 2009; Titus & Gover, 2001; Van & Mason, 2001）。

(三)投機性(Speculative)

Gottfredson 和 Hirschi(1990)指出，低自我控制者通常花費很少的時間或精力，期望在最短的時間或花費最少力氣的情況下追求最大程度的享樂。Baumeister(2002)指出，低自我控制者較少從事長期穩定的投資規劃及儲蓄的行為，並經常尋求立即獲利、付出很少金融投資及努力的快速致富機會，因此容易從事高風險的金融行為。多數研究顯示，低自我控制者希望付出很少的努力或花費很小的投資就可得到大量獲利的機會，並經常具有以小搏大的賭徒心理和充滿風險的理財觀念，這些原因使其更容易成為詐欺犯罪之被害者(Baumeister, 2002; Tangney et al., 2004; Trahan, Marquart, & Mullings, 2005)。

范國勇等人(2004)研究發現，詐欺被害者遭詐騙時之認知多為心存貪念、防備心低、社會經驗不足及執迷不悟。林清榮(2006)研究亦發現，詐欺犯罪者無所不用其極地散發誘人的信息，以吸引民眾心動，經訪談多位被害者後發現，平時未接觸社會資訊、沒有經驗或缺乏警覺、較貪心者較容易成為詐欺被害者。許清事(2006)通訊金融詐欺之研究發現，個人在通訊金融詐欺被害歷程中之心理多為：貪念、巧合、認知不足、欠缺查證。溫怡婷(2008)詐欺犯罪之重複被害者特性研究中發現，多數詐欺被害者存有僥倖心態、且具有短視近利，使其經常從事高投機性的風險投資行為。葉雲宏(2008)網路詐欺被害影響因素研究指出，被害原因包括:疏忽大意、自己太笨、過於相信別人及貪小便宜。鄭佳虹(2006)網路拍賣詐欺實證研究指出，受訪者一致認為，以網路拍賣做為購物途徑，除了係因網路具有方便及迅速性外，商品較市價為低。國外 Fischer、Lea 和 Evans(2013)研究發現，詐欺被害者對於加害者所提供之高投機性訊息通常深信不疑。

綜上所述，低自我控制者經常從事投機性的金融投資行為，這種具投機性的行為將大大地增加消費者詐欺被害的機率，而多數研究均指出，網路詐欺被害者之被害原因多為貪小便宜、投機心理作祟，透過加害者在詐欺的商品上所顯示較低價格之訊息來吸引被害者，使被害者認為該商品明顯低於市場價格，而在未能詳細考慮風險、互不相識、未有正式管道或合法方式的情況之下貿然進行購買或投資行為，從而遭受詐騙(許清事，2006；溫怡婷，2008；蔡佳瑜，2010；鄭佳虹，2006)。

三、網路生活型態

Jensen 和 Brownfield(1986)認為，犯罪可以被視為是一種生活方式或日常活動，而參與偏差的生活方式進一步使這些人處於危險之中。自 1979 年 Cohen 和 Felson 提出日常活動理論後，該理論就常用於解釋犯罪或偏差行為(Bachman & Johnston, 1996; Miller, 2013; Osgood, Wilson, O'Malley, 1996)、犯罪率的變化(Bennett, 1991; Messner & Blau, 1987; Roncek & Maier, 1991)、不同類型的犯罪被害行為及被害者日常生活模式的變化(Farrell & Pease, 2004; Fisher, Cullen, & Turner, 2002; Jensen & Brownfield,1986; Maxfield, 1987; Miethe & Meier, 1990; Reyns, 2013; Tseloni & Wittebrood, 2002)，而多數實證研究均顯示日常活動理論的多重功能性及被害行為之高度解釋力，故逐漸發展成為犯罪被害者學領域中的重要理論，以下對於各實證研究內涵分述如下:

有關個人特性與網路生活型態之網路詐欺被害研究，在性別方面，多數研究顯示，男性比女性更可能會從事網路行為及使用網路交易(Chang & Samuel, 2004; Farag et al., 2006; Korgaonkar & Wolin, 2002; Soopramanien & Robertson, 2007)。教育程度及收入方面，研究顯示，經常從事網路購物或網路交易者，往往具有較高的教育程度及收入水平(Farag et al., 2006; Ratchford, Talukadar, & Lee, 2001; Soopramanien & Robertson, 2007; Stranahan & Kosiel, 2007; Swinyard & Smith, 2003)。Korgaonkar 和 Wolin(1999)研究發現，高收入和受過良好教育的網路使用者其上網時間較長，而 Van Wilsem(2013)研究亦指出，教育程度與網路使用呈正相關，經常使用社交網站和網路論壇會提高人們對潛在犯罪者的可見度及可接觸性，研究亦顯示，詐欺犯罪者可以根據網路公佈的個人資料訊息選擇目標，並制定適當的策略來誘導特定的個體。

綜上所述，有關個人特性與網路生活型態之相關實證研究顯示，男性、高收入者和受過良好教育的網路使用者，在網路上花費的時間通常較長、從事網路購物或網路交易的頻率亦較高(Fallows, 2005; Farag et al., 2006; Korgaonkar & Wolin, 1999; Nielsen, 2008; Ratchford et al., 2001; Van, 2013)。

（一）網路使用特性

國內有關網路使用頻率、接觸時間與網路詐欺被害之研究結論並未一致，王秋惠(2007)研究發現，大多數網路詐欺被害者的上網時間並不長，從事的網路活動較為單一。吳嫦娥、蔡麗滿(2004)以性別、年齡、教育程度、上網期間、每週上網平均時數為基本特性變項，調查台北市少年網路被害發現，網路被害者以上網五年以上有較多被害情形，每週上網平均時數，以 3 至 9 小時佔最多數。廖釗頡(2010)研究發現，網路釣魚被害者每週上網日數較長。葉雲宏(2008)研究發現，具有網路詐欺被害經驗者其每周上網次數、每次上網時數均顯著高於未被害者，在接觸網路時間方面，具有網路詐欺被害經驗者其接觸網路時間大多介於 5 年以上未滿 10 年。鄭英瑋(2004)青少年網路使用行為之生活適應及偏差行為研究發現，青少年每日在網咖的上網時間若超過 7 個小時，更容易出現網路偏差行為。賴克宗(2007)網路犯罪被害研究發現，以上網為休閒活動、接觸網路的時間愈久、上網次數愈頻繁及在深夜時段上網者，較容易遭受網路犯罪被害。

國外有關上網時間、頻率與網路詐欺被害之研究結果並不一致，部分研究發現，當個人在網路上花費的時間越長、越頻繁地使用社交網站和從事網路購物行為，越會增加人們與潛在犯罪者接觸的機會，進而增加個人成為網路詐欺被害者之可能性(Pratt el al., 2010; Ross & Smith, 2011; Wilsem, 2011a, 2011b)，但 Bossler 和 Holt(2009)研究則顯示，個人電腦使用時間之長短，對於個人是否成為網路犯罪被害者並無顯著關聯性。

有關網路使用地點與網路詐欺被害之研究，國內多數研究顯示，網路詐欺被害者之網路使用場所與個人被害具有顯著關聯性。部分研究顯示，網路詐欺被害者其被害時的網路使用地點係在個人的私人住宅（王秋惠，2007；蔡佳瑜，2010）。葉雲宏(2008)研究發現，網路詐欺被害與使用網路的場所息息相關，但研究卻顯示，發生被害最多的地點是「網咖」，其次為「住宅」，並指出網路詐欺被害類型與被害場所間具有時空的密集性。國外學者 Titus 和 Boyle(1995)對於個人詐欺消費被害之研究則發現，被害地點大多是在被害者工作場所、鄰里、加害人的家中、工作場所而非被害者的家中。

（二）網路休閒與職業活動

有關個人網路休閒與職業活動及網路詐欺被害之研究，國內王秋惠(2007)研究指出，網路生活正如一個充滿犯罪機會的情境，在此情境中，加害者與被害者之間的互動顯著影響個人的被害機會。廖釗頡(2010)研究指出，在網路釣魚被害者之上網行為中，大多以玩線上遊戲及部落格為主。蔡佳瑜(2010)對於少年網路詐欺被害者進行研究後發現，被害者之網路生活型態以遊樂型休閒活動為主，且網路詐欺被害青少年大多與同儕友伴相同，會頻繁地使用即時通訊軟體或社群網站以進行互動聯繫。蔡其芳(2006)研究發現，網路被害者的生活型態大多為獨居、較少與家人互動、日常休閒娛樂有限且生活單調、對網路使用具有高度依賴，並據以作為人際關係聯繫的重要管道，且對於線上遊戲投入相當多的時間和精力。葉雲宏(2008)研究發現，有網路詐欺被害經驗者擁有較高的網路使用滿足感、較多的網路被害經驗與較嚴重的網路依賴程度，研究亦指出，具網路詐欺被害經驗者經常以網路從事各項休閒娛樂活動，並作為通訊的管道。

一般而言，評估個人暴露於網路中具犯罪傾向者的潛在風險通常是透過「個人接觸網路時間」、「每周上網次數」及「每次上網時間」等變項來測量。多數研究均顯示，當個人接觸網路時間越早、上網次數越頻繁、上網時間越長，就有更高的機會暴露於潛在網路犯罪者的風險中(Bossler & Holt, 2007; Coupe & Blake, 2006; Holt & Bossler, 2009; Holtfreter et al., 2008; Hutchings & Hayes, 2009; Whitty, 2019)。

Bossler 等人(2012)研究發現，網路上網時間與網路被害間不具關聯性，但「使用社交網站的時間」卻能預測網路被害。Holt 和 Graves(2007)之研究發現，網路詐欺加害者通常以電子郵件方式寄送至當事人信箱，而被害者大多在接收電子郵件後，將個人訊息回復給加害者或是與加害人進行訊息互動後進而被害。Holtfreter 等人(2008)以日常活動理論及自我控制理論研究詐欺被害與個人生活型態之關聯性發現，個人在網路上的遠程購物行為將會影響消費者成為詐欺目標的暴露程度，進而影響其成為詐欺被害者之風險。Kerstens 和 Jansen(2016)研究發現，花費較多時間上網者，將提升其網路被害的可能性。Pratt 等人(2010)研究個人網路日常活動及網路詐欺被害之關聯性後發現，經常從事網路購物者其成為網路詐欺目標的可能性較未從事網路購物者提高 377%。

雖然多數研究顯示，使用網路的時間、頻率與個人是否成為網路犯罪被害者有關，但國外學者 Bossler 和 Holt(2009)、Holt 和 Bossler(2009)之研究則顯示，個人電腦使用時間之長短與個人是否成為網路被害者並無顯著關聯性，而 Leukfeldt(2014)以日常活動理論要素對於個人和財務特徵、網路活動和網路可接觸性進行研究發現，上述這些因素似乎不會增加個人被害風險。Reyns 等人(2011)將日常活動理論應用於網路被害者追蹤，研究指出，個人在網路上的暴露程度並未在追蹤行為類型中產生顯著影響。

（三）網路風險休閒與職業活動

有關網路風險休閒與職業活動及網路詐欺被害之關聯性研究發現，日常網路活動是網路被害的正向預測因素，而高風險的網路休閒活動更進一步增加了個人遭受網路犯罪被害之可能性。部分研究亦發現，個人在網路上所花費的時間越長、更頻繁地使用網路社群媒體或網路論壇，都會增加個人揭露其私人訊息之機會，而這也使潛在的網路詐欺犯罪者可以根據網路上獲得的訊息來選擇合適的目標(Pratt et al., 2010; Wilsem, 2013)。Leukfeldt 和 Yar(2016)對於不同類型之網路被害行為進行研究發現，在網路消費者詐欺之被害類型中，網路購物行為是一種增加個人成為網路詐欺被害者的網路風險休閒活動，而個人增加上網和瀏覽網頁的時間亦增加其網路詐欺被害的機率。Mesch 和 Dodel(2018)研究指出，最有可能成為網路詐欺被害者的族群是經常在網路日常活動中揭露個人訊息並缺乏自我控制能力的老年男性。Reisig 等人(2009)研究指出，減少個人上網時間及其網路購物頻率就能有效降低個人網路詐欺被害之可能性。Whitty(2019)對於網路詐欺之重複被害者進行研究後發現，網路詐欺被害者之網路風險日常活動較未被害者更頻繁。

多數研究均顯示，網路風險生活型態與網路詐欺被害之間具有顯著相關，網路詐欺犯罪者依靠各種網路途徑來尋找及鎖定潛在的被害者，而經常在網路上散播個人訊息、從事風險網路活動或瀏覽高風險網站者，皆有可能成為犯罪者鎖定之網路詐欺被害標的(Aghekyan- Simonian et al., 2012; Baker & Faulkner, 2003; Chen & Beaudoin, 2016; Franklin et al., 2012; Holt & Turner, 2012; Hover, Coffey, & Hobbs, 2003; Marcum et al., 2010; Pratt et al., 2010; Shover, Coffey, & Sanders, 2004; Yazdanifard & Mercy, 2011)。

國外學者 Choi(2008)、Choi(2017)及 Marcum(2008)研究發現，經常從事風險性網路休閒活動（例如，經常瀏覽未知網站或下載免費遊戲或音樂）者，較容易成為網路犯罪被害者，而多數研究亦發現，經常下載文件、軟體或打開未知來源的文件，可能會增加個人暴露於具有動機犯罪者之可能性(Bossler & Holt, 2009; Choi, 2008; Holt & Copes, 2010; Szor, 2005; Wolfe, Higgins, & Marcum, 2007)。Chen 等人(2017)研究發現，高風險網路日常活動（網路購物、下載文件及開啟不明來源的電子郵件）與個人網路詐欺被害可能性呈正相關，並認為個人的風險網路生活型態可有效預測其網路詐欺被害的可能性。Van 和 Mason(2001)對於消費者詐欺被害脆弱性之研究發現，年輕人比老年人更容易受到消費型詐騙被害，因為年輕人比老年人有較多的風險社交活動，且年輕人比老年人有更多風險性的經濟投資行為。

此外，透過實證研究之量化資料分析與質化訪談內容後發現，人們所從事的各項網路風險日常活動（例如:花費更多時間從事高風險的網路行為、從事更多的網路交易行為、經常使用即時通訊軟體或聊天室、在網路上從事越多購物行為等）會使個人更有可能成為各類型的網路犯罪被害者，而網路風險暴露程度亦與個人被害程度成正相關(Chen et al., 2017; Choi, 2008; Louderback & Antonaccio, 2017; Marcum, 2008; Marcum et al., 2010; Mesch & Dodel, 2018; Mustaine & Tewksbury, 1998; Pratt et al., 2010; Stewart et al., 2004; Tewksbury & Mustaine, 2000; Whitty, 2019)。

四、被害情境與機會

Franklin 和 Franklin(2015)指出，個人、財產性的犯罪及被害可透過評估特定事件下的情境因素加以詮釋。日常活動理論著重於探討「機會」與「情境」兩個因素，認為機會是被害的根本原因，若缺乏機會與情境因素，則犯罪被害之可能性將大大地降低(Felson & Clarke, 1998)。有鑑於「機會」與「情境」要素在網路詐欺被害研究之重要性，以下茲就網路安全監控(社會監控、物理監控)、網路負面誘因及網路偏差動機相關實證研究分別闡述如下:

（一）網路安全監控

有能力的監控者，係指監控個人從事網路行為的相關人、事、物，抑或是阻礙具有動機的犯罪者傷害、攻擊或獲得標的物的能力。所謂有能力的監控者並不一定單指代表國家、具有公權力之執法人員或是實體的監控設備，即使是父母、親友或同儕等人皆可成為有能力之監控者。日常活動理論更進一步將有能力的監控者區分為「物理監控」及「社會監控」兩個類型(Bossler & Holt, 2009; Cohen & Felson, 1979; Marcum et al., 2010)，而在網路詐欺被害中，社會監控與物理監控則扮演了非常重要的角色。

1.社會監控

在社會監控方面，國內溫怡婷(2008)對於詐欺重複被害特性及其歷程進行研究發現，詐欺重複被害者較缺乏防詐意識、通常被隔離於他人的協助之外，因而使其形成一種與外界資訊隔離的狀態，形成了一種監控的缺乏，並呈現一種疏離狀態(Alienation status)。陳永鎮(2007)對於台灣地區新興詐欺犯罪趨勢與歷程研究發現，詐騙集團之行為通常是一個階段扣著一個階段，讓被害者最後信以為真而依賴加害者，使被害者陷於一種孤立、缺乏外界資訊接觸的階段。葉雲宏(2008)網路詐欺被害影響因素研究發現，在個人遭受網路詐欺被害時，有 53.75%的被害者其周圍並無其他監控。

國外學者 Fisher 等人(2002)研究發現，單獨生活確實會增加個人的被害風險，因為單獨生活致使個人缺乏有能力的社會監控者，而社會監控者的缺乏使犯罪者在從事犯罪行為時減少阻力，並增加其直接接觸目標的能力。Grabosky 和 Smith(2001)網路犯罪之研究發現，許多不同類型之網路被害行為，皆係因為缺乏有能力的社會監控者而發生。Lwin 等人(2008)研究指出，社會監控者在網路犯罪中扮演重要的角色，並認為父母積極的網路監控行為確實能有效遏阻個人參與網路偏差行為或成為網路犯罪被害者的機會。Yar (2005)對於網路騷擾犯罪進行研究後發現，社會監控者顯著地影響網路騷擾被害者，研究指出，社會監控者極可能在網路騷擾中發揮作用。當一個人的同伴參與電腦犯罪或偏差行為時，偏差同伴之增加將會大大地減少了個人受到網路騷擾時，可以提供幫助的社會監控者之數量，因此，缺乏社會監控者將會使犯罪者獲得直接接觸標的物的能力。

綜上所述，多數國內外相關研究均顯示，網路詐欺被害者在從事網路行為的過程中，若有重要他人適時地介入個人行為，並適當地扮演「有能力的社會監控者」，便極有可能降低其被害行為之發生（溫怡婷，2008；陳永鎮，2007；蔡佳瑜，2010；葉雲宏，2008；Grabosky & Smith, 2001; Wall, 2007; Welte & Wieczorek, 2001; Zhang, 2002）。

2.物理監控

在物理監控方面，國內廖釗頡(2010)的網路釣魚被害者研究發現，當網路使用者對於個人資訊有較高的防護能力或有較高的被害意識時，就較不易成為網路釣魚被害者。Choi(2008)對於個人網路日常活動（使用電子郵件和下載）、數位監控與網路犯罪被害進行研究發現，擁有較高數位監控程度之大學生能有效降低其電腦遭受病毒被害的風險。Leukfeldt 和 Yar(2016)的研究發現，在網路消費者詐欺的被害類型中，個人的高度網路被害風險感知，確實降低其成為網路詐欺被害者之機會，並認為具有高網路風險意識者往往較能防範詐欺行為，進而較不易成為網路詐欺被害者。Ybarra 等人(2007)研究發現，在網路上與陌生人之交談與個人網路被害間具有關聯性，並認為個人應提升其風險意識並減少與陌生人的互動，因為它可能增加不同形式網路被害的可能性。

部分研究發現，隨意開啟不明來源的電子郵件或點擊其附件，均有可能會因郵件中所夾帶具詐欺性的訊息或竊取個人資訊的附件而增加個人被害風險(Chen et al., 2017; Taylor et al., 2010)，因此，對於經常更換或使用複雜密碼的網路使用者而言，較能有效減少其成為網路被害者之機會(Furnell, 2002; Nazario, 2003; Taylor et al., 2010)。

此外，個人監控在網路犯罪預防中具有重要的作用。Reisig 等人(2009)研究發現，個人的網路風險認知程度與其網路生活方式有關，當個人具有較高的網路風險認知時，其從事風險性網路行為的機會便會降低。多數實證研究亦發現，個人對於從事各項網路行為所可能會帶來的後果、風險危機意識程度及個人所採取的相關防護措施，皆能有效降低各種網路犯罪的被害(Bossler & Holt, 2010; Chen et al., 2017; Choi, 2008; Choi, 2017; Forsythe & Shi, 2003; Grabosky & Smith, 2001; Holt & Bossler, 2010; Ngo & Paternoster, 2011; Wall, 2007; Ybarra, Mitchell, Finkelhor, & Wolak, 2007)。當個人對於網路情境中的

風險意識提升，就會減少與陌生人的網路互動，而個人在從事網路行為時對於該行為的風險與後果之了解，以及個人採取降低風險的預防措施等，均能有效減少網路犯罪被害的可能性(Choi, 2008; Holt & Bossler, 2009; Whitty, 2019; Wolack et al., 2006)。

雖然上述研究支持物理及社會監控者與是否遭受網路被害具有關聯性，但仍有部分研究發現兩者間並未有顯著關聯性。Holt 和 Bossler(2009)以日常電腦使用、社會監控和物理監控的影響進行調查後發現，日常活動理論的要素與網路騷擾被害並無顯著關聯性，研究指出，僅有在特定情況下長時間與他人接觸才會提升個人網路騷擾被害之風險。Marcum(2010)之研究亦指出，有能力的監控者並無法有效降低網路被害行為之發生。Ngo 和 Paternoster(2011)以可見性、可接觸性和監控對於七種不同形式的網路被害類型進行調查後發現，情境特徵與網路監控要素並不會影響個人在網路空間被害的可能性。

（二）網路負面誘因

生活方式暴露理論認為，在日常活動中愈常與犯罪者接觸者，個人被害風險愈高。所謂「網路負向誘因」，係指個人在網路使用的過程中，曾接受違法交易訊息之機會，以提供個人機會而造成網路偏差或被害行為之發生。國內簡鳳容(2018)研究發現，接收較多網路負面誘因或刺激者，個人網路偏差動機越高，其自陳網路偏差及被害行為越多。陳怡璇(2007)研究性別、少年網路偏差與犯罪行為影響因素發現，網路負面誘因係少年網路偏差及犯罪行為之重要解釋及預測因素。黃俊祥(2007)少年網路偏差及犯罪行為之成因研究後亦發現，網路負面誘因與個人的網路偏差及犯罪行為具有顯著關聯性存在。葉雲宏(2008)網路詐欺被害研究發現，網路詐欺被害者相較於未被害者，有較高的網路負面誘因，在網路使用過程中，接收較多網路負面誘因者，其網路詐欺被害機會亦越高。

綜觀多數國外研究亦均指出，網路負面誘因在日常活動理論中所扮演的角色，代表合適的標的物，因此，當網路使用者越常接受網路負面誘因或被網路負面誘因所吸引者，其成為合適標的物之程度越高，亦即個人遭受各類型網路被害行為之可能性也越高(Blackburn et al., 2014; Bossler & Holt, 2009; Holt et al., 2012; Holt et al., 2018; Kerstens & Jansen, 2016; Marcum, 2010; Reyns , 2010; Xu, Xu, & Yayla, 2013)。

（三）網路偏差動機

Wysocki(2001)指出，網路生活型態與個人網路偏差動機有關，而網路偏差動機則與個人網路偏差行為存在高度相關。網路中大量且豐富的資訊容易成為誘發犯罪或偏差行為的因子，而網路的方便、刺激與匿名性更有可能使個人習得偏差行為（王茜，2014）。

在網路偏差動機方面，國內江南逸(2003)對於國中生網路偏差行為及網路沉迷對於個人生活適應狀況之研究發現，個人的網路偏差動機越高，則越容易產生網路沉迷現象。王茜(2014)研究指出，偏差動機較高或具有較多偏差行為者，其網路被害的機率較高。黃俊祥(2007)、陳怡璇(2007)研究發現，網路偏差動機能有效預測網路偏差及犯罪行為。

國外學者 Donner 等人(2014)研究自我控制與網路偏差之關聯性發現，低自我控制與網路偏差行為存在顯著正相關，自我控制確實能有效解釋不同形式的網路偏差行為。Gilboa (1996)、Taylor (2003)、Marcum 等人(2011)之研究均發現，參與電腦犯罪和網路偏差行為可能會增加個人與具有動機的犯罪者之接觸，從而導致更高的網路被害可能性。Greenfield(2000)研究指出，經常瀏覽色情網站的青少年，對於兩性間的情感互動及歸屬將產生網路上的偏差概念。Holt 和 Bossler(2009)對於網路偏差行為與網路被害間關聯性之研究發現，若個人和同儕參與網路偏差行為，將顯著地增加其各類型網路被害之風險。Pratt 等人(2010)研究發現，在網路詐欺之被害情境中，待在家中並從事各種偏差的網路行為，皆會增加個人暴露於潛在犯罪者之可能性，使個人成為詐欺被害目標可能性增加。Sampson 和 Laurtisen(1990)研究發現，網路被害者之網路偏差行為顯著高於未被害者，研究更進一步指出，網路使用者參與的一些偏差行為確實將使其暴露於更多潛在犯罪者中，進而增加其網路被害風險。此外，部分研究對於網路偏差行為與個人基本特性進行研究後發現，男性、較年輕者更容易發生網路偏差行為(Buzzell, Foss, & Middleton, 2006; Higgins, Wolfe, & Marcum, 2008; Jensen & Brownfield, 1986)。

綜上所述，多數研究均指出，在網路中所從事之偏差生活方式將使個人與具有動機犯罪者接觸的機會增加，從而使個人被害的風險提升(Buzzell et al., 2006; Foster, 2004; Holt et al., 2012; Jensen & Brownfield, 1986; Lauritsen et al., 1992; Zhang et al., 2001)。

五、網路詐欺犯罪之重複被害

多數被害者學理論皆指出，被害現象並非隨機分布，多數被害行為不僅集中於特定時間、地點，亦集中於特定之少數人，使這些人相較於其他人更容易被害(Clare & Morgan, 2009)，從而形成所謂「重複被害者」(Repeated Victim ; Revictimization)，且因少部分人遭受高比例之犯罪被害事件，故學者 Farrell(1992)將這些重複被害者稱為「慢性被害者」(Chronic victims)或「核心被害者」(Hard-core victims)，這些 2%的人經歷了超過 41%的財產性犯罪(Pease, 1998)，其中更有 8 分之 1 的重複被害者是所謂的超級目標(Chenery et al., 1997)。在重複被害中，被害的類型可以是相同或不同的犯罪類型，因此，在多數研究之定義中，包括在特定時間、空間中遭受同一犯罪類型之單一犯罪類型重複被害(Repeated Victimization)，以及某特定時間或地點遭受 2 種以上被害類型之多重被害(Multiple Victimization)等兩種意涵。

Turanovic 與 Pratt(2012)指出，重複被害是一個複雜的社會現象，Levy 和 Tarturo(2010)則進一步指出，犯罪在空間上集中所造成之犯罪熱點，其實往往是因為重複被害之現象所導致，學者 Johnson 等人(1998)更認為重複被害之研究對於犯罪學及犯罪統計具有極為重要且實質性之貢獻，多數學者亦指出，由於少數的潛在被害者重複遭受大量的傷害，因此若能將有限的犯罪預防措施與刑事司法資源全數挹注於重複被害者，除了能大量減少犯罪的集中性與重複性，有效提升犯罪預防之效能外，亦能更合理且更公平的分配風險及損害(Farrell, 1995; Farrell & Grove, 2012; Grove et al., 2014; Ignatans & Pease, 2018)，綜上所述，重複被害之研究無論在犯罪學或犯罪預防領域中均具有其研究之必要性。

在重複被害研究中，多數學者認為重複被害係因一連串負面因果機制所導致，除了係因被害者具有之特定個人弱點特質外，Hindelang 等人(1978)認為生活方式在重複被害現象中扮演重要角色，認為個人日常活動的改變，將使其在特定時間、地點與特定潛在犯罪者接觸、暴露於犯罪情境，並因此帶來不同程度之被害風險，故多數研究經常以日常活動、機會及自我控制理論探究個人日常生活方式、低自我控制與重複被害之關聯性(Averdijk, 2011; Averdijk & Loeber, 2012; Franklin, 2011; Miethe, 1990; Posick & Zimmerman, 2015; Schreck et al., 2006; Turanovic & Pratt, 2012; Turanovic et al., 2016)。

在重複被害之研究方面，Farrell 與 Pease (1993)認為重複被害現象之發生係由外在環境因素及個人風險因素交互作用下所產生之結果，Pease 和 Ignatans(2016)研究發現，重複被害者之個人及社會基本特性，確實與未被害者有顯著差異，而 Spark 等人(1996)亦認為，重複被害現象之發生與被害者之性別、種族及年齡等個人特性有顯著之影響，經過多數實證研究後，自我控制與偏差生活方式被證實為重複被害現象之重要預測因素。在生活型態及日常活動理論部分，多數研究均發現，偏差的日常活動將會導致被害者與潛在的犯罪者接觸，並減少有能力之監控者(Burrow & Apel, 2008; Gover, 2004; Mustaine & Tewksbury, 1998; Sampson & Lauritsen, 1990; Smith & Ecob, 2007; Taylor et al., 2008)；而在自我控制理論部分，研究發現，個人的自我控制能力不僅會使其容易陷入高風險之危險情境中，亦使其參與偏差日常活動之可能性大幅增加，從而增加其重複被害之機會(Schreck, 1999; Schreck et al., 2002; Schreck & Fisher, 2004; Schreck et al., 2008)。

此外，國內外多數研究進一步發現，個人過去所發生之偏差或被害行為確實增加其未來再次被害之風險，因此，曾有被害經驗者其重複被害之可能性，較無被害經驗者高（許春金，2000 ; Finkelhor et al., 2007; Gottfredson, 1984; Lauritsen & Quinet, 1995; Menard, 2002; Outlaw et al., 2002; Pease, 1998; Ruback et al., 2014; Turanovic & Pratt, 2012）。

在詐欺犯罪之重複被害現象方面，早期因受限於經濟活動和較保守的通訊科技型態，詐欺行為的手法也較單純，並多以賭博詐欺、票據詐欺、假冒身分詐欺等犯罪類型為主（溫怡婷，2008），但近年來由於網際網路之蓬勃發展，而導致人們的日常生活型態發生結構性的變化，據此，各式各樣的網路生活型態及消費行為亦隨之改變，並增加各階層網路詐欺被害之可能性，這也導致詐欺手法逐漸透過網際網路的管道，以不受時空限制、無遠弗屆之特性而深入人們的生活中，形成以網路為重要渠道的詐欺犯罪行為。

有關國內在網路詐欺重複被害之實證研究部分，張隆興(2005)對於詐欺犯罪之重複被害者進行研究，針對單次被害及重複被害者進行研究發現，重複被害者以男性居多、年齡約介於 20 至 29 歲之間、教育程度以高中及大學占多數、職業則多以無業、工礦、商業及金融業為主。張耀中、周愫嫻(2002)以大台北地區之倒會重複被害者為例進行研究，經量化統計分析結果發現，倒會之重複被害者以女性居多、年齡層多為青壯年、教

育程度多為高中職以下且家庭收入較低。此外，研究亦進一步發現，在被害者當中，年齡層較高、教育程度較低、收入較低及理財較多樣者，較可能成為倒會之重複被害者。溫怡婷(2008)以官方次級資料及深度訪談法對於詐欺犯罪之重複被害特性及歷程進行分析，在量化分析部分，詐欺重複被害者之基本人口特性中，性別、年齡和居住地分布未有顯著差異，在性別部分，男性(52.7%)略高於女性(47.3%)，在年齡部分，大多集中於較有經濟能力之青壯年族群，而在年齡與詐欺金額之交叉分析部分，研究發現，重複被害者有年齡較高的狀況。在深度訪談之結果部分，詐欺犯罪重複被害者具有剛愎自用、堅信不疑、缺乏警覺、疏忽大意、僥倖心態、短視近利、心急如焚以及當局者迷等個人特質，在機會及監控因素部分，包括人際互動存在盲點，在從事休閒娛樂時，缺乏警覺性與判斷力、具有投機性心理之風險理財觀念、缺乏防詐警覺心並缺乏外在監控。

國外有關日常活動與重複被害相關實證研究方面，Miethe 等人(1990)探究個人日常生活模式與重複被害之關聯性，研究發現，經常從事偏差生活型態者較容易被害，個人若在被害後仍持續從事相類似之偏差生活型態，則個人重複被害之可能性將隨之提升。此外，研究更指出，被害風險係隨著時間推移所產生之生活方式之變化和穩定而決定。Averdijk (2011)則試圖進一步拓展 Miethe 等人(1990)之研究，期望藉由日常活動理論所建構之指標，探究重複被害之重要原因機制，在其研究後發現，由於數據之部分限制，故僅發現日常活動理論確實係解釋被害之重要因素，而無法據以推論至重複被害現象。Pratt 和 Turanovic(2016)、Schreck 和 Stewart(2011)對於偏差生活型態與重複被害之研究亦指出，雖然偏差生活方式有許多型態，但與被害直接相關的是與犯罪有關的生活方式。Keay 和 Kirby (2017)、Titus 和 Gover(2001)研究發現，網路詐欺重複被害與空間位置之因素間並不具關連性，亦即在網路詐欺重複被害中，個人特質及行為才是決定是否遭受重複被害之重要因素。Whitty(2019)以心理學、犯罪學理論研究網路詐欺被害感知性、網路詐欺單次被害與重複被害者之差異，研究發現，網路詐欺單次被害或重複被害者之個人基本特性、心理特質及網路日常活動並未有顯著差異，且兩者被害者共通特徵多為:年齡較大、在衝動性及尋求刺激性得分較高、在網路成癮性的得分較高，並具有較頻繁的網路風險日常活動。

在自我控制與重複被害之實證研究方面，Schreck(2006)首先探究低自我控制能力者是否增加其重複被害之風險、自我控制程度是否影響個人過往被害經驗，以及自我控制程度是否會導致個人再次參與高風險生活型態，進而再次成為重複被害者，在其研究後發現，低自我控制者其重複被害之風險相對較高，且當低自我控制者被害後，其將再次從事相類似之高風險生活方式，進而形成重複被害者，因此，研究亦證實自我控制理論確實係影響重複被害之重要因素。自 Schreck(2006)建構自我控制理論與重複被害之間的關係後，自我控制與偏差生活型態之間的改變關係就被視為是理解重複被害之基礎。Turanovic 與 Pratt(2012)則進一步將自我控制理論及日常活動理論結合，除了試圖了解被害者之自我控制程度在多大程度上解釋了個人被害後從事危險生活方式的可能性外，亦探究重複被害是否與個人改變其生活型態有關，研究發現，個人的自我控制程度顯著影響其在被害後是否改變了危險的生活方式，而這些危險生活方式之改變則決定了個人是否再次成為重複被害者之可能性。此外，研究亦發現危險生活方式之改變完全調節了自我控制對於重複被害之影響，這個發現也進一步證實兩者間確實具有重要之關聯性。Turanovic 和 Pratt (2014)再次以日常活動理論及自我控制理論對於重複被害者進行分析，研究亦指出，當被害者減少其風險偏差行為，則其再次遭受被害之機率亦隨之降低。Turanovic、Pratt 與 Piquero(2016)對於偏差生活型態與重複被害之關聯性進行研究，除研究繼續從事偏差生活方式是否導致重複被害外，亦以結構性限制(structural constraints)對於個人是否繼續從事偏差生活型態進行研究後發現，在重複被害現象中，結構性約束限制個人偏差生活方式之改變，使個人繼續從事偏差生活型態，進而導致重複被害。

綜上所述，多數國內外實證研究具體反映出犯罪學領域長期以來對於重複被害現象解釋之關注，這不僅代表其研究重要性，也代表在犯罪預防中具有實質性之貢獻及意義，而在多數以自我控制及日常活動理論為架構，探究重複被害之研究發現，重複被害者之低自我控制特質及偏差生活型態，確實與個人是否成為重複被害者，具有根本上之關係。此外，儘管部分研究對於重複被害之現象已奠定了相當大的基礎，但對於造成網路詐欺重複被害之因果機制，仍有許多方面值得深入探討，故本研究將以網路日常活動理論及自我控制理論，對於網路詐欺重複被害之因素進行深入探討。

第六節 綜合評述

Newman 和 Clarke(2003)指出，社會結構的變化以及隨後犯罪模式之變化可歸因於科技技術的進步。隨著科技日新月異及網路無遠弗屆，帶給了人們許多生活上的便利並促使社會變遷，社會變遷使得人們生活型態漸漸受到網路影響，原本在實體物理空間中，人與人之間面對面的直接接觸，逐漸轉變為透過網際網路及電子科技設備在虛擬社群中與陌生他人的交流及互動，而在網路技術持續更新的同時，犯罪手法亦不斷地更新其管道及場域。近年來，網路詐欺犯罪所造成的社會成本及被害損失日趨增加，越來越多的潛在網路詐欺犯罪者利用各種不同的網路渠道尋找合適的被害標的物，而網路無遠弗屆的特性也使得犯罪者與被害者之間的接觸不受時間、空間限制。綜合上述有關網路詐欺犯罪被害之相關文獻，對於網路詐欺被害特性歸納如下:

首先，個人基本特性方面，多數研究顯示，性別係網路詐欺被害之重要預測因子，被害者中以男性為多數。在年齡分布上，雖多數實證研究顯示被害者年齡介於 20 至 29 歲間，但亦有研究顯示為 18 至 24 歲間，整體而言，被害者年齡大多介於 18 至 39 歲間。職業方面，研究發現，被害者職業以學生、工業及無業者居多。收入方面之相關研究則尚未有一致性定論，但綜合國內外相關實證研究發現，多數被害者之收入為五萬元以下。教育程度方面，網路詐欺被害者大多以中等教育程度、高中以上至大學／專科以下居多。婚姻狀況方面，研究發現未婚者、單身者較容易成為網路詐欺被害者。

其次，在低自我控制與個人基本特性方面，研究指出，性別為自我控制的強力預測因子，男性通常較女性缺乏自我控制。在年齡方面，自我控制因不同年齡而有所差異，較年輕者其自我控制程度通常較低，而具低自我控制特質者將顯著增加個人被害風險。具有衝動性特質者，往往在未充分考慮後果的情況下從事衝動性的行為，從而增加個人暴露於犯罪情境或機會的可能性，並增加其與犯罪者接觸的機會。具冒險性特質者經常從事高風險的投資行為，而風險較高的投資行為較易使其成為網路詐欺被害者。具投機性特質者，經常期望能以最少的投資或付出很小的努力而獲取立即致富的機會，且具有以小搏大的賭徒心理和充滿風險的理財觀念，使個人成為網路詐欺被害者的機會提升。

再者，網路生活型態與個人基本特性方面，多數研究指出，性別、教育程度及個人收入與網路詐欺被害具有顯著關聯性，其中，男性、受過良好教育及高收入水平者從事網路交易、網路購物或網路使用頻率較高，其遭受網路詐欺被害之可能性也相對較高。有關個人網路生活型態及網路詐欺被害方面，研究指出，個人的日常網路生活型態與其是否成為網路詐欺被害者具有顯著之關聯性，經常從事高風險網路休閒或職業活動者，可能增加個人與具有犯罪動機犯罪者接觸，從而增加其遭受網路詐欺被害之可能性。

多數實證研究指出，網路詐欺犯罪者依循各種網路途徑來尋找及鎖定潛在的被害者，而網路詐欺被害者大多高度依賴於網路之使用、不僅以上網為其網路休閒活動、亦經常從事網路交易、網路購物、經常瀏覽高風險性的網站並經常開啟不明來源的電子郵件或其夾帶之附件。此外，研究亦指出，個人高頻率的日常網路活動行為將使他們更有可能成為各類型的網路犯罪被害者，當個人接觸網路之時間越早、接觸網路的時間越長、接觸網路的頻率越高，其暴露於有動機之潛在犯罪者之風險可能性就會增加，這也可能使網路使用者更容易成為網路詐欺被害者。

最後，被害情境與機會變項方面，多數研究顯示，網路詐欺被害者通常缺乏有效的物理或社會監控。在物理監控方面，研究指出，個人的被害意識及其採取的防護措施與其是否成為網路詐欺被害者具有顯著關聯性，藉由個人提升其風險意識、減少與陌生者的網路互動及採取有效降低風險的網路預防措施等，均可有效減少網路詐欺被害之風險。在社會監控方面，研究顯示，有效的社會監控者在網路詐欺被害中扮演十分重要的角色，缺乏社會監控者將減低個人監控之能力，並進一步強化犯罪者獲得直接接觸標的之能力，而外在社會監控者亦能有效遏阻個人參與網路偏差行為或成為網路詐欺被害者的機會。在網路負面誘因，多數研究皆認為，網路負面誘因代表個人成為合適標的物之程度，當個人在網路使用過程中接收越多負面誘因，其網路偏差或被害行為之程度將隨之提升。在網路偏差動機方面，研究指出，網路偏差動機與網路詐欺被害之間存在顯著關聯性，個人所參與的一些網路偏差行為將使其暴露於更多犯罪者或被害的情境中，進而增加其網路詐欺被害的風險。綜上所述，本研究根據上述文獻回顧，整理網路詐欺被害之相關因素如下表 2-6-1 所示:

表 2-6-1 網路詐欺犯罪被害國內外相關實證研究彙整表

變項名稱	內容	相關性	相關實證研究	研究發現
個人基本特性變項	性別	+/-	王秋惠(2007)；黃祥益(2006)；葉雲宏(2008)；蔡佳瑜(2010)；Mesch & Dodel(2018); Reyns(2015)	多數研究發現男性被害者顯著多於女性 僅有少數研究發現女性被害者多於男性
		NS	Leukfeldt & Yar(2016); Louderback & Antonaccio(2017); Ngo & Paternoster(2011); Pratt et al.(2010)	
	年齡	+/-	王秋惠(2006)；黃祥益(2006)；蔡佳瑜(2010)；葉雲宏(2008)；廖釗頡(2010)；Leukfeldt & Yar(2016) Mesch & Dodel(2018); Jorna(2016b); Pratt et al.(2010); Reyns(2013); Reyns(2015); Ross & Smith(2011)	大多數研究顯示被害者之年齡約介於18至40歲之間，其中以18至24歲者居多。
		NS	王秋惠(2007)；Leukfeldt & Yar(2016); Louderback & Antonaccio(2017); Ngo & Paternoster(2011)	
	職業	+/-	蔡其芳(2006)；王秋惠(2007)；黃祥益(2006); 廖釗頡(2010)；Kigerl(2012); Leukfeldt & Yar(2016)	多數研究顯示被害者之職業以學生、工、無業者居多。
		NS	Ngo & Paternoster (2011); Reyns(2013)	
	收入	+/-	蔡其芳(2006)；廖釗頡(2010);Pratt et al.(2010); Kigerl(2012); Reisig, Pratt, & Holtfreter(2009); Ross & Smith(2011)	多數研究顯示被害者收入為五萬元以下。
		NS	Leukfeldt & Yar(2016)	
	教育程度	+/-	王秋惠(2006)；黃祥益(2006)；蔡其芳(2006)；葉雲宏(2008)；蔡佳瑜(2010)；廖釗頡(2010) Pratt et al. (2010); Leukfeldt & Yar(2016)	研究顯示被害者以中等教育程度、高中以上至大學／專科以下佔多數。
		NS	Mesch & Dodel(2018)	
	婚姻狀況	+/-	蔡其芳(2006)；葉雲宏(2008)；Holtfreter(2008); Ross & Smith (2011); Titus & Boyle(1995)	研究顯示未婚者、單身者較容易成為被害者。
		NS	Ngo & Paternoster(2011); Pratt et al.(2010); Reyns(2013); Reyns(2015)	

低自我控制特性變項	衝動性 冒險性 投機性	+	王秋惠(2007)；林清榮(2006)；葉雲宏(2008)；溫怡婷(2008)；Baumeister(2002); Chen et al.(2017); Holtfreter et al.(2008); Leukfeldt & Yar(2016); Reisig et al.(2009); Romal & Kaplan(1995); Tangney et al. (2004); Van Wilsem(2001); Van & Mason (2001)	大多數研究發現低自我控制特質與網路詐欺被害具有正相關。多數研究亦顯示低自我控制特質者(衝動性、冒險性、投機性)較容易因各種因素而成為犯罪被害者。
		NS	Leukfeldt & Yar(2016); Louderback & Antonaccio(2017); Ngo & Paternoster(2011); Pratt et al.(2010)	
網路生活型態變項	網路使用特性	+	王秋惠(2007)；吳嫦娥、蔡麗滿(2004)；廖釗頡(2010)；廖釗頡(2010)；鄭英瑋(2004)；賴克宗(2007) Pratt el al.(2010); Ross & Smith(2011); Wilsem(2011)	多數研究發現，個人接觸網路時間越早接觸時間越長、接觸頻率越高，且在家中上網者，較易成為網路詐欺被害者
		NS	Bossler & Holt(2009)	
	網路休閒與職業活動	+	吳嫦娥、蔡麗滿(2004)；黃祥益(2006)；葉雲宏(2008)；蔡佳瑜(2010)；蔡其芳(2006)；賴克宗(2004)；廖釗頡(2010)；Aghekyan-Simonian et al. (2012); Mesch & Dodel(2018); Pratt et al.(2010); Reisig et al.(2009); Smith et al.(2005); Van Wilsem(2011a, 2011b)	多數研究發現花費更多時間從事具有風險的網路行為、使用越多網路交易行為、在網路上有越多購物行為，以網路為休閒活動者較易成為網路詐欺被害者。
		NS	Bossler & Holt(2009); Holt & Bossler(2009) Leukfeldt(2014); Reyns et al.(2011)	研究顯示，個人電腦使用時間之長短對於個人是否成為網路犯罪被害者並無顯著關聯性。
	網路風險休閒與職業活動	+	廖釗頡(2010);葉雲宏(2008)；Choi(2008); Choi & Lee (2017); Holt & Bossler(2009); Reyns(2013); Leukfeldt & Yar(2016); Mesch & Dodel(2018); Pratt et al. (2010)	研究顯示，具風險性的網路使用行為(長時間、頻繁地使用網路交易、從事網路購物及網路下載軟體等)，使他們更容易成為網路犯罪之被害者。
		NS	Holt & Bossler(2009); Leukfeldt(2014)	

被害情境與機會變項	網路安全監控	-	王秋惠(2007)；陳永鎮(2007)；葉雲宏(2008)；廖釗頡(2010)；溫怡婷(2008)；蔡佳瑜(2010)；Bossler & Holt(2009); Choi(2008); Choi(2017); Fisher et al. (2002); Grabosky & Smith(2001); Leukfeldt & Yar(2016); Lwin et al. (2008); Ngo & Paternoster(2011); Reyns(2015); Welte & Wieczorek(2001); Yar(2005); Ybarra et al.(2007)	研究發現，多數網路犯罪被害者係因缺乏有能力的監護者(物理、社會監控)而發生。缺乏安全監控會使犯罪人在從事犯罪時減少阻力，並增加其直接接觸目標的能力而導致個人被害風險增加。
		NS	Holt & Bossler(2009); Marcum(2010) Ngo & Paternoster(2011); Reyns et al.(2011)	
	網路負面誘因	+	黃俊祥(2007)；陳怡璇(2007)；簡鳳容(2018) 葉雲宏(2008); Blackburn et al.(2014); Holt & Bossler(2009); Holt et al.(2012); Holt et al.(2018); Kerstens & Jansen(2016); Marcum(2010); Reyns(2010)	研究顯示，在網路使用過程中接受到負面訊息或誘因的頻率高低，與個人是否成為網路詐欺被害者成正相關。
		NS	尚未有相關研究	
	網路偏差動機	+	王茜(2014)；黃俊祥(2007)；陳怡璇(2007)；簡鳳容(2018); Baker & Faulkner(2003); Donner(2004) Franklin et al.(2012); Holt & Bossler(2009); Marcum et al.(2011); Sampson & Laurtisen(1990) Shover et al.(2003); Shover et al.(2004)	研究顯示，在網路上散播個人訊息、經常從事具網路偏差行為，皆較有可能成為網路詐欺犯罪被害的目標。
		NS	Ngo & Paternoster (2011); Reyns(2013)	

註:N.S.表示未達統計上之顯著差異(Non-Significant)

（資料來源：本研究彙整）

網路詐欺犯罪被害與其他犯罪被害類型不同，需要被害者和犯罪者之間在某種程度上進行合作。透過前述犯罪學理論及近年來國內外相關實證研究，可以得知，犯罪手法隨著電子通訊科技的發展與整合更加多元、犯罪場域亦隨著網路無遠弗屆的特性而不受時間與地點之限制，犯罪者除了透過日新月異的科技設備及管道散播、傳達不同的詐欺訊息外，更利用人性的貪婪、恐懼、懦弱及同情心等個人弱點，以卸除民眾警戒，民眾稍有不慎，就容易因錯誤的判斷而遭到財務上的詐騙損失。

綜觀上述國內外實證研究，雖對於網路詐欺被害者之個人基本特性、自我控制程度、網路生活型態與被害情境及機會均有部分探討，但對於網路詐欺被害之性別差異因素則鮮少有深入研究，多數研究僅將性別做為控制變項，而並未將其納入主要的觀察變項、探討不同性別間被害差異現象之特殊性。

此外，雖然有些個人特質有助於辨識個人是否將成為網路詐欺被害者，但部分學者認為，由於網路詐欺之犯罪者係透過網路渠道，深入人們的日常生活型態，並對於來自各種不同人口背景之網路使用者遂行其詐欺行為，因此僅單獨以社會基本人口特性因素，並無法準確預測個人是否將成為網路詐欺被害者(Pratt et al., 2010; Ross &Smith, 2011)。有鑑於此，本研究除了綜合歸納國內外相關實證研究外，亦擬以「網路日常活動理論」、「自我控制理論」之理論概念作為研究架構，以深入探討不同性別網路使用者間之個人基本特性、低自我控制特性、網路生活型態及被害情境與機會等網路詐欺被害差異因素，並根據上述理論與相關文獻回顧，將性別納入主要觀察變項，對於不同性別之網路詐欺被害者進行深入分析與研究，相關研究架構理論模式如後。

第三章 研究設計與實施

本研究依據前述研究背景、動機與目的，並以網路詐欺被害相關理論及文獻為基礎，採用文獻探討法、網路問卷調查法進行研究。本章共分為六節，以下擬對於研究流程、研究架構、研究假設、研究方法、研究對象、研究工具、實施程序、資料處理與分析及本研究所涉及之研究倫理原則等，分述如下：

第一節 研究流程與研究架構

一、研究流程

本研究主要目的在於探討不同性別間網路詐欺被害之差異、特性及重複被害之因素。本研究之研究流程係透過蒐集網路詐欺被害相關理論、文獻資料及根據國內外實證研究所編製之網路問卷，蒐集網路詐欺被害者之相關資料進行分析，以探討不同性別間被害差異之影響因素，並對於網路詐欺被害現象作一綜觀性的了解。有關本研究之研究流程如下圖 3-1-1 所示:

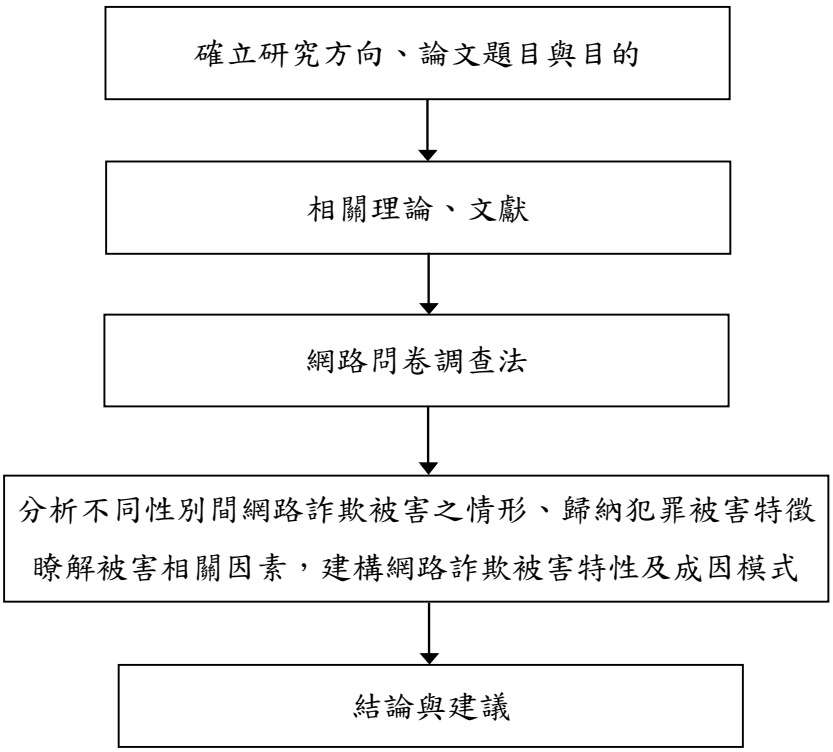

圖 3-1-1 研究流程圖

二、研究架構

本研究基於前述研究動機與目的，以犯罪學相關理論作為基礎並參酌國、內外相關實證研究與文獻資料，建構本研究之概念架構如下圖 3-1-2 所示：

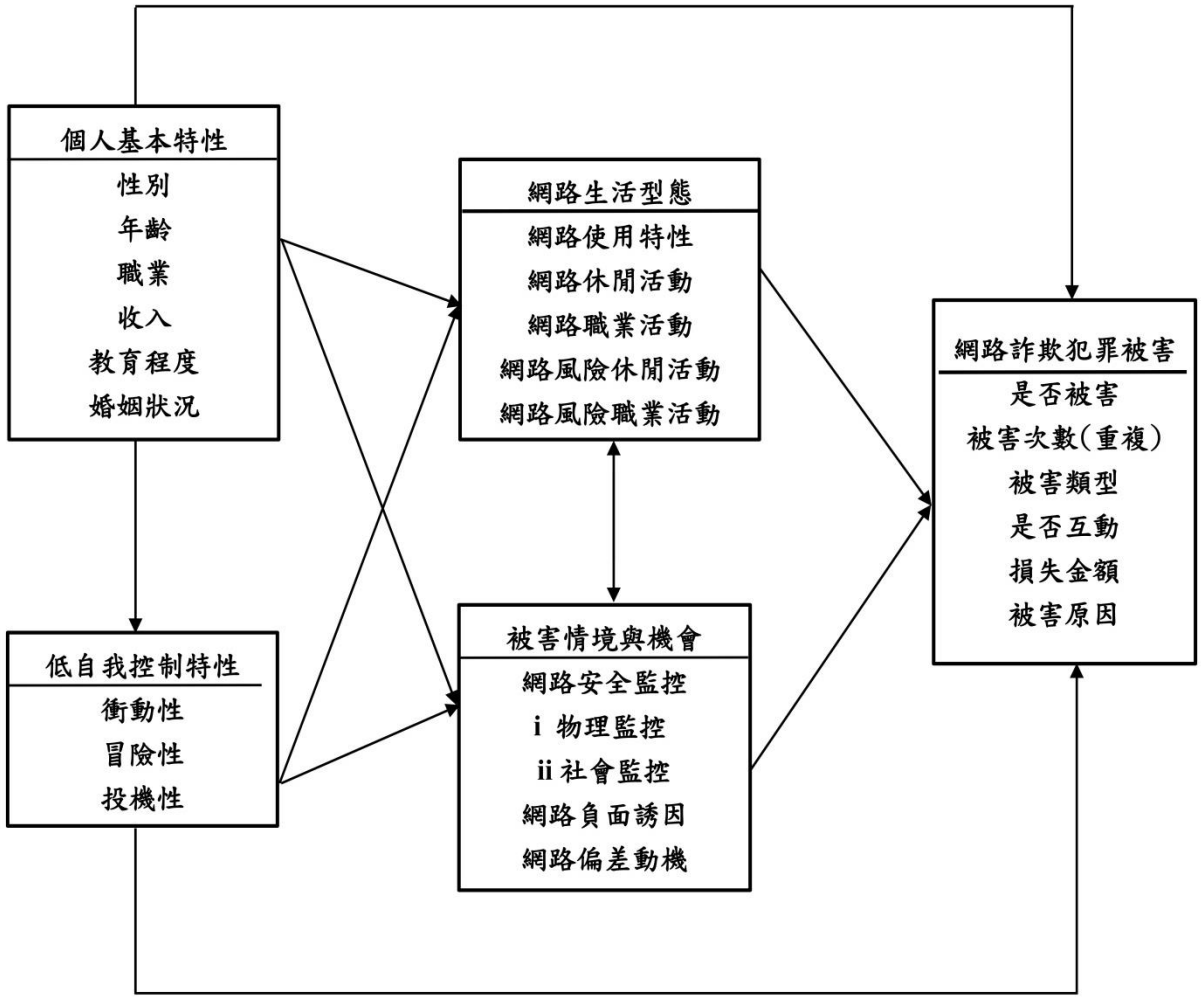

圖 3-1-2 研究架構圖

本研究架構之變項包括個人基本特性、低自我控制特性變項、網路生活型態變項、被害情境與機會及網路詐欺被害變項。本研究探討不同性別網路使用者之個人基本特性、低自我控制特性、被害情境與機會及網路詐欺犯罪被害間之關聯性，並以低自我控制與日常活動要素對於不同性別網路詐欺被害之解釋力與預測力進行檢驗。

本研究自變項為網路詐欺使用者「個人基本特性」，中介變項為「低自我控制特性」、「網路生活型態」及「被害情境與機會」，依變項為「網路詐欺犯罪被害」。有關本研究架構圖所示各變項之內涵如表 3-1-1 所示：

表 3-1-1 研究概念與變項測量表

變項類別	變項群名稱	變項內容
自變項	個人基本特性	性別
		年齡
		職業
		收入
		教育程度
		婚姻狀況
中介變項	低自我控制特性	衝動性
		冒險性
		投機性
	網路生活型態	網路使用特性
		網路休閒活動
		網路職業活動
		網路風險休閒活動
		網路風險職業活動
	被害情境與機會	網路安全監控(物理監控、社會監控)
		網路負面誘因
		網路偏差動機
依變項	網路詐欺犯罪被害	是否被害
		被害次數(重複)
		被害類型
		是否與加害者互動
		損失金額
		被害原因

本研究變項包括「個人基本特性」、「低自我控制特性變項」、「網路生活型態變項」、「被害情境與機會變項」及「網路詐欺犯罪被害」等五個變項群。

自變項為網路使用者之「個人基本特性」，係指網路使用者之個人基本特性，其中包括性別、年齡、職業、收入、教育程度與婚姻狀態等。

中介變項為「低自我控制特性變項群」、「網路生活型態變項群」、「被害情境與機會群」。「低自我控制特性變項群」係指網路使用者個人低自我控制之人格特質，包括衝動性、冒險性、投機性等三個層面。「網路生活型態變項群」係指網路使用者在日常網路使用的各項行為調查，包括網路使用特性、網路休閒活動、網路職業活動、網路風險休

閒活動及網路風險職業活動等變項。「被害情境與機會變項群」係指網路使用者暴露於網路詐欺被害情境及機會變項，其中，包括網路安全監控(物理監控、社會監控)、網路負面誘因及網路偏差動機等變項。

依變項為「網路詐欺犯罪被害」。網路詐欺犯罪被害係指網路使用者之被害經驗，包括是否被害、被害次數(重複)、被害類型、是否與加害者互動、損失金額、被害原因等項目。

三、研究假設

本研究假設不同性別的行為人具有不同的個人特性（年齡、職業、收入、教育程度及婚姻狀況)、不同程度的低自我控制特性,在不同網路生活型態及被害情境與機會下，遭受不同程度的網路詐欺犯罪被害。基於上述研究架構，本研究之研究假設如下:

（一)不同性別網路使用者之「個人基本特性」在「低自我控制特性」、「網路生活型態」、「被害情境與機會」及「網路詐欺犯罪被害」有顯著差異。

（二)不同性別網路使用者在「低自我控制特性」、「網路生活型態」、「被害情境與機會」及「網路詐欺被害經驗」有顯著差異。

（三)「網路生活型態」、「被害情境與機會」、「低自我控制特性」、「網路詐欺犯罪被害」有顯著關聯性。

（四)「個人基本特性」、「低自我控制特性」、「網路生活型態」與「被害情境與機會」對於「網路詐欺被害經驗」有顯著影響力。

（五)「個人基本特性」、「低自我控制特性」、「網路生活型態」與「被害情境與機會」對於不同性別之「網路詐欺被害經驗」，有顯著影響力。

（六)「個人基本特性」、「低自我控制特性」、「網路生活型態」與「被害情境與機會」對於「網路詐欺被害次數」有顯著影響力。

（七)「個人基本特性」、「低自我控制特性」、「網路生活型態」與「被害情境與機會」對於「網路詐欺重複被害次數」有顯著影響力。

第二節 研究方法

本研究係以文獻探討法與網路問卷調查法為主。為期能更全面、更深入地了解不同性別網路使用者之個人特性與網路詐欺被害之影響因素,除依前述文獻探討及相關實證研究所得之資料加以蒐集、分析網路詐欺被害者特性外，再依據歸納、分析所得之結果用以設計網路問卷進行調查，並於回收問卷資料後，進行統計資料之分析及理論觀點之驗證與探討，以下茲將本研究所採行之研究方法分述如下:

一、文獻探討法

文獻探討係對於研究議題和研究方向提出概念架構背景,透過對於不同資料之蒐集、整理、歸納與分析等步驟，以做為研究假設之基礎。以本研究而言，本研究以網路日常活動理論及自我控制理論作為理論分析架構,以檢視不同性別間網路詐欺被害之差異，並根據此研究架構，進一步分析網路詐欺重複被害者之特性，故本研究須蒐集網路詐欺被害有關之網路日常活動理論及自我控制理論內容及國內外相關實證研究資料。

有關本研究文獻探討資料包括:網路詐欺被害之國內外學術著作、期刊論文、圖書、實證研究、官方紀錄、法規命令及相關文獻，並於蒐集後加以閱覽、整理、分析及歸納，以期能更加全面且深入地了解現今網路詐欺犯罪被害現況，同時，藉由不同文獻資料之交叉分析比對，綜合歸納、整理出網路詐欺被害特性之相關影響因素。

二、網路問卷調查法

問卷調查用於描述性、解釋性或探索性的研究，所謂「問卷調查法」是透過研究者將預先設計好的問卷，對於具有代表性的受調查對象以瞭解情況或蒐集意見，並在彙整填答意見後,據以推估至全體母群對於某研究議題之態度或行為反應的一種研究方法。問卷調查法包括郵寄、面訪實施、電話訪問及網路調查問卷法等四種(許春金等,2016)。

本研究採取「網路調查問卷法」,所謂網路調查問卷法，係指利用網路的方式直接進行問卷調查所收集之第一手資料。本研究為深入分析不同性別間網路詐欺被害之差異因素及其特性,擬以自陳式網路問卷調查方式來調查受試者之個人基本特性及網路使用型態等變項，以下就網路問卷調查法之優、缺點分述如下:

(一) 網路問卷調查法之優點

網路問卷調查具有許多優點。首先，在樣本及抽樣方面，網路問卷除了能使受試者不受時空條件限制，隨時隨地進行填答外，更因網路無遠弗屆的特性，使研究問卷能夠觸及更多具高度異質性之潛在網路受訪者。其次，在問卷回收方面，網路問卷調查相較於傳統問卷調查(電訪式、郵寄式、面訪式)，具有低成本、高效益及回收時間快之優點(李政忠，2004)，而研究者也可以透過網路問卷管理平台進而精準掌控問卷回收進度。最後，在問卷內容及受試者填答方面，部分學者認為網路問卷調查可以有效減少研究者在面對面進行問卷調查時，對於受試者所產生的心理壓力及威脅感(Walsh, Kiesler, Proull, & Hesse, 1992)，因此可以有效減少受試者因心理壓力所產生之填答不正確性。

此外，在對於某些特殊、敏感性議題、研究主題之母體範圍不明確，或是受訪者之身分較為敏感、特殊之情況下，網路問卷較具有匿名性、私密性及隱私性，不僅能減少外在人為干擾，亦能使受試者在一個放心、安全的場域下進行問卷的填答，進而增加其自我揭露之可能性及填答真實性。

有鑑於本研究係對於網路使用行為者平日之網路使用情形進行調查，研究主題係涉及受試者較為私密性、隱私性之網路詐欺被害經驗，故採取網路問卷調查法，期望能透過匿名、隱私性的網路施測場域，對於曾有網路詐欺被害經驗之受試者，提供較為安全的施測環境，以提升本研究之問卷填答正確性。

(二)網路問卷調查法之缺點

雖然網路問卷具有上述諸多優點，但仍有其弊端。首先，網路使用人口不具代表性之問題，學者 Couper(2000)、Dillman(2000)指出，利用網路問卷調查第一個遇到的問題即為「涵蓋誤差」(Coverage error)之問題，亦即抽樣架構與目標母體之間具有落差，而根據此抽樣結構分析所得之統計資料，在推論統計時可能會產生誤差。由於本研究所欲探討之內容係為網路使用行為，而受試者為曾有或現有網路使用經驗者，故在抽樣結構與推論統計上，將基於涵蓋誤差之考量，盡量將問卷調查內容與目標母體維持一致性，並避免過度推論，以期減少上述研究產生之誤差。

其次，網路調查缺乏有效的抽樣結構，李政忠(2004)指出，在網路調查之情況下，研究者無法評估抽樣架構與實際母體之差異為何，因此也無法清楚得知涵蓋誤差的範圍。本研究對於此部分所產生之問題，除了以嚴謹的態度將研究母體侷限於網路使用者外，亦避免實際施測之內容過度推論至目標母體外，同時，更採取增加問卷樣本數之方式，以有效降低抽樣所產生的涵蓋誤差問題。

再者，網路問卷調查也包括非回應誤差(Nonresponse error)之缺點，所謂非回應誤差係問卷填答者或受訪者與拒絕接受受訪者在某些特質上具有差異，故這種差異所得出的樣本，在推論全體人口時會產生相當的誤差現象(Groves & Couper, 1998)。李政忠(2004)指出，問卷調查均會產生此一問題，特別係當問卷的回覆率很低時，更容易產生較大的誤差，但若能提高網路問卷調查之回覆率，將會降低樣本推論至母體時的誤差現象。網路調查研究雖然很難取得拒答率之分母，但本研究將以造訪問卷網頁或連結之人數，以及實際填答的受訪者數，盡可能地計算樣本的回覆率，以減少非回應誤差之現象。

最後，則是網路問卷之能見度及回復率之問題。網路問卷雖然回收時間快，但是相對而言回收率較低，因此，有關網路問卷之能見度及受試者之回復率係網路問卷調查的重要問題。本研究為有效解決此一問題，擬將網路問卷之相關連結網址或 QRcode 置於各大學校論壇、網路知名遊戲、ptt 論壇網站或透過各知名網路問卷調查平台進行調查，將問卷所能觸及到的人數最大化，以期獲得最大的填答率及最高的能見度。

本研究以 suveycake 網路問卷表單作為本研究編製之正式問卷。當填答者進入網路問卷填答初始頁面時，會先以文字說明本次網路問卷調查之研究目的、研究對象與相關填答說明，並告知受試者本問卷係採匿名設計，個人資料均保密，沒有任何填答風險，而填答內容僅以彙整的統計資訊呈現，不會揭露任何可資辨識之個人資料或是挪作他途，對於蒐集所得之資料亦遵守個人資料保護法之規定，在讓受試者能完整瞭解施測之目的與程序，並經受試者親自閱讀、同意後始進入問卷調查內容。

此外，有鑑於傳統問卷可能有題項漏填之情形，故研究者將所有題目均設定為必填題項，當受試者結束問卷之填答後，若程式發現有漏答之題目，程式將會自動告知受試者應補答題目，否則無法送出問卷資料，藉以提升問卷之完整度與施測之有效性。

第三節 抽樣技術與樣本特性

一、抽樣技術

本研究係探究不同性別間網路詐欺被害之影響因素，透過分析不同性別網路詐欺被害者之個人基本特性、網路生活型態、低自我控制特性、被害情境與機會等相關變項，以了解其網路詐欺被害之差異因素。在研究對象上，除了曾有網路詐欺被害經驗者外，亦將曾有或現有網路使用經驗之網路使用者納入本研究之研究母體，藉由分析不同性別之網路生活使用特性，可進一步分析不同性別網路使用者在網路生活型態之差異，並可藉此與具有網路詐欺被害經驗之網路使用者進行分析比較，深入探究不同性別網路詐欺被害之相關因素，故本研究將曾有或現有網路使用經驗者界定為研究之母群體，而根據 Insight-Xplorer 創世際市場顧問公司及國家通訊發展委員會(NCC)2019 年對於全體網路使用人數進行調查，相關統計資料依據「性別」及「年齡」變項整理如下表 3-3-1 所示:

表 3-3-1 2019 年 12 月我國整體網路使用人口數統計表

人口變項	類別	網路使用人口母體[1]	
		人數	結構百分比(%)
性別	男性	9,625,800	52.60
	女性	8,674,200	47.40
	總計	18,300,000	100.00
年齡	18 歲以下	786,900	4.30
	19-29 歲	4,084,560	22.32
	30-39 歲	3,965,610	21.67
	40-49 歲	4,101,030	22.41
	50-59 歲	3,385,500	18.50
	60 歲以上	1,976,400	10.80
	總計	18,300,000	100.00

資料來源：整理自 Insight-Xplorer 及國家通訊傳播委員會(NCC)

[1] 該調查係以內政部 2019 年 12 月台灣地區人口之性別、年齡及地區人口結構進行加權。

李政忠(2003)指出，由於網路問卷調查具有非隨機取樣之特性，故在抽樣上係屬於非隨機抽樣。在非隨機抽樣的方法中，包括便利抽樣(Convenience sampling)、立意抽樣(Purposive sampling)、配額抽樣(Quota sampling)及滾雪球抽樣(Snowball sampling)等方法。由於網路問卷調查中無法得知實際母群體，因而無法進行隨機抽樣，因此，本研究除了考量樣本選擇及調查執行之可行性及便利性外，亦考量具有高度同質性之網路使用人口樣本資料蒐集，故本研究係以非隨機抽樣方法之配額抽樣方法擇定受試對象。

此外，本研究為避免網路問卷調查存在樣本缺乏代表性之問題，故本研究係以分層抽樣之方式，依據財團法人台灣網路資訊中心(TWNIC)2019 年對於全台 2018 年上網人口分析調查之母體結構，控制抽取樣本當中之「性別」及「年齡」比例，並依各年齡分層比例計算，以計算出各分層配額抽樣之人數，並視為配額抽樣(Quota sampling)，藉以降低網路問卷樣本代表性不足之疑慮。

在分層抽樣之配額部分，首先以「年齡」作為抽樣數量配額之依據，根據各年齡層進行分層配額抽樣，並依據母體抽樣結構與抽取出之樣本結構，進行卡方適合度檢定，由下表 3-3-2 之檢定結果可得知，母體與樣本結構兩者並未有顯著差異(χ^2=.297 ; d.f.=5 ; p>.05)，代表樣本結構與母體結構一致，故在年齡分層上，樣本具有代表性。

表 3-3-2 本研究之年齡抽樣數量配額結構表

年齡	母體人數	母體結構百分比(%)	母體結構		樣本結構		卡方適合度檢定
			樣本數	百分比(%)	樣本數	百分比(%)	
18 歲以下	786,900	4.30	37	4.25	36	4.14	χ^2=.297 d.f.=5 p>.05
19-29 歲	4,084,560	22.32	194	22.30	202	23.24	
30-39 歲	3,965,610	21.67	189	21.73	191	21.95	
40-49 歲	4,101,030	22.41	195	22.41	193	22.17	
50-59 歲	3,385,500	18.50	161	18.51	156	17.93	
60 歲以上	1,976,400	10.80	94	10.80	92	10.57	
總計	18,300,000	100.00	870	100.00	870	100.00	

其次，本研究再以「性別」作為抽樣數量配額之依據，根據不同年齡層與性別進行分層配額抽樣，並依據母群體抽樣結構與抽取所得之樣本結構，進行卡方適合度檢定。由下表 3-3-3 之檢定結果可得知，母體與樣本結構兩者在不同性別之各年齡分層上並未有顯著差異，各分層結構經檢定結果 p 值均大於.05，代表樣本結構與母體結構一致，故本研究所抽取之樣本具有代表性。

表 3-3-3 本研究母體之性別、年齡分層抽樣數量配額結構表

年齡	性別	母體人數	母體結構百分比(%)	母體結構		樣本結構		卡方適合度檢定
				樣本數	百分比	樣本數	百分比	
18 歲以下	男性	457,500	2.50	22	2.53	20	2.30	χ^2=.228
	女性	329,400	1.80	15	1.72	16	1.84	d.f.=1
	總和	**786,900**	**4.30**	**37**	**4.25**	**36**	**4.14**	p>.05
19-29 歲	男性	2,126,460	11.62	101	11.61	102	11.72	χ^2=.191
	女性	1,958,100	10.70	93	10.69	100	11.50	d.f.=1
	總和	**4,084,560**	**22.32**	**194**	**22.30**	**202**	**23.22**	p>.05
30-39 歲	男性	2,117,310	11.57	101	11.61	103	12.19	χ^2=.324
	女性	1,848,300	10.10	88	10.12	88	9.77	d.f.=1
	總和	**3,965,610**	**21.67**	**189**	**21.73**	**191**	**21.96**	p>.05
40-49 歲	男性	2,124,630	11.61	101	11.61	107	12.30	χ^2=1.027
	女性	1,976,400	10.80	94	10.80	86	9.88	d.f.=1
	總和	**4,101,030**	**22.41**	**195**	**22.41**	**193**	**22.18**	p>.05
50-59 歲	男性	1,701,900	9.30	81	9.31	71	8.16	χ^2=1.089
	女性	1,683,600	9.20	80	9.20	85	9.77	d.f.=1
	總和	**3,385,500**	**18.50**	**161**	**18.51**	**156**	**17.93**	p>.05
60 歲以上	男性	1,098,000	6.00	52	5.98	49	5.63	χ^2=.158
	女性	878,400	4.80	42	4.82	43	4.94	d.f.=1
	總和	**1,976,400**	**10.80**	**94**	**10.80**	**92**	**10.57**	p>.05
性別總和	男性	9,625,800	52.60	458	52.64	455	52.30	χ^2=.041
	女性	8,674,200	47.40	412	47.36	415	47.70	d.f.=1
	總和	**18,300,000**	**100.00**	**870**	**100.00**	**870**	**100.00**	p>.05

二、樣本特性

本研究經由上述控制抽取樣本中之「性別」及「年齡」比例，並依各年齡分層依比例計算，計算出配額抽樣之人數後，共抽取 870 個樣本，以下茲就本研究全體調查樣本之人口特性分述如下:

(一)性別:調查樣本之性別部分，全體樣本中男性共占 455 位(52.3%)、女性占 415 位(47.7%)，顯示兩性間比例相近，此比例亦與整體網路使用人口比例相近。

(二)年齡:調查樣本之年齡分布，18 歲以下占 36 位(4.1%)、19 至 29 歲占 202 位(23.3%)30 至 39 歲占 191 位(22.0%)、40 至 49 歲占 193 位(22.2%)、50 至 59 歲占 156 位(17.8%)，以及 60 歲以上占 92 位(10.6%)。

(三)職業:職業分布部分，未就業(含退休)占 83 位(9.5%)、學生占 231 位(26.6%)、軍警公教人員(含老師)占 151 位(17.4%)、從事家庭管理占 64 位(7.4%)、服務及事務工作人員占 176 位(20.2%)、技術員及助理專業人員占 144 位(16.5%)、行政主管及經理人員占 21 位(2.4%)。

(四)收入:調查樣本之收入分布，未滿 1 萬元占 206 位(23.7%)、1 萬以上至 3 萬未滿占 224 位(25.7%)、3 萬以上至 6 萬未滿占 236 位(27.1%)、6 萬以上至 9 萬未滿占 156 位(17.9%)、9 萬以上至 12 萬未滿占 35 位(4.1%)、12 萬元以上占 13 位(1.5%)。

(五)教育程度:調查樣本之教育程度分布部分,國小(肄)畢業占 1 位(.1%)、國中(肄)畢業占 22 位(2.5%)、高中、高職(肄)畢業占 122 位(14.0%)、專科、大學(肄)畢業占 477 位(54.9%)、研究所(肄)畢業以上占 248 位(28.5%)，整體教育程度以專科、大學(肄)畢業占最大多數。

(六)婚姻狀況:調查樣本之婚姻狀況分布部分，單身占 419 位(48.2%)、未婚(非單身)占 191 位(22.0%)、已婚(含同居)占 224 位(25.7%)、離婚(含分居)占 20 位(2.3%)、喪偶占 9 位(1.0%)、再婚占 7 位(.8%)。

表 3-3-4 調查樣本個人基本特性分析(N=870)

人口特性	組別	調查樣本	
		人數	百分比(%)
性別	男性	455	52.3
	女性	415	47.7
年齡	18 歲以下	36	4.1
	19 至 29 歲	202	23.3
	30 至 39 歲	191	22.0
	40 至 49 歲	193	22.2
	50 至 59 歲	156	17.8
	60 歲以上	92	10.6
職業	未就業(含退休)	83	9.5
	學生	231	26.6
	軍警公教人員(含老師)	151	17.4
	從事家庭管理	64	7.4
	服務、事務工作人員	176	20.2
	技術員及助理專業人員	144	16.5
	行政主管及經理人員	21	2.4
收入	未滿 1 萬元	206	23.7
	1 萬以上至 3 萬未滿	224	25.7
	3 萬以上至 6 萬未滿	236	27.1
	6 萬以上至 9 萬未滿	156	17.9
	9 萬以上至 12 萬未滿	35	4.1
	12 萬元以上	13	1.5
教育程度	國小(肄)畢業	1	.1
	國中(肄)畢業	22	2.5
	高中、高職(肄)畢業	122	14.0
	專科、大學(肄)畢業	477	54.9
	研究所(肄)畢業以上	248	28.5
婚姻狀況	單身	419	48.2
	未婚(非單身)	191	22.0
	已婚(含同居)	224	25.7
	離婚(含分居)	20	2.3
	喪偶	9	1.0
	再婚	7	.8

三、施測場域

本研究之抽樣母體為曾有或現有網路使用經驗者，故係以網際網路作為問卷施測之主要場域。本研究係以 suveycake 網路問卷調查平台作為正式研究施測之工具，除了將問卷連結放置於該網路問卷平台網頁上外，亦將網址及連結張貼於各大學校之網路論壇、Ptt 電子公布欄、各社群媒體網站、網路購物看板及相關問卷調查平台，以期將問卷之能見度及觸及率最大化。此外，為避免網路調查問卷中有受訪者重複填答之情況發生，故本研究將系統設定為自動偵測重複填答 IP，並對於重複填答之樣本資料逕予刪除，以避免一人多填，造成填答樣本重複之情況產生。

四、施測流程

本研究採用網路問卷調查做為原始資料之蒐集工具，在量表之建構上，除參考以往有關網路詐欺被害理論與相關國內外之實證研究外，亦參酌國內外學者所編制之問卷。本研究為期能建構較高信效度之量表內容，故在正式問卷施測前，先進行二次問卷預試，並在二次問卷預試施測後，分別對於較低信效度之題項進行修正，並據以作為正式施測問卷，以下茲就本研究問卷施測流程分述如下:

(一)第一次預試

本研究在實施問卷調查前，先藉由相關文獻探討及國內外實證研究資料彙整之結果，預先擬定問卷初稿內容。由於本問卷部分內容係援引國外學者所編製之量表，故在題項之中文語意轉換上先以表面效度，對於初稿問卷題項中題意不清或較不適切之題目進行初步修改，並於修正完畢後，於 2019 年 11 月 2 日起將預試問卷之網頁連結置於各大學之網路論壇及社群網站中，不限制問卷回收日期，而係設定系統以回收數量最高 40 份為限，以進行問卷之第一次前測，並於 11 月 5 日止，共計回收有效問卷 40 份。

在第一次預試問卷結束後，隨即進行調查問卷之回收、資料之編碼、轉換以及問卷題項之信效度分析。在信度分析方面，各構面之內部一致性係數(Cronbach's α)大多介於 0.785 至 0.926，整體而言，各構面之題項間均具有較高之內部一致性，問卷題項中僅有「網路休閒與職業活動」構面之信度係數為 0.516，呈現較低的信度值。

在效度分析方面，各構面之特徵值(eigenvalue)均大於 1，且各題項之因素負荷量(factor loading)大多大於 0.6，整體而言具有較佳之效度，但在「網路休閒與職業活動」構面中之第一題(在過去一年內，您經常使用即時通訊軟體)之因素負荷量為 0.132，及「網路風險職業活動」構面中之第四題(在過去一年內，經常點擊即時通訊軟體檔案)之因素負荷量為 0.360 過低。

第一次預試問卷經由信效度分析後，多數構面及問卷題項均呈現較高信效度，僅在「網路休閒與職業活動」構面及上述兩個題項之信效度較低，故研究者對於構成此構面之所有題項進行重新修正及編制，並在此構面題項修正完畢後進行問卷之第二次預試，除對於題意不清或有疑義之題項進行檢驗外，亦再次考驗該構面題項之信效度。

(二)第二次預試

本問卷於第一次前測施測完畢、進行信效度分析後，除了對於信效度較低題項進行內容之修正、刪除及構面題項之重新編製外，亦針對第一次預試中，受試者在填答過程中對於問卷中不清楚或有疑義之題項進行內容之再次修正。針對上述內容修正完畢後，研究者於 11 月 6 日將問卷之連結置於網路社群網站中，進行第二次預試問卷之施測，同樣亦未限制問卷回收日期，而係設定樣本回收至 30 份即停止回收，並於 11 月 8 日止，共計收取有效問卷 30 份。

第一次預試分析後，研究者對於信效度較低之「網路休閒與職業活動」構面及部分題項進行內容修正及題項之重新編製，除刪除部分較低信效度之題項外，亦於參酌相關文獻後增加該構面題項，並進行第二次預試，而第二次預試，除再次檢視是否仍有題意不清之題項外，亦對於上述修正後構面之問卷題項再次進行信效度之檢驗。

在信度部分，該構面之內部一致性係數(Cronbach's α)從 0.516 提升至 0.857，整體信度顯著提升。在效度部分，除了該構面之特徵值(eigenvalue)大於 1 外，建構該構面之各題項的因素負荷量(factor loading)，亦約介於 0.696 至 0.823，整體效度相較於第一次預試而言已顯著提升。第二次問卷預試後，各構面題項已具有較佳信效度，故以此做為正式網路問卷調查內容，並進行網路問卷之正式施測。

(三)正式問卷施測

本研究所編製之正式網路問卷於 2019 年 11 月 15 日至 2020 年 1 月 15 日期間進行正式網路調查,並將網路問卷連結放置於網際網路平台上,讓受試者自行於網路上填答。此外，研究者於 2019 年 11 月 15 日起，便開始在網路上發布本研究問卷之調查訊息，同時在各大電子公佈欄(Bulletin Broad System, BBS)、Dcard 網路論壇、各大學網路論壇、各遊戲社群網站及各網路社群媒體上張貼網路問卷廣告,讓網路使用者能看到本問卷之網址，期望讓本研究問卷所觸及之人數達到最大化，且為有效提升受測者之填答意願，本研究於問卷回收完畢後隨機抽取 50 名受訪者,提供便利超商之商品折價卷各 100 元。

本次網路問卷調查期程共計 2 個月，本研究於問卷施測完畢後，隨即進行問卷回收與整理，除剔除固定答案之無效問卷外，亦考量網路問卷中可能有一人填具多份問卷之重複填答之情況，故除系統設定為偵測重複 IP，對於重複 IP 之問卷視為無效問卷，並設定系統逕予刪除。本研究共計收取 925 份問卷，經上述固定答案或重複 IP 者篩選進行刪除後,共計刪除 55 份無效問卷,並以此 870 份有效問卷進行後續資料處理與分析。有關本研究問卷調查與資料分析流程，如下圖 3-3-1 所示:

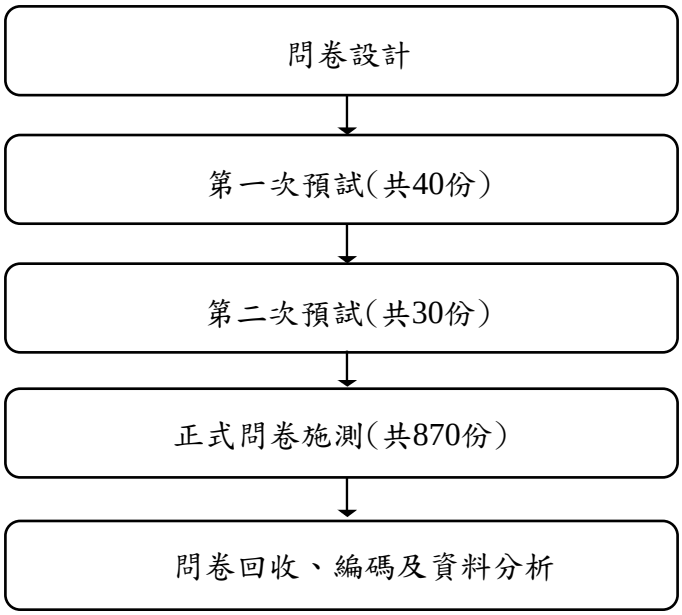

圖 3-3-1 問卷調查與資料分析流程

第四節 研究工具與概念測量

一、研究工具

本研究所使用之研究工具，係根據過去有關網路詐欺犯罪與被害之官方統計資料、深度訪談分析研究結果，以及相關犯罪學理論及國內外文獻資料，並參酌黃俊祥(2008)所編製之「網路生活經驗調查表」後所修改編製之「網路生活型態問卷」(如附錄)。

本研究問卷於初稿設計完畢後，先以表面效度對於問卷中較不適切之題項進行內容之討論與修改。其次，為有效提升本量表之信度與效度，於問卷修改後共施以二次前測，以檢視是否有題意不清或重複詢問之情形，並於二次前測施測完畢後，針對較低信效度之題項內容進行修正，並於修正完畢後，以此問卷作為本研究施測之正式問卷。

量表信度方面，主要係以 Cronbach's α 係數，作為本量表信度考驗之主要方法，DeVellis(2003)指出，各分量表之 α 係數必須大於 0.6，始認為該量表具有良好之一致性及穩定性。量表效度分析部分，在取樣適切性方面，係以 K-M-O 量數(Kaiser-Meyer-Olkin measure of sampling adequacy)檢驗資料是否適合進行因素分析，Dziuban 與 Shirkey(1974)認為，K-M-O 值在 0.7 以上者，代表資料適合進行因素分析。本研究為深入了解各構面變項之間的潛在結構，遂於 K-M-O 值檢驗後，以探索式因素分析中之主成分分析法(Principle Component Analysis, PCA)進行因素之萃取，並經最大變異法進行直交轉軸後，將原始變項簡化為數個貢獻度較高之構面，並對簡化後之構面重新命名。

量表之初步建構效度部分，係由收斂效度及區別效度所組成。本研究之收斂效度係根據 Kaiser(1958, 1970)所提出較高收斂效度量表之四個評斷準則，以探索式因素分析法檢視各構面之衡量題項是否皆可收斂於同一共同因素下，並萃取出特徵值(Eigenvalues)大於 1 之因素、選取各因素構面中因素負荷量(Factor loading)大於 0.6 之變項，並檢驗各題項建構構面之累積解釋變異量是否均達 50%以上，以期能得到較高收斂效度之量表，而量表之區別效度係根據探索式因素分析轉軸後之成分矩陣，檢視各題項在非其所屬之因素構面中是否具有較低之因素負荷量(小於 0.5)，以檢驗各構面是否具有區別效度。經檢視後，本研究建構之量表均符合高信效度量表之準則，故依此進行後續分析。

二、概念測量

依據前述研究架構，本研究問卷測量概念共分為五個部分，第一部分係為了解網路使用者在日常網路使用中網路使用特性、網路使用行為及經驗之「網路生活型態分量表」、第二部分為了解網路使用者在上網過程中有無他人監控、網路上的不法誘因是否出現及其網路偏差和犯罪動機的出現等要素，以探究網路情境與機會之「被害情境機會分量表」、第三部分為瞭解網路使用者自我控制程度之「低自我控制分量表」、第四部分為調查網路使用者是否曾有網路詐欺被害經驗之「網路詐欺犯罪被害分量表」，第五部分係蒐集網路使用者個人基本特性之「個人基本特性分量表」，以下茲將本問卷各研究變項之測量概念及探索式因素分析與信度分析之結果說明如下:

(一)網路生活型態分量表

Whitty(2019)指出，在網路詐欺被害之研究中，網路使用者之網路生活型態，係為被害調查的重要項目，因此，問卷的第一部分係為了解個人日常生活中的網路使用情形，本研究構面除參考國外學者 Choi(2008)、Choi(2017)、Chen 等人(2017)、Pratt 等人(2010)、Reyns(2015)之研究外，亦參酌國內黃俊祥(2007)所編製之「網路生活型態分量表」後，對於網路生活型態變項共設計 27 個題目，其中各包括類別變項 7 題及連續變項 20 題，有關類別變項之相關測量包括:每次上網時數、每周上網次數、平日上網時段、假日上網時段、接觸網路時間、最常上網地點及最常上網原因等 7 個變項。

網路生活型態之態度分量表部分，共計 20 題，各題項均採取 Likert 四點量表且均為 4 選 1 答式的題項，並以經常、偶爾、很少和從未等四個等級測量之，回答「經常」給 4 分、回答「偶爾」給 3 分、回答「很少」給 2 分、回答「從未」給 1 分，而分量表加總後的總得分越高，代表個人以網路從事各項活動之機會越高。

本分量表 K-M-O 值為.847，代表取樣適切性佳，經探索式因素分析之主成分分析法進行因素之萃取，並經最大變異法轉軸後，共萃取出 4 個因子，各因子各為 5 題、累積總解釋變異量為 59.58%、分量表信度之內部一致性 Cronbach's α 係數為.758。

經考量各因子所包含之題項內容後，將四個因子依序命名為「網路風險職業活動」、「網路職業活動」、「網路風險休閒活動」及「網路休閒活動」，並依據此四個構面作為網路生活型態概念之觀察變項，進行信度分析，以下就探索性因素分析結果分述如下:

1.網路風險職業活動

經轉軸後所萃取出之因素 1 命名為「網路風險職業活動」，該因素係由分量表當中的第 16 至 20 題所構成，特徵值為 3.930、解釋變異量為 19.651%、各子題之因素負荷量介於.731 至.879 間、內部一致性係數(Cronbach's α)值為.897，顯示該本分量表具有高內部一致性與穩定性。所謂「網路風險職業活動」概念，係指網路使用者日常網路使用過程中從事具有風險性的網路職業活動行為。

2.網路職業活動

經轉軸後所萃取出之因素 2 命名為「網路職業活動」，該因素係由分量表中的第 6 題至第 10 題所構成，特徵值為 2.804、解釋變異量為 14.020%、各子題之因素負荷量介於.587 至.815 間、內部一致性係數(Cronbach's α)值為.809，而所謂「網路職業活動」概念，係指網路使用者日常使用網路中所從事之各項職業活動行為。

3.網路風險休閒活動

經轉軸後所萃取出之因素 3 命名為「網路風險休閒活動」，該因素係由分量表當中第 11 至 15 題所構成，特徵值為 2.613、解釋變異量為 13.066%、各子題之因素負荷量介於.544 至.778 間、內部一致性係數(Cronbach's α)值為.775，而所謂「網路風險職業活動」概念，係指網路使用者日常使用網路中從事具有風險性的休閒活動行為。

4.網路休閒活動

經轉軸後所萃取出之因素 4 命名為「網路休閒活動」，該因素係由分量表當中的第 1 題至第 5 題所構成，特徵值為 2.570、解釋變異量為 12.852%、各題項中之因素負荷量約介於.556 至.747 間、內部一致性係數(Cronbach's α)值為.710，而所謂「網路休閒活動」概念，係指網路使用者日常使用網路中所從事之各種休閒活動行為。有關網路生活型態分量表經探索性因素分析及信度分析後之詳細分析結果，如下表 3-4-1 所示:

表 3-4-1 網路生活型態分量表之因素分析與信度分析

因素名稱	因素構面內容[2]	轉軸後之因素負荷量[3]			
		因素 1	因素 2	因素 3	因素 4
網路風險職業活動	18.您經常點擊不明來源電子郵件的相關網頁連結	.898			
	17.您經常點擊不明來源電子郵件的附件檔案	.891			
	20.您經常寄送信件至不明來源的電子郵件	.824			
	16.您經常點擊不明來源的電子郵件	.804			
	19.您經常點擊經由即時通訊軟體所接收到的未知來源檔案或附件	.731			
網路職業活動	7.您經常寄送電子郵件		.815		
	8.您經常利用網路來進行檔案傳輸		.777		
	6.您經常檢查您的電子郵件		.777		
	10.您經常在網路上下載資料		.661		
	9.您經常利用網路來搜尋資料		.587		
網路風險休閒活動	13.您經常從網站上下載免費音樂			.778	
	12.您經常從網站上下載免費遊戲			.775	
	14.您經常從網站上下載免費電影			.745	
	11.您經常瀏覽色情網站			.646	
	15.您經常從網站上下載不明來源檔案			.544	
網路休閒活動	2.您經常使用網路社群媒體				.747
	1.您經常使用即時通訊軟體與他人溝通互動				.708
	5.當您無聊時經常花時間上網				.700
	4.您經常在網路上瀏覽或觀看新聞				.644
	3.您經常從事網路購物行為				.556
K-M-O 值=.847					
題目數(number)		5	5	5	5
特徵值(Eigenvalue)		3.930	2.804	2.613	2.570
內部一致性係數(Cronbach's α)		.897	.809	.775	.710
解釋總變異量百分比(% of variance)		19.651	14.020	13.066	12.852
累積解釋總變異量百分比(% of variance)		19.651	33.670	46.736	59.588

[2] 各因素構面題項均係依據因素負荷量(Factor Loading)之大小進行排序。

[3] 為有利於資料之判讀及詮釋，故表格中未顯示絕對值小於.40 之因素負荷量。

(二)被害情境與機會分量表

問卷的第二部分旨在透過情境與機會之角度,探究個人被害時之情境及機會因素,本研究構面除了參考國外學者 Bossler & Holt(2009)、Choi(2008)、Chen 等人(2017)、Leukfeldt 和 Yar(2016)研究外,亦參酌國內陳怡璇(2007)編製之「網路遏阻監控分量表」,對於被害情境與機會構面共設計 21 個題目,各題項均採取 Likert 四點量表且為 4 選 1 答式的題項,並以經常、偶爾、很少和從未等四個等級測量之,回答「經常」給 4 分、回答「偶爾」給 3 分、回答「很少」給 2 分、回答「從未」給 1 分,而分量表中共分為「網路偏差動機」、「社會監控」、「物理監控」及「網路負面誘因」四個概念,網路安全監控部分,分量表加總後的總得分越高,代表受訪者在網路使用的過程中所受到的物理、社會監控程度較高,在網路負面誘因及網路偏差動機部分,分量表加總後的總得分越高,代表受訪者在網路使用的過程中,具有較高的負面誘因及偏差動機。

本分量表 K-M-O 值為.842,代表取樣適切性佳,經探索式因素分析之主成分分析法進行因素之萃取,並經最大變異法轉軸後,共萃取出 4 個因子、累積總解釋變異量為 60.528%,量表信度之內部一致性 Cronbach's α 係數為.760,顯示本分量表具有高內部一致性與穩定性。

經考量各因子所包含之題項內容後,將四個因子依序分別命名為「網路偏差動機」、「社會監控」、「物理監控」及「網路負面誘因」,並依此四個構面作為被害情境與機會概念之觀察變項,進行信度分析,以下就探索性因素分析所萃取出之四個因子分述如下:

1.網路偏差動機

經轉軸後所萃取出之因素 1 命名為「網路偏差動機」,該因素係由分量表中的第 15 至 21 題所構成,特徵值為 4.417、解釋變異量為 21.033%、各子題之因素負荷量介於.536 至.878 間、內部一致性係數(Cronbach's α)值為.835,顯示該本分量表具有高內部一致性與穩定性,而所謂「網路偏差動機」係指網路使用者在網路使用的過程中,曾經出現網路偏差或是具曾有犯罪動機之情形。

2.社會監控[4]

經轉軸後所萃取出之因素 2 命名為「社會監控」，該因素係由分量表當中的第 1 至 5 題構成，特徵值為 2.907、解釋變異量為 13.842%、各子題因素負荷量介於.635 至.813 間、內部一致性係數(Cronbach's α)值為.818，而所謂「社會監控」(Social guardianship)概念係指個人在網路使用過程中，除了本人之外的第三方有能力監控者是否存在現場。

3.物理監控

經轉軸後所萃取出之因素 3 命名為「物理監控」，該因素係由分量表中第 6 題至第 10 題所構成，特徵值為 2.784、解釋變異量為 13.258%、各子題因素負荷量介於.624 至.795 間、內部一致性係數(Cronbach's α)值為.797，而所謂「物理監控」(Physical guardianship)，係指透過物理環境及物理安全設備的強化或是個人的風險意識程度（網路風險技術知識）及其所採取降低風險發生，以阻礙犯罪者獲得標的物機會之各種預防措施。

4.網路負面誘因

經轉軸後所萃取出之因素 4 命名為「網路負面誘因」，該因素係由分量表中的第 11 題至第 14 題所構成，特徵值為 2.603、解釋變異量為 12.395%、各子題之因素負荷量介於.721 至.831 間、內部一致性係數(Cronbach's α)值為.813，而所謂「網路負面誘因」，係指網路使用者在使用網路的過程中，曾經接收或看到非法或偏差誘因訊息的機會，進而提供機會而造成網路偏差行為的發生。有關被害情境與機會分量表經探索性因素分析及信度分析後之詳細分析結果，如下表 3-4-2 所示:

[4]根據 Cohen 和 Felson(1979)日常活動理論之定義，有能力之監控者係由「社會監控」(Social guardianship)及「物理監控」(Physical guardianship)兩個概念所構成，而此兩個概念又可進一步轉化為 Choi(2008)研究中所稱之「數位監控」(Digital Guardianship)概念，因此，「社會監控」及「物理監控」概念可進一步構成「網路安全監控」概念，而所謂「網路安全監控」，係指有能力監控個人從事網路行為的相關人、事、物，抑或是阻礙具有犯罪動機之犯罪者從事傷害、攻擊或獲得標的物的能力。惟本研究經探索式因素分析之結果後，共萃取出兩個因子，並依據題項內容分別命名為「社會監控」及「物理監控」，故未將社會監控及物理監控合併為網路安全監控概念，特此說明。

表 3-4-2 被害情境與機會分量表之因素分析與信度分析

因素名稱	因素構面內容[5]	轉軸後之因素負荷量[6]			
		因素 1	因素 2	因素 3	因素 4
網路偏差動機	19.您曾經想利用網路詐騙別人財物	.878			
	20.您曾經想利用網路從事網路賭博	.870			
	21.您曾經想利用網路從事非法交易	.868			
	17.您曾經想在未經所有者許可的情況下，在其電腦中增、刪任何資訊	.798			
	16.您曾經想在不知情或的情況下使用他人的帳戶或文件	.705			
	15.您曾想利用網路干擾他人網路使用	.675			
	18.您曾經想利用瀏覽色情網站或援交	.536			
社會監控	4.您上網時，同學外的朋友會在您身邊		.813		
	3.您上網時，同學(或同事)會在您身邊		.807		
	2.您上網時，兄弟姐妹會在您身邊		.761		
	5.您上網時，師長(或上司)會在您身邊		.760		
	1.您上網時，父母會在您身邊		.635		
物理監控	7.您的電腦有定期更新防毒軟體			.795	
	8.您對於不同網路帳號會使用不同密碼			.776	
	6.您對於不同的電腦會安裝防毒軟體			.764	
	9.您會定期更改個人網路帳號的密碼			.722	
	10.您會注意到在網路的空間中該留下何種個人資訊			.624	
網路負面誘因	12.您曾經在網路上看到網路援交訊息				.831
	11.您曾經在網路上看網路賭博的訊息				.770
	14.您曾經在網路上看到買賣盜版軟體的訊息。				.745
	13.您曾經在網路上看到買賣違禁物品的訊息。				.721
	K-M-O 值=.842				
	題目數(number)	7	5	5	4
	特徵值(Eigenvalue)	4.417	2.907	2.784	2.603
	內部一致性係數(Cronbach's α)	.877	.818	.797	.813
	解釋總變異量百分比(% of variance)	21.033	13.842	13.258	12.395
	累積解釋總變異量百分比(% of variance)	21.033	34.875	48.133	60.528

[5] 各因素構面題項均係依據因素負荷量(Factor Loading)之大小進行排序。

[6] 為有利於資料之判讀及詮釋，故表格中未顯示絕對值小於.40 之因素負荷量。

三、低自我控制分量表

問卷的第三部分則是瞭解網路使用者之自我控制程度。量表內容係根據 Gottfredson 和 Hirschi(1990)對於低自我控制者所具有之特徵，並參考國外學者 Chen 等人(2017)、Holt 等人(2008)、Holtfreter 等人(2010)、Grasmick 等人(1993)、國內許春金和孟維德(1997)、黃俊祥(2007)等研究中關於低自我控制之量表所編製而成。

Schreck 等人(2012)指出，由於不同的被害類型具有不同的根本原因，故自我控制效果之大小可能會因不同被害類型而異。Holt 等人(2008)研究中指出，過去最常使用之 Grasmick 等人(1993)所建構之自我控制量表，其效度受到許多實證研究質疑，多數研究發現該量表對於同一群受試者中有極高的歧異性(DeLisi, Hochstetler, & Murphy, 2003; Higgins & Tewksbury, 2006; Marcus, 2003, 2004; Wiebe, 2004)。此外，若是將全部的自我控制指標應用於特定類型的偏差和犯罪被害時，可能會帶來大量的測量誤差，造成研究產生偏誤，因此在其研究中僅根據能有效反應詐欺風險的項目進行其量表題項之建構。

Gottfredson 和 Hirschi(1990)明確指出，自我控制的兩個面向包括對「風險行為」和「立即滿足」的傾向，而多數研究亦指出，此兩個層面係被害行為的強力預測因子(Arneklev et al., 1993; Baron et al., 2007; Kerley et al., 2008; Lagrange & Silverman, 1999; Longshore et al., 1996; Ribeaud & Eisner, 2006)。故在此兩個面向的測量上，Holt 等人(2008)研究參考以往 Baumeister(2002)、Van 和 Benson(1997)及 Van 和 Mason(2001)詐欺被害研究中有關詐欺被害風險概念所建構之量表而編製而成，並認為其建構之量表具有高信效度，能準確預測詐欺被害者之自我控制程度。因此，本研究於低自我控制之測量方面，除依照 Holt 等人(2008)研究所建構之量表外，亦參酌過去有關實證研究中所指出網路詐欺被害者所具有的被害特質後所編製之分量表。

此外，由於低自我控制變項係屬抽象概念之檢驗，故須針對操作化過程及信、效度分析加以說明。該變項於問卷調查中，係衡量受試者個人日常生活經驗與個人性格特質中之低自我控制傾向。本研究藉由因素分析萃取重要因子，俾更細緻地呈現低自我控制變項對依變項之影響。

本分量表對於低自我控制構面設計 12 個題目，測量內容包括「衝動性」、「冒險性」、「投機性」等三個概念，每一概念各包含 4 題，並採用李克特(Likert)四點態度量表，將各題分為「非常不同意」、「不同意」、「同意」、「非常同意」四個等級測量，計分方式分別為 1、2、3、4 分，在問卷中得分總計越高者，其自我控制能力越低。

本分量表 K-M-O 值為.845，代表取樣適切性佳，經探索式因素分析之主成分分析法進行因素之萃取，並經最大變異法轉軸後，共萃取出 3 個因子、累積總解釋變異量為 71.785%，分量表信度之內部一致性 Cronbach's α 係數為.844，顯示本分量表具有高度內部一致性與穩定性。

經考量各因子所包含之題項內容、Gottfredson 和 Hirschi(1990)及多數學者對於網路詐欺所建構之低自我控制指標，將 3 個萃取出因子依序分別命名為「衝動性」、「投機性」及「冒險性」，並依此 3 個構面作為建構低自我控制概念之觀察變項，進行信度分析，以下就探索性因素分析所萃取出之 3 個因子分述如下:

1.衝動性

經轉軸後所萃取出之因素 1 命名為「衝動性」，該因素係由量表中的第 1 題至第 4 題所構成，特徵值為 3.174、解釋變異量為 26.447%、各題項中所得之因素負荷量介於.858 至.895 間、內部一致性係數(Cronbach's α)值為.912。

2.投機性

經轉軸後所萃取出之因素 2 命名為「投機性」，該因素係由量表中的第 9 至 12 題所構成，特徵值為 2.744、解釋變異量為 22.866%、各題項中所得之因素負荷量介於.811 至.820 間、內部一致性係數(Cronbach's α)值為.844。

3.冒險性

經轉軸後所萃取出之因素 3 命名為「冒險性」，該因素係由量表中的第 5 至 8 題所構成，特徵值為 2.697、解釋變異量為 22.472%、各題項中之因素負荷量介於.767 至.847 間、內部一致性係數(Cronbach's α)值為.830。有關低自我控制分量表經探索性因素分析及信度分析後之詳細分析結果，如下表 3-4-3 所示:

表 3-4-3 低自我控制分量表之因素分析與信度分析

因素名稱	因素構面內容[7]	轉軸後之因素負荷量[8]		
		因素 1	因素 2	因素 3
衝動性	4.生活做些簡單的事給您無窮的樂趣	.895		
	3.您會因為眼前的立即快樂而較少考慮以後才會發生的事	.873		
	2.有時您無法阻止自己做某事,即使您知道這是錯的	.868		
	1.您經常在不考慮所有選擇的情況下採取行動	.858		
投機性	10.您會逃避您認為是比較困難的事情		.820	
	11.您不喜歡艱鉅且挑戰極限的任務		.820	
	12.您會關心眼前即將發生的事，較少考慮以後才會發生的事		.817	
	9.只要有獲得報酬的機會,您就會進行投資行為		.811	
冒險性	7.有時候您會覺得做些惹麻煩的事反而刺激			.847
	6.刺激跟冒險對您來說比安全更重要			.820
	5.您會做些有點冒險的事情來考驗一下自己			.781
	8.您偶爾會進行風險性的金融投資			.767
	K-M-O 值=.845			
	題目數(number)	4	4	4
	特徵值(Eigenvalue)	3.174	2.744	2.697
	內部一致性係數(Cronbach's α)	.912	.844	.830
	解釋總變異量百分比(% of variance)	26.447	22.866	22.472
	累積解釋總變異量百分比(% of variance)	26.447	49.313	71.785

[7] 各因素構面題項均係依據因素負荷量(Factor Loading)之大小進行排序。

[8] 為有利於資料之判讀及詮釋，故表格中未顯示絕對值小於.40 之因素負荷量。

四、網路詐欺犯罪被害分量表

問卷的第四部分內容係參考黃俊祥(2007)、陳怡璇(2007)、葉雲宏(2008)相關研究，與吳嫦娥、蔡麗滿(2004)所編「台北市少年使用網路經驗問卷調查」量表所編製而成的網路詐欺犯罪被害分量表，共計 15 題，旨在瞭解個人受到網路詐欺被害之相關因素，其中包括:個人是否曾經被害、被害次數、被害類型、是否與加害者互動、損失金額及被害原因等 6 個變項。有關本分量表之測量內容如表 3-3-4 所示:

表 3-4-4 網路詐欺犯罪被害分量表之測量內容

變項名稱	測量尺度	測 量 內 容
是否被害	名義尺度	請問您最近一年是否曾經有網路詐欺犯罪被害的經驗?
被害次數	等距尺度	請問您最近一年網路詐欺被害次數?
被害類型	名義尺度	請問您最近一次所遭遇的網路詐欺犯罪被害型態為何?
是否與加害者互動	名義尺度	請問您最近一次的網路詐欺犯罪被害，您跟加害者的關係為何?
	名義尺度	請問您最近一次的網路詐欺犯罪被害，是否與加害者互動?
	名義尺度	請問您最近一次的網路詐欺犯罪被害，係透過何種管道與加害者互動?
損失金額	次序尺度	請問您最近一次網路詐欺犯罪被害損失之總金額為多少?
	名義尺度	請問您最近一次網路詐欺犯罪被害的交易方式為何
被害原因	名義尺度	請問您最近一次的網路詐欺犯罪被害，您覺得自己被害的原因為何?

五、個人基本特性分量表

本問卷之第五部分為個人基本特性分量表，本量表係參考黃俊祥(2007)、陳怡璇(2007)、國外 Leukfeldt 和 Yar(2016)等人之問卷編製而成，共計 6 題。本分量表係對於網路使用者之性別、年齡、職業、收入、教育程度及婚姻狀況等個人基本背景變項進行調查，以探討網路使用者個人基本特性變項與網路詐欺被害之關聯性。有關本分量表之測量變項及其內容如表 3-3-5 所示:

表 3-4-5 個人基本特性分量表之測量內容

變項名稱	測量尺度	測 量 內 容
性別	名義尺度	(1)男 (2)女
年齡	次序尺度	(1) 18 歲以下 (2) 19 至 29 歲 (3) 30 至 39 歲 (4) 40 至 49 歲 (5) 50 至 59 歲 (6) 60 歲以上
職業	名義尺度	(1)未就業(含退休) (2) 學生 (3) 軍警公教人員 (4) 從事家庭管理 (5) 服務、事務工作人員 (6) 技術員及助理專業人員 (7)非技術工、體力工 (8) 行政主管及經理人員 (9)其他(請說明：)
收入	次序尺度	(1)未滿 1 萬元 (2)1 萬以上至 3 萬未滿 (3)3 萬以上至 6 萬未滿 (4)6 萬以上至 9 萬未滿 (5)9 萬以上至 12 萬未滿 (6)12 萬以上
教育程度	次序尺度	(1) 國小(肄) 畢業 (2) 國中(肄) 畢業 (3) 高中、高職(肄) 畢業 (4) 專科、大學(肄) 畢業 (5) 研究所(肄) 畢業以上 (6) 其他(請說明：)
婚姻狀況	名義尺度	(1) 單身 (2) 未婚(非單身) (3)已婚(含同居) (4) 離婚(含分居) (5) 喪偶 (6)再婚 (7) 其他(請說明：)

第五節 資料處理與分析

在正式網路問卷回收完畢後，本研究之量化分析主要係透過 SPSS of Window 23.0 電腦套裝軟體對於網路問卷資料進行資料處理與分析。以下茲就本次研究所使用之主要統計分析方法分別敘述如下：

一、描述性統計(Descriptive Statistics)

本研究以次數分配、百分比、平均數及標準差等統計方法進行描述性統計分析，以分析不同性別之網路使用者在各年齡、職業、收入、教育程度及婚姻程度等類別變項及研究中各連續變項之分布情形。

二、探索性因素分析(Exploratory Factor Analysis)

因素分析主要係主要在檢驗施測之量表是否具有建構效度，當因素分析後的特徵值(Eigenvalue)大於 1 時，表示測量變項可以組成共同概念並進行有效測量。本研究係以因素分析法中之主成分分析法進行因素的萃取，並以最大變異轉軸法(Varimax Rotation)萃取因素負荷量較高之題項，組成各分量表，以檢驗並提高各分量表之效度。

三、信度分析(Reliability Analysis)

信度，係指在同樣或類似的條件下，經多次分析操作後所得到穩定或一致的結果。本研究以 Cronbach's α 係數作為考驗各分量表內部一致性之指標。若 Cronbach's α 係數愈高，表示該量表之各題目性質與整個量表趨於一致，也就代表以該量表所建構而成之問卷有較高的信度。Nunnally(1967)指出，Cronbach's α 係數小於 0.3 者為低信度，不被接受，而係數為 0.7 以上者為可接受範圍，並可得知該量表具有中度以上之內部一致性。

四、卡方（χ^2）檢定(Chi-square Test)

卡方檢定係用以檢驗兩個類別變項或次序尺度變項之間的關聯性，當觀察值與期望值的差異越小，χ^2值愈小，越不具統計上的意義（即無關聯性），但差異愈大，χ^2值愈大，愈具有統計上的意義（即有關聯性）。本研究以卡方檢定對網路使用者之個人基本特性及網路詐欺被害進行獨立性檢定，並檢定不同性別之網路使用特性是否有顯著差異。

五、獨立樣本 t 檢定(Independent Sample t test)

獨立樣本 t 檢定用於二個分組變項在連續變項中之平均數差異檢定，主要以平均數差異與隨機差異之比值來決定統計顯著性。以本研究為例，例如檢驗網路詐欺被害者與一般網路使用者在低自我控制、網路生活型態及被害機會與情境等連續變項上是否具有顯著差異，或檢驗不同性別網路使用者在低自我控制、網路生活型態及被害機會與情境等連續變項上是否具有顯著差異。

六、相關分析（Correlation Analysis）

在連續變項之相關分析中，本研究係以皮爾森積差相關(Pearson's product-moment correlation)來檢驗兩個連續變項間是否具有顯著相關性，以本研究而言，係以皮爾森積差相關來檢驗研究構面當中各分量表之間的相關性。此外，對於本研究中二分類別變項與連續變項，以及兩個二分類別變項之顯著相關性，則以點二系列相關(point-biserial correlation)加以檢驗，例如檢驗性別與各連續變項之相關性、檢驗性別與網路詐欺被害與否之關聯性。

七、二元邏輯斯迴歸模型（Binary Logistic Regression Model）

在傳統線性迴歸分析中，自變數與依變數通常是連續變數，但若依變項為間斷變數時，則因殘差未符合常態性分配及依變項預測機率值無法介於 0 至 1 之間，而須採用邏輯斯迴歸模型(Logistic Regression Model)。在邏輯斯迴歸模型中，依變項係為間斷變項，而根據依變項之類別，又可分為二元(Binary)、次序(Ordered)及多項(Multinomial)邏輯斯迴歸，自變項可為連續變項或間斷變項，但間斷變項須先轉化為虛擬變項，並採用最大概似估計法(Maximum likehood estimation，簡稱 MLE)作為模型估計之方法。

本研究之依變項係為被害與否之二分類間斷變項，故採用二元邏輯斯迴歸模型進行分析，除了以 Hosmer-Lemeshow 檢定統計量對於整體迴歸模型進行配適度之考驗外，亦在不同解釋模式中加入不同觀察變項，比較各模型間-2LL 值(-2 對數概似值)、χ^2 值之改變程度及 Cox & Snell R^2、Nagelkerke R^2 值之高低，以建構最合適的被害解釋模型。

此外，在迴歸模型之解釋部分，各自變項對於依變項解釋力之高低，係以 Wald 值作為判斷指標，越重要之解釋變項其 Wald 值越高，而各變項之解釋比例則以勝算比(Odds ratio)機率比值 EXP(B)，來計算自變數每增加一個單位，被害事件相對於未被害之事件機率增加之可能性。

八、卜瓦松迴歸模型（Poisson Regression Model）

有關本研究之依變項包括「是否被害」之二分類間斷變項及分析被害次數之計數型資料，在二分類間斷變項部份，係以二元邏輯斯迴歸模型(Binary Logistic Regression Model)進行資料之分析，而在離散計數型(Count)資料之處理中，則以卜瓦松迴歸模型(Poisson Regression Model, PRM)進行資料之分析及處理。

在離散計數型資料之迴歸分析中，包括 Poission 迴歸模型、廣義 Poission 迴歸模型、零膨脹 Poission 迴歸模型(Zero-inflated Poission Regression Model)及負二項迴歸模型。在許多離散型資料迴歸模型中，必須根據資料之離散程度，來選擇該適用何種迴歸模型，其中，當資料呈現過度分散(Over-dispersion)時，需以負二項迴歸模型(Negative Binomial Regression Model, NBRM)進行分析，若資料呈現均等分散(Equi-dispersion)或低度離散(Under-dispersion)之狀況，則以卜瓦松迴歸模型加以處理。

經離散性檢定後發現，本研究所建構之模型呈現低度離散(Under-dispersion)情況，故本研究係以卜瓦松迴歸模型對於離散計數型資料進行分析。此外，卜瓦松迴歸模型大多用於稀少且間斷型之依變數(反應變數)資料，例如:個數、次數，並根據某一時間內已發生的次數據以推估未來時間可能發生的行為，故本研究以卜瓦松迴歸模型進行分析並預估被害者在未來時間可能被害次數之機率。

第六節 研究倫理

本研究於研究進行的過程中均恪遵研究倫理之原則，依據 Babbie(2015)、Berg(2001)、Hagan (2003)、Ruane(2007)及中華民國犯罪學學會研究倫理規範(Code of Ethics, Taiwan Society of Criminology)，臚列本研究所涉及之相關研究倫理原則包括:告知後同意與自願參與原則、匿名及保密原則、不傷害研究對象原則及真實呈現研究報告之原則，以下茲就上述倫理原則分述如下:

一、告知後同意與自願參與原則

告知後同意，或者稱為知情同意(Informed Consent)與自願原則，係一項重要的研究倫理規範，指研究者必須使受研究者能充分了解研究所可能產生之風險，進而自主決定是否參與研究。知情同意之核心原則是「尊重」及「自主」，尊重原則係指研究者必須尊重研究對象、誠實告知研究所可能產生之風險及弊端，不得強迫或欺騙他人參與研究。自主原則係指在研究進行過程中，研究對象可自主選擇隨時離開或中止研究，具有自主選擇的權利，而不因此受到任何的懲罰或喪失其原有的權利。

本研究於問卷施測前，於問卷之首頁中先介紹研究人員、此次研究之目的與研究的流程，確保每位問卷填答者於清楚本研究之目的及流程後始進行問卷之填答。本問卷於首頁說明頁，便告知問卷填答者可自主選擇隨時離開或中止問卷填，經當事人親自閱讀完畢，確認個人係自願參與本研究後，始進入問卷內容之填答頁面。

二、匿名及保密原則

Babbie(2015)指出，保護研究對象權益，首要就是在進行調查研究時保護其身分。保護研究對象身分的兩種方法包括:「匿名」(Anonymity)與「保密」(Confidentiality)。匿名，或稱為「不具名」，係指研究者與研究計畫之讀者均無法辨識研究中呈現之資料是屬於何種特定對象之資料，亦即研究者與閱讀者均無法知悉研究資料之受訪者身分。保密，係指研究者能夠辨識研究資料中係來自哪個特定對象，但對於研究對象加以承諾不會公開其身分之謂。Berg(2001)指出，多數研究中要完全達成樣本的匿名性實屬不易，因此必須謹慎處理所得資料，以盡保密之責。

本研究於問卷填答前會告知受訪者，本次填答的內容係採不記名的匿名方式，問卷收集完畢後所得之資料不對外公開、嚴守個人資料保護法之相關規範，並於資料分析完畢後採取適當之安全防護措施，以防止個人資料外洩或遭盜用，以期達成匿名及保密之倫理規範要求。

三、不傷害研究對象原則

Babbie(2015)及 Ruane(2007)指出，研究所帶來的傷害除了生理傷害外，也包括情緒或心理傷害，傷害的可能性亦會因為研究方法之不同而有所差異。一般而言，受研究者大多為較脆弱或易受傷害之族群，而研究的進行常會使這些較脆弱的族群受到二度傷害，因此必須保護研究對象之身體、情感與心理層面以防再度受到傷害。

由於本研究之研究對象涉及網路詐欺犯罪被害者，在問卷之部分題項中亦涉及個人網路詐欺被害之歷程與經驗，因此在問卷填答之前，問卷首頁便會告知填答者本次研究之目的及流程，並告知填答者若在填答期間感受到任何不舒服或有任何不愉快之經驗時，可以自主選擇隨時中斷或離開本問卷調查，以避免受到二度傷害，藉以保護受訪者生理、心理健康，達成不傷害研究對象之重要倫理準則。

四、真實呈現研究報告原則

研究人員除對研究對象負有重要之研究倫理責任外，對於資料收集後之分析及結果的報告撰寫亦負有重要之責。研究過程包括測量、抽樣、研究設計、結果分析及報告，在研究進行過程中，研究者的客觀中立及資料之真實呈現係學術研究中重要的價值內涵，有鑑於此，研究報告分析及結果之真實呈現便成為重要的倫理規範。

本研究於資料分析之過程中均嚴守真實呈現研究報告之原則，不竄改或偽造不實之數據，僅以受訪者填答之真實資料進行分析及研究，對於資料分析完畢後之報告撰寫亦秉持中立客觀之角度，以客觀、公正及嚴謹的方式如實呈現資料分析之結果，並以坦承開放之方式呈現個人研究成果，以符合學術誠信之倫理規範。

第四章 網路詐欺被害性別差異之分析

由於本研究係探究不同性別在網路詐欺被害之差異及原因，故本章將依據前述回收彙整所得之問卷調查資料，以性別為本章之分析及探討主軸，依序對於個人基本特性及各態度量表進行描述性統計、差異分析、相關分析及迴歸分析，藉以了解不同性別網路詐欺被害者在各研究變項之分布情形、不同性別網路使用者在各研究變項之間的差異、各變項間之相關性，以及建構影響不同性別網路詐欺被害重要因素之模型。

第一節 網路詐欺被害各組樣本在各測量變項之描述性統計

為更深入了解本研究樣本之性別與網路詐欺被害分布，故本節係就不同性別與被害在各研究變項之分布進行敘述，依據本研究變項可分為兩個部分，第一部分為網路詐欺被害各分組在各主要類別(間斷)變項之分布，第二部分為網路詐欺被害各分組在本研究各態度量表或連續變項之分布情形，茲將分析結果呈現如下:

一、網路詐欺被害各組樣本在各背景變項之描述性統計

(一)個人基本特性分析

在個人基本特性分析方面，包括性別、年齡、職業、收入、教育程度及婚姻狀況等六個變項，以下茲將網路詐欺被害各分組樣本在個人基本特性變項之分析敘述如下:

性別方面，在全體樣本中，男性占 455 名(52.3%)、女性占 415 名(47.7%)，與整體網路使用人口比例相近。在網路詐欺被害者中，計有 142 位，占全體樣本 16.32%，其中，男性被害者占 94 位(66.19%)、女性被害者占 48 位(33.81%)，男性人數多於女性，顯示在本研究樣本中，雖然全體樣本中男性與女性樣本之比例相近，但在被害樣本中，男性網路詐欺被害人數則多於女性。

年齡方面，在網路詐欺被害全體樣本中，以年齡介於 30-39 歲占 49 位(34.5%)比例最高，其中，男性被害組部分，以年齡介於 30-39 歲占 40 位(42.6%)比例最高，而女性被害組中，則以年齡介於 19-29 歲占 18 位(37.5%)比例最高，顯示兩性在網路詐欺被害之年齡分布上有所差異。

職業方面，在網路詐欺被害全體樣本中，以學生占 50 位(35.2%)比例最高，其中，在男性被害組中，以學生占 39 位(41.5%)比例最高，而在女性被害組中，則以從事家庭管理占 12 位(25.0%)比例最高，顯示網路詐欺被害者之職業分布上，男性與女性被害者有所差異。

收入方面，在網路詐欺被害全體樣本中，以收入介於 1 萬以上至 3 萬未滿占 72 位(50.7%)比例最高，其中，男性被害組中，以收入介於 1 萬以上至 3 萬未滿占 49 位(52.1%)比例最高，女性被害組中，亦以收入介於 1 萬以上至 3 萬未滿占 23 位(47.9%)比例最高，顯示在網路詐欺被害者之收入分布上，男性及女性皆以收入介於 1 萬以上至 3 萬未滿占最高比例。

教育程度方面，在網路詐欺被害全體樣本中，以專科、大學(肄)畢業占 87 位(61.3%)比例最高，其中，男性被害組中，以專科、大學(肄)畢業占 55 位(58.5%)比例最高，而女性被害組中亦以專科、大學(肄)畢業占 32 位(66.7%)比例最高，顯示網路詐欺被害者之教育程度分布上，男性及女性被害者之教育程度程度，皆以專科、大學(肄)畢業占最大多數。

婚姻狀況方面，在網路詐欺被害全體樣本中，以單身者占 77 位(54.2%)比例最高，其中，男性被害組中以單身者占 57 位(60.6%)比例最高，女性被害組中亦以單身者占 20 位(41.7%)比例最高，顯示網路詐欺被害者之教育程度分布上，男性及女性之婚姻狀況皆以單身占最大多數。有關本研究對於網路詐欺被害各分組樣本在個人基本特性之分析，詳細分析情形如下表 4-1-1 所示：

表 4-1-1 網路詐欺被害各組樣本在個人基本特性之分析

項目	組別	網路詐欺被害(人次/百分比)		
		全體 (N=142)	男性 (N=94)	女性 (N=48)
年齡	18 歲以下	11(7.7)	9(9.6)	2(4.2)
	19-29 歲	42(29.6)	24(25.6)	18(37.5)
	30-39 歲	49(34.5)	40(42.6)	9(18.8)
	40-49 歲	16(11.3)	7(7.4)	9(18.8)
	50-59 歲	11(7.7)	7(7.4)	4(8.3)
	60 歲以上	13(9.2)	7(7.4)	6(12.4)
職業	未就業(含退休)	29(20.4)	20(21.3)	9(18.8)
	學生	50(35.2)	39(41.5)	11(22.9)
	軍警公教人員	10(7.0)	6(6.4)	4(8.3)
	從事家庭管理	13(9.2)	1(1.1)	12(25.0)
	服務、事務工作人員	21(14.8)	15(16.0)	6(12.5)
	技術員及助理專業人員	12(8.5)	6(6.4)	6(12.5)
	非技術工、體力工	5(3.5)	5(5.2)	0(0.0)
	行政主管及經理人員	2(1.4)	2(2.1)	0(0.0)
收入	未滿 1 萬元	17(12.0)	13(13.8)	4(8.3)
	1 萬以上至 3 萬未滿	72(50.7)	49(52.1)	23(47.9)
	3 萬以上至 6 萬未滿	27(19.0)	15(16.0)	12(25.0)
	6 萬以上至 9 萬未滿	16(11.3)	10(10.7)	6(12.5)
	9 萬以上至 12 萬未滿	7(4.9)	5(5.3)	2(4.2)
	12 萬元以上	3(2.1)	2(2.1)	1(2.1)
教育程度	國小(肄)畢業	0(0.0)	0(0.0)	0(0.0)
	國中(肄)畢業	12(8.5)	10(10.6)	2(4.2)
	高中、高職(肄)畢業	22(15.5)	16(17.0)	6(12.5)
	專科、大學(肄)畢業	87(61.3)	55(58.5)	32(66.7)
	研究所(肄)畢業以上	21(14.7)	13(13.9)	8(16.6)
婚姻狀況	單身	77(54.2)	57(60.6)	20(41.7)
	未婚(非單身)	27(19.0)	17(18.1)	10(20.8)
	已婚(含同居)	30(21.1)	15(16.0)	15(31.2)
	離婚(含分居)	5(3.5)	3(3.2)	2(4.2)
	喪偶	2(1.5)	2(2.1)	0(0.0)
	再婚	1(0.7)	0(0.0)	1(2.1)

(二)網路使用特性

在網路使用特性方面，包括每次上網時數、每周上網次數、平日上網時段、假日上網時段、接觸網路時間、經常上網地點及經常上網原因等七個變項，茲將網路詐欺被害各分組分析情形敘述如表 4-1-2 所示:

在每次上網時數方面，在網路詐欺被害全體樣本中，以每次上網 3 小時以上至未滿 7 小時(中上網時數)占 98 名(69.0%)比例最高，其中，男性被害組中以每次上網 3 小時以上至未滿 7 小時(中上網時數)占 65 名(69.1%)比例最高，女性被害組中亦以每次上網 3 小時以上至未滿 7 小時(中上網時數)占 33 名(68.7%)比例最高，顯示在網路詐欺被害組之每次上網時數分布上，兩性之每次上網時數皆以每次上網 3 小時以上至未滿 7 小時(中上網時數)占最高比例。

在每周上網次數方面，在網路詐欺被害全體樣本中，以每周上網 10 次以上(高上網次數)占 83 名(58.5%)比例最高，其中，男性被害組中，以每周上網 10 次以上(高上網次數)占 57 名(60.6%)比例最高，女性被害組中亦以每周上網 10 次以上(高上網次數)，占 26 名(54.2%)比例最高，顯示在網路詐欺被害各組每周上網次數之分布上，兩性皆以每周上網 10 次以上(高上網次數)占最高比例。

在平日上網時段方面，在網路詐欺被害全體樣本中，以平日在 16：01 至 00：00(夜間時段)上網占 119 名(83.8%)比例最高，其中，男性被害組中，以平日在 16：01 至 00：00(夜間時段)上網占 80 名(85.1%)比例最高，女性被害組中，平日上網時段亦以平日在 16：01 至 00：00(夜間時段)上網占 39 名(81.3%)比例最高，顯示在網路詐欺被害組之平日上網時段分布上，兩性均以平日在 16：01 至 00：00(夜間時段)上網占最高比例。

在假日上網時段方面，在網路詐欺被害全體樣本中，以假日在 16：01 至 00：00(夜間時段)上網占 87 名(61.3%)比例最高，其中，男性被害組中，以假日在 16：01 至 00：00(夜間時段)上網占 56 名(59.6%)比例最高，女性被害組中，假日上網時段亦以假日在 16：01 至 00：00(夜間時段)上網占 31 名(64.6%)比例最高，顯示在網路詐欺被害組之假日上網時段分布上，兩性均以假日在 16：01 至 00：00(夜間時段)上網占最高比例。

在接觸網路時間方面，在網路詐欺被害全體樣本中，以接觸網路 10 年以上占 89 名(62.7%)比例最高，其中，男性被害組中，以接觸網路 10 年以上占 62 名(66.0 %)比例最高，女性被害組中，亦以接觸網路 10 年以上占 27 名(56.3%)比例最高，顯示兩性在網路詐欺被害之接觸網路時間分布上，均以接觸網路 10 年以上占最高比例。

在經常上網地點方面，在網路詐欺被害全體樣本中，最常上網的地點為在家中(租屋處)上網占 137 次(36.8%)，其次為在工作場所上網占 107 次(28.8%)，其中，男性被害組中，最常上網的地點為在家中(租屋處)上網占 90 次(35.8%)，其次為在工作場所上網占 75 次(29.7%)，女性被害組中，最常上網的地點亦為在家中(租屋處)上網占 47 次(39.1%)，其次為在工作場所上網占 32 次(26.6%)，顯示兩性在網路詐欺被害之經常上網地點分布上，最常上網地點均為家中(租屋處)，其次皆為工作場所。

在經常上網原因方面，在網路詐欺被害全體樣本中，最常上網原因為搜尋資料占 112 次(19.1%)，其次為休閒娛樂占 109 次(18.6%)，其中，在男性被害組中，最常上網原因為休閒娛樂占 77 次(19.1%)，其次為抒發情緒占 75 次(18.7%)，在女性被害組中，最常上網原因則為抒發情緒占 37 次(20.2%)，其次為在休閒娛樂占 33 次(17.8%)，顯示兩性在網路詐欺被害之經常上網原因分布上有所差異。

表 4-1-2 網路詐欺被害各組樣本在網路使用特性之分析

項目	組別	網路詐欺被害(人次/百分比)		
		全體 (N=142)	男性 (N=94)	女性 (N=48)
每次上網時數	未滿 3 小時(低)	19(13.7)	12(12.8)	7(14.6)
	3 小時以上至未滿 7 小時(中)	98(69.0)	65(69.1)	33(68.7)
	7 小時以上(高)	25(17.3)	17(18.1)	8(16.7)
每周上網次數	未滿 7 次(低)	10(7.0)	6(6.4)	4(8.3)
	7 至 9 次(中)	49(34.5)	31(33.0)	18(37.5)
	10 次以上(高)	83(58.5)	57(60.6)	26(54.2)
平日上網時段	08：01 至 16：00(白天)	5(3.5)	3(3.2)	2(4.2)
	16：01 至 00：00(夜間)	119(83.8)	80(85.1)	39(81.3)
	00：01 至 08：00(深夜)	18(12.7)	11(11.7)	7(14.5)
假日上網時段	08：01 至 12：00(白天)	11(7.7)	4(4.3)	7(14.6)
	16：01 至 00：00(夜間)	87(61.3)	56(59.6)	31(64.6)
	00：01 至 08：00(深夜)	44(31.0)	34(36.1)	10(20.8)
接觸網路時間	3 年未滿	3(2.1)	2(2.2)	1(2.1)
	3 年以上至 5 年未滿	13(9.1)	9(9.6)	4(8.3)
	5 年以上至 10 年未滿	37(26.1)	21(22.2)	16(33.3)
	10 年以上	89(62.7)	62(66.0)	27(56.3)
經常上網地點[9]	在家中(租屋處)上網	137(36.8)	90(35.8)	47(39.1)
	在學校(圖書館)上網	43(11.6)	28(11.1)	15(12.6)
	朋友(同學)家中上網	28(7.5)	17(6.8)	11(9.2)
	在網咖上網	6(1.6)	4(1.5)	2(1.6)
	在公共場所上網	51(13.7)	38(15.1)	13(10.9)
	在工作場所上網	107(28.8)	75(29.7)	32(26.6)
經常上網原因[10]	抒發情緒	112(19.1)	75(18.7)	37(20.2)
	搜尋資料	95(16.2)	63(15.7)	32(17.3)
	買賣東西	61(10.4)	41(10.2)	20(10.4)
	交友聊天	93(15.9)	63(15.7)	30(16.2)
	休閒娛樂	109(18.6)	77(19.1)	33(17.8)
	找尋新奇事物	36(6.2)	25(6.2)	11(6.3)
	收發信件	54(9.2)	38(9.5)	16(9.1)
	滿足網愛	25(4.4)	20(4.9)	5(2.7)

[9] 本題為複選題，故表格中呈現之次數係為各回答題項之統計次數。
[10] 本題為複選題，故表格中呈現之次數係為各回答題項之統計次數。

(三)網路詐欺被害經驗

在網路詐欺被害經驗方面，包括最近一次網路詐欺被害之被害類型、被害損失、交易方式、與加害者關係、是否與加害者互動、與加害者互動管道、如何得知被害、多久發現自己被害、是否報案、報案方式、未報案原因及網路詐欺被害原因等 12 個變項，由於本部份之分析皆為具有網路詐欺被害經驗者，故係依據被害者之性別加以分組，茲將網路詐欺被害各分組分析情形敘述如表 4-1-3 所示:

在最近一次網路詐欺被害類型方面，在網路詐欺被害全體樣本中，以網路購物詐欺(自己是買方)占 80 名(56.3%)最高比例，其中，男性被害組中以網路購物詐欺(自己是買方)占 46 名(48.9%)最高比例，而女性被害組以網路購物詐欺(自己是買方)占 34 名(70.8%)最高比例，顯示最近一次網路詐欺被害類型，兩性皆以網路購物詐欺比例最高。

在最近一次網路詐欺被害損失方面，在全體被害樣本中，以被害損失 1 萬以上至未滿 5 萬元占 53 名(37.3%)最高比例，男性被害組以被害損失 1 萬以上至未滿 5 萬元占 36 名(38.3%)最高比例，女性被害組部份，以被害損失 1 萬以上至未滿 5 萬元占 17 名(35.4%)最高比例，顯示兩性在最近一次網路詐欺被害損失，均以 1 萬以上至未滿 5 萬元占多數。

在最近一次網路詐欺被害之交易方式方面，在網路詐欺被害全體樣本中，以 ATM 轉帳占 55 名(38.7%)最高比例，男性被害組中，以 ATM 轉帳占 36 名(38.3%)最高比例，女性部份亦以 ATM 轉帳占 19 名(39.6%)最高比例，顯示兩性在最近一次網路詐欺被害之交易方式方面，均以 ATM 轉帳占最大多數。

在最近一次網路詐欺被害與加害者關係方面，網路詐欺被害全體樣本中，以陌生人占 120 名(84.5%)最高比例，其中，在男性被害組中，以陌生人 76 名(80.9%)比例最高。在女性被害組中，以陌生人 44 名(91.7%)比例最高，顯示兩性與加害者之關係多為陌生。

在最近一次網路詐欺被害是否與加害者互動方面，在網路詐欺被害全體樣本中，以與加害者互動占 104 位(73.2%)占最高比例，在男性被害組中，與加害者互動占 76 位(80.9%)，而在女性被害組中，與加害者互動占 28 位(58.3%)，顯示在與網路詐欺加害者互動方面，男性與加害者互動之程度較女性高。

在最近一次與加害者互動管道方面，在網路詐欺被害全體樣本中，以網路社群網站占 38 位(36.5%)最高比例，男性被害組中，以網路社群網站占 24 位(31.6%)最高比例，女性被害組中，亦以網路社群網站占 14 位(50.1%)最高比例，顯示兩性在最近一次網路詐欺與加害者互動之管道，均以網路社群網站比例最高。

在最近一次網路詐欺被害如何得知自己被害方面，在網路詐欺被害全體樣本中，以自己察覺占 108 位(76.1%)最高比例，男性被害組中，亦以自己察覺占 73 位(77.7%)最高比例，女性被害組部份，亦以自己察覺占 35 位(72.9%)最高比例，顯示兩性在最近一次網路詐欺被害均以自己察覺被害之比例最高。

在最近一次網路詐欺多久發現自己被害方面，在網路詐欺被害全體樣本中，以 4 至 6 天發現被害占 65 位(45.8%)最高比例，男性被害組中，以 4 至 6 天發現被害占 46 位(48.9%)最高比例，而女性被害組中，亦以 4 至 6 天發現被害占 19 位(39.6%)最高比例，顯示兩性在最近一次網路詐欺被害，均以 4 至 6 天發現自己被害占最大多數。

在最近一次網路詐欺被害是否報案方面，在網路詐欺被害全體樣本中，報案者占 60 位(42.3%)，在男性被害者中，報案者占 40 位(42.6%)，女性被害者中，報案者占 20 位(41.7%)，顯示在最近一次網路詐欺被害是否報案部分，兩性比例相近。

在最近一次網路詐欺被害之報案方式方面，在網路詐欺被害全體樣本中，以親自到警察單位報案占 42 位(70.0%)最高比例，男性被害組中，以親自到警察單位報案占 31 位(77.5%)最高比例;女性部份亦以親自到警察單位報案占 11 位(55.5%)最高比例，顯示兩性在最近一次網路詐欺被害之報案方式，皆以親自到警察單位報案占最大多數。

在最近一次網路詐欺被害未報案原因方面，在網路詐欺被害全體樣本中，以自認倒楣占 57 次(18.6%)最高比例，男性以自認倒楣占 40 次(18.7%)最高比例，女性部份亦以自認倒楣占 17 次(19.4%)最高比例，顯示兩性未報案之原因，均以自認倒楣占最大多數。

在最近一次網路詐欺被害被害原因方面，在網路詐欺被害全體樣本中，以自身疏忽占 113 次(20.6%)最高比例，男性被害者以自身疏忽占 74 次(20.3%)最高比例，女性被害者亦以自身疏忽占 39 次(21.4%)最高比例，顯示兩性在最近一次網路詐欺被害被害原因，均認為係自身疏忽之因素占最大多數。

表 4-1-3 網路詐欺被害各組樣本在被害經驗特性之分析

項目	組別	網路詐欺被害(人次/百分比)		
		全部樣本 (N=142)	男性 (N=94)	女性 (N=48)
最近一次被害類型	網路購物詐欺(買方)	80(56.3)	46(48.9)	34(70.8)
	網路購物詐欺(賣方)	14(9.9)	5(5.3)	9(18.8)
	商業金融詐欺	8(5.6)	7(7.4)	1(2.1)
	網路遊戲詐欺	10(7.1)	10(10.6)	0(0.0)
	網路交友詐欺	24(16.9)	20(21.4)	4(8.3)
	色情網站詐欺	3(2.1)	3(3.2)	0(0.0)
	網路賭博詐欺	3(2.1)	3(3.2)	0(0.0)
最近一次被害損失	500 元以下	2(1.4)	1(1.1)	1(2.1)
	500 至 1000 元	12(8.5)	9(9.6)	3(6.3)
	1000 至 5000 元	31(21.8)	22(23.4)	9(18.8)
	5000 至 1 萬元	26(18.3)	13(13.8)	13(27.1)
	1 萬以上至未滿 5 萬元	53(37.3)	36(38.3)	17(35.4)
	5 萬以上至未滿 10 萬元	9(6.3)	6(6.4)	3(6.2)
	10 萬以上至未滿 15 萬元	4(2.8)	2(2.1)	2(2.1)
	15 萬元以上	5(3.6)	5(5.3)	0(0.0)
最近一次交易方式	現金交付	7(4.9)	4(4.3)	3(6.3)
	ATM 轉帳	55(38.7)	36(38.3)	19(39.6)
	金融機構匯款	47(33.1)	35(37.2)	12(25.0)
	網路銀行付款	20(14.1)	10(10.6)	10(20.8)
	其他	13(9.2)	9(9.6)	4(8.3)
最近一次與加害者關係	同學	1(0.7)	1(1.0)	0(0.0)
	朋友或同事	18(12.7)	15(16.0)	3(6.2)
	陌生人	120(84.5)	76(80.9)	44(91.7)
	其他	3(2.1)	2(2.1)	1(2.1)
是否互動	是	104(73.2)	76(80.9)	28(58.3)
	否	38(26.8)	18(19.1)	20(41.7)
與加害者互動管道	拍賣網站	25(24.0)	16(21.1)	9(32.1)
	網路電話	2(1.9)	0(0.0)	2(7.1)
	線上遊戲	9(8.7)	9(11.8)	0(0.0)
	即時通訊軟體	24(23.1)	23(30.2)	1(3.6)
	網路社群網站	38(36.5)	24(31.6)	14(50.1)
	其他	6(5.8)	4(5.3)	2(7.1)

如何得知被害	自己察覺	108(76.1)	73(77.7)	35(72.9)
	朋友或同事發現	24(16.9)	16(17.0)	8(16.7)
	親人發現	8(5.6)	5(5.3)	3(6.3)
	其他	2(1.4)	0(0.0)	2(4.2)
多久發現自己被害	1 日以內	13(9.2)	8(8.5)	5(10.4)
	1 至 3 天	30(21.1)	19(20.3)	11(22.9)
	4 至 6 天	65(45.8)	46(48.9)	19(39.6)
	7 至 14 天	27(19.0)	17(18.1)	10(20.8)
	14 至 30 天	3(2.1)	2(2.1)	1(2.1)
	30 天以上	4(2.8)	2(2.1)	2(4.2)
是否報案	是	60(42.3)	40(42.6)	20(41.7)
	否	82(57.7)	54(57.4)	28(58.3)
報案方式	電話報案	12(20.0)	6(15.0)	6(30.0)
	網路報案	5(8.3)	2(5.0)	3(15.0)
	傳真報案	1(1.7)	1(2.5)	0(0.0)
	親自到警察單位報案	42(70.0)	31(77.5)	11(55.0)
未報案原因[11]	自認倒楣	57(18.6)	40(18.7)	17(19.4)
	不想追究	40(13.1)	27(12.7)	13(14.8)
	被騙金額不多	42(13.7)	32(14.9)	10(11.4)
	覺得丟臉	43(14.1)	33(15.5)	10(11.4)
	報案無用	40(13.1)	28(13.0)	12(13.6)
	報案程序複雜	34(12.2)	25(11.6)	9(10.2)
	想要私下解決	14(4.6)	9(4.2)	5(5.7)
	害怕加害者報復	13(4.4)	11(5.2)	2(2.2)
	只是消費糾紛	19(6.2)	9(4.2)	10(11.3)
被害原因[12]	自身疏忽	113(20.6)	74(20.3)	39(21.4)
	貪小便宜	86(15.7)	52(14.2)	34(18.7)
	過於相信他人	87(15.8)	63(17.3)	24(13.2)
	自己太笨	57(10.4)	38(10.3)	19(10.5)
	產品吸引人	42(7.7)	24(6.6)	18(9.9)
	缺乏自我保護常識	111(20.3)	73(19.9)	38(20.9)
	不清楚	12(2.2)	11(3.0)	1(0.5)
	運氣不好	40(7.3)	31(8.4)	9(4.8)

[11] 本題為複選題，故表格中呈現之次數係為各回答題項之統計次數。
[12] 本題為複選題，故表格中呈現之次數係為各回答題項之統計次數。

二、網路詐欺被害各組樣本在各態度面向之程度分析

(一)網路生活型態分析

在網路生活型態分析部份，依據各題項內容，調查網路詐欺被害各分組樣本在過去一年內的網路生活型態情形，以下茲就各構面分次敘述如後:

1.網路休閒活動

在網路休閒活動中，共包含以下 5 個題項，在全體網路詐欺被害樣本中，網路休閒活動類型以「經常使用即時通訊軟體與他人溝通互動」平均得分 3.70 最高、其次係為「經常使用網路社群媒體」平均得分 3.58。其中，在男性被害組中，網路休閒活動類型亦以「經常使用即時通訊軟體與他人溝通互動」平均得分 3.66 最高、其次為「經常使用網路社群媒體」平均得分 3.55。在女性被害組中，網路休閒活動類型亦以「經常使用即時通訊軟體與他人溝通互動」平均得分 3.77 最高、其次為「經常使用網路社群媒體」平均得分 3.65。全體受訪者在網路休閒活動構面之平均數為 3.47、標準差為.419、偏態係數為-1.046、峰度係數為.454。

由此可知，在網路詐欺被害各組之網路休閒活動類型中，皆以「經常使用即時通訊軟體與他人溝通互動」頻率最高，其次皆為「經常使用網路社群媒體」，有關網路詐欺被害各分組樣本在網路休閒活動行為程度之分析如下表 4-1-4 所示:

表 4-1-4 網路詐欺被害各組樣本在網路休閒活動行為程度之分析

網路休閒活動類型	網路詐欺被害(平均數/標準差)		
	全體樣本 (N=142)	男性 (N=94)	女性 (N=48)
1.您經常使用即時通訊軟體與他人溝通互動	3.70(0.532)	3.66(0.578)	3.77(0.425)
2.您經常使用網路社群媒體	3.58(0.655)	3.55(0.697)	3.65(0.565)
3.您經常從事網路購物行為	3.15(0.641)	3.09(0.633)	3.27(0.644)
4.您經常在網路上瀏覽新聞	3.37(0.730)	3.33(0.781)	3.46(0.617)
5.當您無聊時經常上網	3.48(0.681)	3.45(0.713)	3.54(0.617)
網路休閒活動(N=870): 平均數=3.47、標準差=.419、偏態係數=-1.046、峰度係數=.454			

2.網路職業活動

在網路職業活動中，共包含以下 5 個題項，在全體網路詐欺被害樣本中，以「經常利用網路來搜尋資料」平均得分 3.54 最高、其次為「經常在網路上下載資料」平均得分 3.52。其中，在男性被害組部分，網路職業活動類型則以「經常在網路上下載資料」平均得分 3.50 最高、其次為「經常利用網路來搜尋資料」平均得分 3.47。

在女性被害組部分，網路職業活動類型以「經常利用網路來搜尋資料」平均得分 3.67 最高、其次為「經常在網路上下載資料」平均得分 3.56。全體受訪者網路職業活動構面平均數為 3.42、標準差為.525、偏態係數為-.907、峰度係數為.595。

由此可知，在網路詐欺被害各組別之網路職業活動類型中，雖多以「經常在網路上下載資料」與「經常利用網路來搜尋資料」頻率較高，但兩性網路詐欺被害者最常從事之網路職業活動則有所差異。有關網路詐欺被害各分組樣本在網路職業活動行為程度之分析如下表 4-1-5 所示:

表 4-1-5 網路詐欺被害各組樣本在網路職業活動行為程度之分析

網路職業活動類型	網路詐欺被害(平均數/標準差)		
	全體樣本 (N=142)	男性 (N=94)	女性 (N=48)
6.您經常檢查您的電子郵件	2.90(0.836)	2.82(0.738)	3.06(0.861)
7.您經常寄送電子郵件	2.76(0.780)	2.70(0.760)	2.88(0.815)
8.您經常利用網路進行檔案傳輸	3.35(0.665)	3.31(0.640)	3.44(0.712)
9.您經常利用網路來搜尋資料	3.54(0.649)	3.47(0.683)	3.67(0.559)
10.您經常在網路上下載資料	3.52(0.702)	3.50(0.715)	3.56(0.681)
網路職業活動(N=870): 平均數=3.42、標準差=.525、偏態係數=-.907、峰度係數=.595			

3.網路風險休閒活動

在網路風險休閒活動中，共包含以下 5 個題項，在全體網路詐欺被害樣本中，網路風險休閒活動類型以「您經常瀏覽色情網站」平均得分 2.31 最高、其次為「您經常從網站下載免費音樂」平均得分 2.13。其中，在男性被害組部分，網路風險休閒活動類型以「您經常瀏覽色情網站」平均得分 2.44 最高、其次為「您經常從網站下載免費遊戲」平均得分 2.24。

女性在被害組部分，網路風險休閒活動類型以「您經常瀏覽色情網站」平均得分 2.06 最高、其次為「您經常從網站下載免費音樂」平均得分 1.98。全體受訪者在網路風險休閒活動構面平均數為 2.02、標準差為.672、偏態係數為.650、峰度係數為-.005。

由此可知，在網路詐欺被害各組方面，兩性在網路風險休閒活動之類型雖然皆以「您經常瀏覽色情網站」最高，但男性其次則為「您經常從網站下載免費遊戲」、女性其次為「您經常從網站下載免費音樂」，顯見不同性別在網路風險休閒活動之行為上亦有所差異。有關網路詐欺被害各分組樣本在網路風險休閒活動行為程度之分析如下表 4-1-6 所示:

表 4-1-6 網路詐欺被害各組樣本在網路風險休閒活動行為程度之分析

網路風險休閒活動類型	網路詐欺被害(平均數/標準差)		
	全體樣本 (N=142)	男性 (N=94)	女性 (N=48)
11.您經常瀏覽色情網站	2.31(0.844)	2.44(0.922)	2.06(0.598)
12.您經常從網站下載免費遊戲	2.09(0.898)	2.24(0.935)	1.79(0.743)
13.您經常從網站下載免費音樂	2.13(0.832)	2.20(0.899)	1.98(0.668)
14.您經常從網站下載免費電影	2.09(0.898)	2.19(0.965)	1.90(0.722)
15.您經常從網站下載不明來源檔案	1.87(0.774)	1.91(0.851)	1.77(0.592)
網路風險休閒活動(N=870):平均數=2.02、標準差=.672、偏態係數=.650、峰度係數=-.005			

4.網路風險職業活動

在網路風險職業活動中，共包含以下 5 個題項，在全體網路詐欺被害樣本中，網路風險職業活動類型以「您經常點擊經由即時通訊軟體接收到的未知來源檔案或附件」之平均得分 1.75 最高、其次為「您經常點擊不明來源電子郵件」平均得分 1.70。其中，在男性被害組中，網路風險職業活動類型以「您經常點擊經由即時通訊軟體接收到的未知來源檔案或附件」平均得分 1.78 最高、其次為「您經常點擊不明來源的電子郵件」平均得分 1.73。在女性被害組部分，網路風險職業活動類型以「您經常點擊經由即時通訊軟體接收到的未知來源檔案或附件」平均得分 1.72 最高、其次為「您經常點擊不明來源電子郵件的相關網頁連結」平均得分 1.71。

全體受訪者在網路風險職業活動平均數為 1.41、標準差為.545、偏態係數為 1.625、峰度係數為 2.775，由於本變項整體分配係呈正(右)偏態分布，故將變項進行自然對數轉換(Natural logarithm transformation)，以符合常態分配。經自然對數轉換後之變項，偏態係數為.958、峰度係數為.076，整體分配已符合常態分布，並據此進行後續分析。

由此可知，在網路詐欺被害各組中，兩性均以「您經常點擊經由即時通訊軟體接收到的未知來源檔案或附件」最高，有關網路詐欺被害各分組樣本在網路風險職業活動之分析如下表 4-1-7 所示:

表 4-1-7 網路詐欺被害各組樣本在網路風險職業活動行為程度之分析

網路風險職業活動類型	網路詐欺被害(平均數/標準差)		
	全體樣本 (N=142)	男性 (N=94)	女性 (N=48)
16.您經常點擊不明來源電子郵件	1.70(0.751)	1.73(0.792)	1.65(0.668)
17.您經常點擊不明來源電子郵件的附件檔案	1.68(0.728)	1.67(0.753)	1.70(0.683)
18.您經常點擊不明來源電子郵件的網頁連結	1.67(0.760)	1.65(0.786)	1.71(0.713)
19.您經常點擊經由即時通訊軟體接收到的未知來源檔案或附件	1.75(0.736)	1.78(0.792)	1.72(0.617)
20.您經常寄信至不明電子郵件	1.55(0.720)	1.61(0.793)	1.44(0.542)
網路風險職業活動(N=870): 平均數=1.41、標準差=.545、偏態係數=1.625、峰度係數=2.775			

(二)被害情境與機會分析

在被害情境與機會分析部份，依據各構面之題項，調查網路詐欺被害各分組受試者在過去一年來在網路使用中所面臨的被害情境、監控程度、負面誘因及網路偏差動機，故包括社會監控、物理監控、網路負面誘因及網路偏差動機等四個部分。以下就各變項分次敘述如後:

1.社會監控

在社會監控中，共包含以下 5 個題項，在全體網路詐欺被害樣本中，以「上網時同學(同事)會在您身邊」平均得分 1.92 最高，其次為「上網時同學以外的朋友會在您身邊」平均得分 1.89。其中，在男性被害組部分，以「上網時同學(同事)會在您身邊」及「上網時同學以外的朋友會在您身邊」平均得分 1.84 最高、其次為「上網時師長(上司)會在您身邊」平均得分 1.83。在女性被害組部分，以「上網時同學(同事)會在您身邊」平均得分 2.06 最高、其次為「上網時同學以外的朋友會在您身邊」平均得分 1.98。全體受訪者在社會監控構面平均數為 1.99、標準差為.628、偏態係數為.358、峰度係數為-.337。

在社會監控程度方面,得分越高代表個人在網路使用的過程中受到的社會監控程度越高。在網路詐欺被害組之社會監控類型中,兩性均以「上網時同學(同事)會在您身邊」之平均得分最高，而男性在社會監控之各題項平均得分則低於女性，有關網路詐欺被害各分組樣本在社會監控類型分析如下表 4-1-8 所示:

表 4-1-8 網路詐欺被害各組樣本在社會監控類型之分析

社會監控類型	網路詐欺被害(平均數/標準差)		
	全體樣本 (N=142)	男性 (N=94)	女性 (N=48)
1.您上網時父母會在您身邊	1.70(0.605)	1.63(0.568)	1.85(0.652)
2.您上網時兄弟姐妹會在您身邊	1.78(0.632)	1.74(0.585)	1.85(0.714)
3.您上網時同學(同事)會在您身邊	1.92(0.748)	1.84(0.752)	2.06(0.727)
4.您上網時同學外朋友會在您身邊	1.89(0.835)	1.84(0.884)	1.98(0.729)
5.您上網時師長(上司)會在您身邊	1.85(0.828)	1.83(0.838)	1.88(0.815)
社會監控(N=870):平均數=1.99、標準差=.628、偏態係數=.358、峰度係數=−.337			

2.物理監控

在物理監控中，共包含以下 5 個題項，在全體網路詐欺被害樣本中，以「您對於不同的電腦會安裝防毒軟體」平均得分 2.80 最高、其次為「您的電腦有定期更新防毒軟體」平均得分 2.53。在男性被害組部分，以「您對於不同的電腦會安裝防毒軟體」平均得分 2.82 最高、其次為「您的電腦有定期更新防毒軟體」平均得分 2.47。

女性被害組部分，以「您對於不同的電腦會安裝防毒軟體」平均得分 2.75 最高、其次為「您的電腦有定期更新防毒軟體」平均得分 2.65。全體受訪者在物理監控平均數為 2.69、標準差為.661、偏態係數為-.136、峰度係數為-.556。

在物理監控程度分析方面，得分越高代表個人受到的物理監控程度越高，由下表 4-1-9 可得知，在網路詐欺被害各分組之物理監控類型中，兩性均以「您對於不同電腦會安裝防毒軟體」之平均得分最高，而男性在物理監控各題項之平均得分則低於女性，有關網路詐欺被害各分組樣本在物理監控類型之分析如下表 4-1-9 所示:

表 4-1-9 網路詐欺被害各組樣本在物理監控類型之分析

物理監控類型	網路詐欺被害(平均數/標準差)		
	全體樣本 (N=142)	男性 (N=94)	女性 (N=48)
6.您對於不同的電腦會安裝防毒軟體	2.80(0.863)	2.82(0.867)	2.75(0.863)
7.您的電腦有定期更新防毒軟體	2.53(0.760)	2.47(0.786)	2.65(0.699)
8.您對於不同網路帳號會使用不同的密碼	2.37(0.812)	2.37(0.855)	2.35(0.729)
9.您會定期更改個人網路帳號密碼	2.26(0.769)	2.29(0.785)	2.21(0.743)
10.您會注意到在網路空間中該留下何種個人資訊	2.37(0.803)	2.34(0.824)	2.42(0.767)
物理監控(N=870):平均數=2.69、標準差=.661、偏態係數=−.136、峰度係數=−.556			

3.網路負面誘因

在網路負面誘因中，包含以下 4 個題項，在全體網路詐欺被害樣本中，以「您曾經在網路上看到網路援交訊息」平均得分 2.20 最高、其次為「您曾經在網路上看到網路賭博訊息」、「您曾經在網路上看到買賣違禁物品」平均得分 2.04。其中，在男性被害組部分，以「您曾經在網路上看到網路援交訊息」平均得分 2.33 最高、其次為「您曾經在網路上看到買賣違禁物品」平均得分 2.15。

女性被害組部分，以「您曾經在網路上看到網路援交訊息」平均得分 1.94 最高、其次為「您曾經在網路上看到買賣盜版軟體」平均得分 1.88。全體受訪者網路負面誘因平均數為 1.93、標準差為.734、偏態係數為.608、峰度係數為-.277。

在網路負面誘因分析方面，若構面平均得分越高，代表個人在網路使用的過程中所接受到的網路負面誘因程度越高，由下表 4-1-10 可得知，網路詐欺被害各分組中，皆以「您曾經在網路上看到網路援交訊息」平均得分最高，其中，男性在網路負面誘因各題項之平均得分皆大於女性。有關網路詐欺被害各分組樣本在網路負面誘因類型之分析如下表 4-1-10 所示:

表 4-1-10 網路詐欺被害各組樣本在網路負面誘因類型之分析

網路負面誘因類型	網路詐欺被害(平均數/標準差)		
	全體樣本 (N=142)	男性 (N=94)	女性 (N=48)
11.您曾經在網路上看到網路賭博訊息	2.04(0.926)	2.14(0.934)	1.83(0.883)
12.您曾經在網路上看到網路援交訊息	2.20(0.991)	2.33(1.010)	1.94(0.909)
13.您曾經在網路上看到買賣違禁物品	2.04(0.944)	2.15(0.834)	1.83(0.834)
14.您曾經在網路上看到買賣盜版軟體	2.03(0.940)	2.14(0.968)	1.88(0.866)
網路負面誘因(N=870): 平均數=1.93、標準差=.734、偏態係數=.608、峰度係數=−.277			

4.網路偏差動機

在網路負面誘因中，共包含以下 7 個題項，在全體網路詐欺被害樣本中，以「您曾想利用網路瀏覽色情網站或進行網路援交」平均得分 1.53 最高。其中，在男性被害組部分，以「您曾經想利用網路瀏覽色情網站或進行網路援交」平均得分 1.62 最高，而在女性被害組部分，以「您曾想利用網路干擾他人網路使用」平均得分 1.46 最高。

全體受訪者在網路偏差動機之平均數為 1.22、標準差為.415、偏態係數為 2.937、峰度係數為 2.096。由於本變項呈中度右偏態分布，故將變項進行平方根轉換(Square root transformation)，經轉換後之變項，偏態係數為 1.296、峰度係數為 1.066，整體分配已近似常態分配，並據此進行後續分析。

由此可知，在網路偏差動機方面，網路詐欺被害之男性及女性在網路偏差動機類型有所差異。此外，男性在網路偏差動機各題項平均得分皆大於女性，有關網路詐欺被害各分組樣本在網路偏差動機類型之分析如下表 4-1-11 所示:

表 4-1-11 網路詐欺被害各組樣本在網路偏差動機類型之分析

網路偏差動機類型	網路詐欺被害(平均數/標準差)		
	全體樣本 (N=142)	男性 (N=94)	女性 (N=48)
15.您曾經想利用網路干擾他人網路使用	1.52(0.778)	1.55(0.798)	1.46(0.743)
16.您曾經想在不知情或的情況下使用他人的帳戶或文件	1.37(0.748)	1.47(0.851)	1.17(0.429)
17.您曾經想在未經所有者許可的情況下，在其電腦中增加或刪除任何資訊	1.35(0.736)	1.45(0.838)	1.17(0.429)
18.您曾經想利用瀏覽色情網站或進行網路援交	1.53(0.787)	1.62(0.881)	1.33(0.519)
19.您曾經想從事網路詐騙	1.35(0.685)	1.44(0.784)	1.17(0.377)
20.您曾經想從事網路賭博	1.35(0.707)	1.44(0.797)	1.19(0.445)
21.您曾經想從事網路非法交易	1.33(0.702)	1.45(0.811)	1.10(0.309)
網路偏差動機(N=870): 平均數=1.22、標準差=.415、偏態係數=2.937、峰度係數=2.096			

(三)低自我控制程度分析

在低自我控制程度分析部份，依據各構面之題項，依序調查網路詐欺被害之各分組受試者的個人低自我控制程度，其中包括衝動性、冒險性及投機性等三個部分，以下茲分次敘述如下:

1.衝動性

在低自我控制量表中,經探索性因素分析後所萃取出之第一個因子命名為「衝動性」，其概念係由量表中之第 1 題至第 4 題所建構而成。在全體網路詐欺被害樣本中,係以「您經常在不考慮所有選擇的情況下採取行動」平均得分 2.35 最高、其次為「生活做些簡單的事給您無窮的樂趣」平均得分 2.34。

在男性被害組部分，以「您經常在不考慮所有選擇的情況下採取行動」平均得分 2.46 最高、其次為「生活做些簡單的事給您無窮的樂趣」平均得分 2.45。女性被害組部分，則以「生活做些簡單的事給您無窮的樂趣」平均得分 2.13 最高、其次為「您經常在不考慮所有選擇的情況下採取行動」平均得分 2.10。

全體受訪者衝動性構面平均數為 2.02、標準差為.712、偏態係數為.473、峰度係數為-.150。由下表 4-1-12 可知，網路詐欺被害各分組中，男性各題項之衝動性平均得分較女性高。有關不同性別與網路詐欺被害在衝動性程度之分析，如下表 4-1-12 所示:

表 4-1-12 網路詐欺被害各組樣本在衝動性程度之分析

衝動性	網路詐欺被害(平均數/標準差)		
	全體樣本 (N=142)	男性 (N=94)	女性 (N=48)
1.您經常在不考慮所有選擇的情況下採取行動	2.35(0.981)	2.46(1.033)	2.10(0.831)
2.有時您無法阻止自己做某事，即使您知道這是錯的	2.24(0.930)	2.34(0.979)	2.04(0.798)
3.您會因為眼前的立即快樂而較少考慮以後才會發生的事	2.19(0.945)	2.32(0.941)	1.94(0.909)
4.生活做些簡單的事給您無窮的樂趣	2.34(0.974)	2.45(1.001)	2.13(0.890)
衝動性(N=870): 平均數=2.02、標準差=.712、偏態係數=.473、峰度係數=-.150			

2.冒險性

在低自我控制量表中，經探索性因素分析後所萃取出之第二個因子重新命名為「冒險性」，其概念係由量表中之第 5 題至第 8 題所建構而成。在全體網路詐欺被害樣本中，以「您會做些有點冒險的事情來考驗一下自己」平均得分 2.65 最高、其次為「您偶爾會進行風險性金融投資」平均得分 2.50。在男性被害組部分，以「您會做些有點冒險的事情來考驗一下自己」平均得分 2.71 最高、其次為「您偶爾會進行風險性金融投資」平均得分 2.60。

在女性被害組部分，亦以「您會做些有點冒險的事情來考驗一下自己」平均得分 2.52 最高、其次為「刺激跟冒險對您來說比安全更重要」平均得分 2.33。

全體受訪者在冒險性構面之平均數為 2.21、標準差為.616、偏態係數為-.132、峰度係數為-.480。由下表 4-1-13 可知，網路詐欺被害各分組中，男性在各題項之冒險性平均得分較女性高。有關不同性別與網路詐欺被害在冒險性程度之分析，如下表 4-1-13 所示:

表 4-1-13 網路詐欺被害各組樣本在冒險性程度之分析

冒險性	網路詐欺被害(平均數/標準差)		
	全體樣本 (N=142)	男性 (N=94)	女性 (N=48)
5.您會做些有點冒險的事情來考驗一下自己	2.65(0.621)	2.71(0.616)	2.52(0.618)
6.刺激跟冒險對您來說比安全更重要	2.41(0.609)	2.45(0.580)	2.33(0.663)
7.有時候您會覺得做些惹麻煩的事反而刺激	2.39(0.663)	2.49(0.635)	2.21(0.683)
8.您偶爾會進行風險性金融投資	2.50(0.660)	2.60(0.610)	2.31(0.719)
冒險性(N=870):平均數=2.21、標準差=.616、偏態係數=-.132、峰度係數=-.480			

3.投機性

在低自我控制量表中，經探索性因素分析後所萃取出之第三個因子重新命名為「投機性」，其概念係由量表中之第 9 題至第 12 題所建構而成。在全體網路詐欺被害樣本中，以「您不喜歡艱鉅且挑戰極限的任務」平均得分 2.79 最高，其次則為「您會逃避您認為是比較困難的事情」、「只要有獲得報酬的機會，您就會進行投資行為」平均得分 2.74。其中，在男性被害組部分，以「您不喜歡艱鉅且挑戰極限的任務」平均得分 2.70 最高，其次則為「您會逃避您認為是比較困難的事情」平均得分 2.68。

在女性被害組部分，以「您不喜歡艱鉅且挑戰極限的任務」平均得分 2.96 最高、其次為「只要有獲得報酬的機會，您就會進行投資行為」平均得分 2.90。

全體受訪者在投機性構面之平均數為 2.43、標準差為.584、偏態係數為-.062、峰度係數為.555。網路詐欺被害各分組中，女性在各題項之投機性平均得分則高於男性。有關不同性別與網路詐欺被害在投機性程度之分析，如下表 4-1-14 所示:

表 4-1-14 網路詐欺被害各組樣本在投機性程度之分析

投機性	網路詐欺被害(平均數/標準差)		
	全體樣本 (N=142)	男性 (N=94)	女性 (N=48)
9.只要有獲得報酬的機會，您就會進行投資行為	2.74(0.973)	2.66(0.934)	2.90(1.036)
10.您會逃避您認為是比較困難的事情	2.74(0.814)	2.68(0.751)	2.85(0.922)
11.您不喜歡艱鉅且挑戰極限的任務	2.79(0.733)	2.70(0.701)	2.96(0.771)
12.您會關心眼前即將發生的事，較少考慮以後發生的事	2.60(0.808)	2.52(0.800)	2.75(0.812)
投機性(N=870): 平均數=2.43、標準差=.584、偏態係數=-.062、峰度係數=.555			

第二節 性別與網路詐欺被害在各主要變項之差異分析

一、調查樣本重新分組

本研究為避免調查樣本在卡方檢定中出現部份細格之期望(理論)次數小於 5 進而造成計算值產生偏誤,以及組數過多造成統計分析解讀困難,故將彙整所得之調查樣本,依據部分類別變項進行重新合併與分組,以符合本研究之目的與實際統計分析之需求,有關重新分組後之類別資料包括:年齡、職業、收入、教育程度、婚姻狀況等 5 個變項(詳如表 4-2-1),以下茲就重新分組後各組情形分述如下:

(一)年齡:由原本六組重新分組為四組,除原本 18 歲以下組 36 名(4.1%)及 60 歲以上組 92 名(10.6%)兩組未更動外,將原本 19 至 29 歲組 202 名(23.3%)、30 至 29 歲組 191 名(22.0%)兩組合併為 19 至 39 歲組 393 名(45.2%),而 40 至 49 歲組 193 名(22.2%)、50 至 59 歲組 156 名(17.9%)兩組合併為 40 至 59 歲組 349 名(40.1%)。年齡分組依序為: 18 歲以下、19 至 39 歲、40 至 59 歲及 60 歲以上四組。

(二)職業:由原本七組重新分組為五組,除原本學生組 231 名(26.6%)、軍警公教人員 151 名(17.4%)及技術員及助理專業人員 144 名(16.6%)三組未更動外,將原本未就業(含退休)組 83 名(9.5%)、從事家庭管理組 64 名(7.4%)兩組合併為未就業(含退休、家管)組 147 名(16.8%),而原本服務、事務工作人員組 176 名(20.2%)、行政主管及經理人員組 21 名(2.4%)兩組合併為服務、事務工作人員組 197 名(22.6%)。職業分組依序為:未就業(含退休、家管)、學生、軍警公教人員、服務及事務工作人員、技術員與助理專業人員五組。

(三)收入:由原本六組重新分組為五組,除將 9 萬以上至 12 萬未滿組 35 名(4.0%)、12 萬元以上組 13 名(1.5%)兩組合併為 9 萬元以上組 48 名(5.5%),其餘未滿 1 萬元組 206 名(23.7%)、1 萬以上至 3 萬未滿組 224 名(25.7%)、3 萬以上至 6 萬未滿組 236 名(27.2%)及 6 萬以上至 9 萬未滿組 156 名(17.9%)四組均未更動。收入分組依序為:未滿 1 萬元、1 萬以上至 3 萬未滿、3 萬以上至 6 萬未滿、6 萬以上至 9 萬未滿,以及 9 萬元以上五組。

(四)教育程度:由原本五組重新分組為四組,除將國小(肄)畢業組 1 名(0.1%)、國中(肄)畢業組 22 名(2.5%)兩組合併為國中(肄)畢業以下組 23 名(2.6%),其餘高中、高職(肄)畢業組 122 名(14.1%)、專科、大學(肄)畢業組 477 名(54.8%)及研究所(肄)畢業以上 248 名(28.5%)則未更動。

(五)婚姻狀況:由原本六組重新分組為四組,除單身組 419 名(48.1%)、未婚(非單身)組 191 名(22.0%)兩組未更動外,將原本已婚(含同居)組 224 名(25.7%)及再婚組 7 名(0.8%)兩組合併為已婚(含同居、再婚)組 231 名(26.6%),而離婚(含分居)組 20 名(2.3%)及喪偶組 9 名(1.0%)兩組合併為離婚(含分居、喪偶)組 29 名(3.3%)。

表 4-2-1 調查樣本重新分組分析表(N=870)

人口特性	組別	人數	百分比(%)
年齡	18 歲以下	36	4.1
	19-39 歲	393	45.2
	40-59 歲	349	40.1
	60 歲以上	92	10.6
職業	未就業(含退休、家管)	147	16.8
	學生	231	26.6
	軍警公教人員	151	17.4
	服務、事務工作人員	197	22.6
	技術員及助理專業人員	144	16.6
收入	未滿 1 萬元	206	23.7
	1 萬以上至 3 萬未滿	224	25.7
	3 萬以上至 6 萬未滿	236	27.2
	6 萬以上至 9 萬未滿	156	17.9
	9 萬元以上	48	5.5
教育程度	國中(肄)畢業以下	23	2.6
	高中、高職(肄)畢業	122	14.1
	專科、大學(肄)畢業	477	54.8
	研究所(肄)畢業以上	248	28.5
婚姻狀況	單身	419	48.1
	未婚(非單身)	191	22.0
	已婚(含同居、再婚)	231	26.6
	離婚(含分居、喪偶)	29	3.3

二、卡方檢定

本研究於卡方檢定之差異分析部分，分別就性別、是否被害、以及性別與是否被害等三個部分，檢驗其與各研究變項間是否具有顯著差異，故在檢定結果之呈現，係依據性別、是否被害及性別與網路詐欺是否被害等三個部分加以敘述，茲分次敘述如下:

(一)性別與各變項之差異分析

1.性別與網路生活型態之差異性

在性別與每次上網時數方面，由下表 4-2-2 可知，男性與女性皆以每次上網 3 小時以上至未滿 7 小時(中上網時數組)占最多數，而兩性在每次上網時數各組之差異，並未達統計上之顯著水準(χ^2=2.330 ; d.f.=2 ; p>.05)，顯示不同性別在每次上網時數部分並未有明顯差異。

表 4-2-2 性別與每次上網時數之差異性分析

性別	每次上網時數(次數/%)			卡方值 自由度 (顯著水準)
	未滿 3 小時 (低上網時數組)	3 小時以上至未滿 7 小時 (中上網時數組)	7 小時以上 (高上網時數組)	
男性	136(52.3)	236(54.3)	83(47.4)	χ^2=2.330 d.f.=2
女性	124(47.7)	199(45.7)	92(52.6)	

在性別與每周上網次數方面，由下表 4-2-3 可知，男性與女性皆以每周上網 10 次以上(高上網次數組)占最多數，而兩性在每周上網次數各組之差異，並未達統計上之顯著水準(χ^2=5.445 ; d.f.=2 ; p>.05) ，顯示不同性別在每周上網次數並未有明顯差異。

表 4-2-3 性別與每周上網次數之差異性分析

性別	每周上網次數(次數/%)			卡方值;自由度 (顯著水準)
	未滿 7 次 (低上網次數組)	7 至 9 次 (中上網次數組)	10 次以上 (高上網次數組)	
男性	54(60.7)	71(45.5)	330(52.8)	χ^2=5.445 d.f.=2
女性	35(39.3)	85(54.5)	295(47.2)	

在性別與平日上網時段方面，由下表 4-2-4 可知，不同性別之網路使用者，平日皆以在夜間時段上網(16：01- 00：00)占最大多數，而兩性在平日上網各時段之差異，並未達統計上之顯著水準(χ^2=1.091 ; d.f.=2 ; p>.05)，顯示不同性別在平日上網時段部分並未有顯著差異。

表 4-2-4 性別與平日上網時段之差異性分析

性別	平日上網時段(次數/%)			卡方值 自由度 (顯著水準)
	08：01-16：00 (白天上網時段)	16：01- 00：00 (夜間上網時段)	00：01- 08：00 (深夜上網時段)	
男性	59(48.0)	372(53.1)	24(52.2)	χ^2=1.091 d.f.=2
女性	64(52.0)	329(46.9)	22(47.8)	

在性別與假日上網時段方面，由下表 4-2-5 可知，不同性別之網路使用者，假日皆以在夜間時段上網(16：01- 00：00)占最大多數，經檢定後發現，兩性在假日上網時段之差異，達統計上之顯著水準(χ^2=6.972 ; d.f.=2 ; p<.05)，其中，女性在白天時段(08：01-16：00)上網之比例(55.1%)顯著高於女性(44.9%)，但男性在深夜時段上網(00：01- 08：00)之比例(60.8%)卻顯著高於女性(39.2%)。由此可知，在白天上網時段部分女性比例顯著高於男性，但在夜間上網時段男性比例比例則多於女性，在深夜時段上網者，男性比例更是顯著高於女性。

表 4-2-5 性別與假日上網時段之差異性分析

性別	假日上網時段(次數/%)			卡方值 自由度 (顯著水準)
	08：01-16：00 (白天上網時段)	16：01- 00：00 (夜間上網時段)	00：01- 08：00 (深夜上網時段)	
男性	89(44.9)	318(53.6)	48(60.8)	**χ^2=6.972*** d.f.=2
女性	109(55.1)	275(46.4)	31(39.2)	

註:*P<.05

在性別與接觸網路時間方面，由下表 4-2-6 可知，不同性別之網路使用者，在網路接觸時間上以接觸網路 10 年以上占最高比例，而不同性別網路使用者在接觸網路時間各分組，並未達統計上之顯著水準(χ^2=2.845 ; d.f.=3 ; p>.05)，顯示不同性別在接觸網路時間上並未具顯著差異。

表 4-2-6 性別與接觸網路時間之差異性分析

性別	接觸網路時間(次數/%)				卡方值 自由度 (顯著水準)
	3 年未滿	3 年以上 5 年未滿	5 年以上 10 年未滿	10 年以上	
男性	5(38.5)	28(47.5)	110(49.8)	312(54.1)	χ^2=2.845 d.f.=3
女性	8(61.5)	31(52.5)	111(50.2)	265(45.9)	

在性別與經常上網地點方面，由下表 4-2-7 可知，男性以經常在家中(租屋處)上網占最高比例、其次為在工作場所上網，而女性亦以經常在家中(租屋處)上網占最高比例、其次則為在學校(圖書館)上網，而經檢定後，不同性別在與經常上網地點各分組，並未達統計上之顯著水準(χ^2=9.914 ; d.f.=5 ; p>.05)，顯示不同性別與經常上網地點並不具顯著差異。

表 4-2-7 性別與經常上網地點之差異性分析

性別	經常上網地點(次數/%)[13]						卡方值 自由度 (顯著水準)
	家中 (租屋處)	學校 (圖書館)	朋友 (同學)家	網咖	公共場所	工作場所	
男性	404(51.3)	165(46.7)	52(52.5)	14(70.0)	137(51.1)	220(56.5)	χ^2=9.914 d.f.=5
女性	382(48.7)	188(53.3)	47(47.5)	6(30.0)	131(48.9)	169(43.5)	

[13] 本題為複選題，故表格中呈現之次數係為各回答題項之統計次數。

在性別與經常上網原因方面，由下表 4-2-8 可知，經卡方檢定結果後，不同性別在與經常上網原因達統計上之顯著差異(χ^2=54.296 ; d.f.=6 ; p<.01)，其中，男性在經常上網原因以抒發情緒占最高比例、其次為休閒娛樂，女性在經常上網原因則以買賣東西占最高比例，但其次則為搜尋資料。

表 4-2-8 性別與經常上網原因之差異性分析

性別	經常上網原因(次數/%)[14]							卡方值 自由度 (顯著水準)
	抒發情緒	搜尋資料	買賣東西	交友聊天	休閒娛樂	尋找新奇事物	收發信件	
男性	229 (55.9)	352 (50.7)	185 (46.2)	246 (50.9)	276 (55.3)	162 (54.7)	198 (53.6)	**χ^2=54.296****
女性	180 (44.1)	342 (49.3)	215 (53.8)	237 (49.1)	223 (44.7)	134 (45.3)	171 (46.4)	d.f.=6

註:**p<.01

2.性別與網路詐欺被害經驗之差異性

在性別與網路詐欺被害經驗之差異性分析部分，本研究以性別與網路詐欺被害經驗有關變項進行差異性分析，其中包括:是否被害、被害類型、交易方式、是否與加害者互動、互動方式、是否報案及報案方式，分析內容敘述如下:

在性別與是否被害方面，由下表 4-2-9 可知，不同性別在網路詐欺被害與否達統計上之顯著差異(χ^2=12.482 ; d.f.=1 ; p<.001)，其中，在有網路詐欺被害經驗中，男性共有 94 位(66.2%)，顯著高於女性 48 位(33.8%)曾有網路詐欺被害經驗，有關性別與網路詐欺被害之差異性分析如下表 4-2-9 所示:

表 4-2-9 性別與網路詐欺被害之差異性分析

性別	是否被害(次數/%)		卡方值;自由度 (顯著水準)
	是	否	
男性	94(66.2)	361(49.6)	**χ^2=12.482***[15]
女性	48(33.8)	367(50.4)	d.f.=1

註:***p<.001

[14] 本題為複選題，故表格中呈現之次數係為各回答題項之統計次數。

[15] Pearson 卡方值為 13.140，因本表係 2x2 表格，故使用 Yate's 連續校正卡方值 12.482。

在性別與網路詐欺被害類型方面，由下表 4-2-10 可知，不同性別在網路詐欺被害類型達統計上之顯著水準(χ^2=20.328 ; d.f.=4 ; p<.01)，顯示性別與網路詐欺被害類型具有顯著差異，男性在網路詐欺被害類型中，商業金融詐欺、網路遊戲(賭博)詐欺及網路交友(色情網站)詐欺，均顯著高於女性。有關性別與網路詐欺被害類型之差異性分析如下表 4-2-10 所示:

表 4-2-10 性別與網路詐欺被害之差異性分析

性別	網路詐欺被害類型(次數/%)					卡方值 自由度 (顯著性)
	網路購物詐欺(買方)	網路購物詐欺(賣方)	商業金融詐欺	網路遊戲(賭博)詐欺	網路交友(色情網站)詐欺	
男性	46(57.5)	5(35.7)	7(87.5)	13(100.0)	23(85.1)	**χ^2=20.328**[16]
女性	34(42.5)	9(64.3)	1(12.5)	0(0.0)	4(14.9)	d.f.=4

註:**p<.01

在性別最近一次網路詐欺被害損失方面，由下表 4-2-11 可知，不同性別在最近一次網路詐欺被害金額未達統計上之顯著水準(χ^2=3.897 ; d.f.=3 ; p>.05)，雖然兩性皆以 1 萬以上未滿 5 萬元比例最高，但卡方檢定後，性別與網路詐欺被害金額不具顯著差異，有關性別與網路詐欺被害金額之差異性分析如下表 4-2-11 所示:

表 4-2-11 性別與網路詐欺被害損失金額之差異性分析

性別	網路詐欺被害損失金額(次數/%)				卡方值 自由度 (顯著性)
	5000 元以下	5000 至 1 萬元	1 萬以上未滿 5 萬元	5 萬元以上	
男性	32(71.1)	13(50.0)	36(67.9)	13(72.2)	χ^2=3.897
女性	13(28.9)	13(50.0)	17(32.1)	5(27.8)	d.f.=3

[16] Pearson 卡方值為 21.460，但因細格中有 3 單位期望次數小於 5，故採用 Fisher 精確檢定卡方值 20.328。

在性別與網路詐欺被害交易方式方面，由下表 4-2-12 可知，不同性別在網路詐欺被害交易方式並未達統計上之顯著水準(χ^2=4.205 ; d.f.=4 ; p>.05)，顯示性別與網路詐欺被害交易方式並不具顯著差異，有關性別與網路詐欺被害交易方式之差異性分析如下表 4-2-12 所示:

表 4-2-12 性別與網路詐欺被害交易方式之差異性分析

性別	網路詐欺被害交易方式(次數/%)					卡方值;自由度（顯著水準）
	現金交付	ATM 轉帳	金融機構匯款	網路銀行付款	其他	
男性	4(57.1)	36(65.5)	35(74.5)	10(50.0)	9(69.2)	χ^2=4.205[17]
女性	3(42.9)	19(34.5)	12(25.5)	10(50.0)	4(30.8)	d.f.=4

在性別與網路詐欺與網路詐欺加害者關係方面，由下表 4-2-13 可得知，不同性別網路詐欺被害者與加害者間之關係並未達統計上之顯著水準(χ^2=3.313 ; d.f.=3 ; p>.05)，顯示不同性別網路詐欺被害者與加害者關係不具顯著差異，其中，不同性別網路詐欺被害者與加害者關係雖然皆以陌生人占最高比例，但經卡方檢定後則未達顯著差異性，有關不同性別網路詐欺被害者與網路詐欺加害者關係之差異性分析，如下表 4-2-13 所示:

表 4-2-13 性別與網路詐欺加害者關係之差異性分析

性別	網路詐欺被害與加害者關係(次數/%)				卡方值 自由度（顯著性）
	同學	朋友或同事	陌生人	其他	
男性	5(100.0)	10(58.8)	71(67.6)	7(53.8)	χ^2=3.313[18]
女性	0(0.0)	7(41.2)	34(32.4)	6(46.2)	d.f.=3

[17] Pearson 卡方值為 4.105，但因細格中有 3 單位期望次數小於 5，故採用 Fisher 精確檢定卡方值 4.205。
[18] Pearson 卡方值為 3.035，但因細格中有 1 單位期望次數小於 5，故採用 Fisher 精確檢定卡方值 3.313。

在性別與是否與網路詐欺加害者互動方面，由下表 4-2-14 可知，不同性別在是否與網路詐欺加害者互動達統計上之顯著水準(χ^2=7.112 ; d.f.=1 ; p<.01)，顯示性別與是否與加害者互動具有顯著差異，其中，男性有 76 位(73.1%)曾在網路詐欺被害之過程中與加害者互動，顯著高於女性 28 位(26.9%)與加害者互動，有關性別與是否與加害者互動之差異性分析如下表 4-2-14 所示:

表 4-2-14 性別與是否與加害者互動之差異性分析

性別	是否與加害者互動(次數/%)		卡方值;自由度（顯著水準）
	是	否	
男性	76(73.1)	18(47.4)	**χ^2=7.112**[**19]
女性	28(26.9)	20(52.6)	d.f.=1

註:**p<.01

在不同性別與網路詐欺加害者之互動方式方面，由下表 4-2-15 可知，不同性別在網路詐欺被害過程中與加害者互動方式達統計上之顯著水準(χ^2=18.346 ; d.f.=3 ; p<.01)，顯示不同性別與加害者互動方式具有顯著差異，其中，男性與網路詐欺加害者之互動方式無論在拍賣網站、即時通訊軟體(含網路電話)、網路社群網站或線上遊戲(含其他)，均顯著高於女性。有關性別與是否與網路詐欺加害者互動之差異性分析如下表 4-2-15 所示:

表 4-2-15 性別與加害者互動方式之差異性分析

性別	與加害者互動方式(次數/%)				卡方值 自由度（顯著水準）
	拍賣網站	即時通訊軟體（含網路電話）	網路社群網站	線上遊戲（含其他）	
男性	16(64.0)	23(88.4)	24(63.1)	13(86.6)	**χ^2=18.346**[**20]
女性	9(36.0)	3(11.6)	14(36.9)	2(13.4)	d.f.=3

註:**p<.01

[19] Pearson 卡方值為 8.220，因本表係 2x2 表格，故使用 Yate's 連續校正卡方值 7.112。

[20] Pearson 卡方值為 18.134,但因細格中有 2 單位期望次數小於 5,故採用 Fisher 精確檢定卡方值 18.346。

在性別與如何得知網路詐欺被害方面，由下表 4-2-16 可知，不同性別在如何得知網路詐欺被害未達統計上之顯著水準(χ^2=3.561 ; d.f.=3 ; p>.05)。雖然不同性別網路詐欺被害者皆以自己察覺占最高比例，但經檢定後發現，不同性別與如何得知網路詐欺被害各組並未有顯著差異。有關性別與是否與如何得知網路詐欺被害之差異性分析如下表 4-2-16 所示:

表 4-2-16 性別與如何得知被害之差異性分析

性別	如何得知被害(次數/%)				卡方值 自由度 (顯著水準)
	自己察覺	朋友與同事發現	親人發現	其他	
男性	67(69.0)	16(66.6)	5(38.4)	6(75.0)	χ^2=3.561[21] d.f.=3
女性	30(31.0)	8(33.4)	8(61.6)	2(25.0)	

在性別與多久發現網路詐欺被害方面，由下表 4-2-17 可知，不同性別網路詐欺被害者在多久發現網路詐欺被害未達統計上之顯著水準(χ^2=1.421 ; d.f.=3 ; p>.05)。雖然不同性別網路詐欺被害者皆以被害發生後 4 至 6 天內發現自己被害占最高比例，但經卡方檢定後發現，不同性別被害者與多久發現網路詐欺被害並未有顯著差異。有關不同性別網路詐欺被害者與多久發現網路詐欺被害之差異性分析如下表 4-2-17 所示:

表 4-2-17 性別與多久發現自己被害之差異性分析

性別	多久發現自己被害(次數/%)				卡方值 自由度 (顯著水準)
	3 天以內	4 至 6 天	7 至 14 天	14 天以上	
男性	27(62.8)	46(70.8)	17(63.0)	4(57.1)	χ^2=1.421[22] d.f.=3
女性	16(37.2)	19(29.2)	10(37.0)	3(42.9)	

[21] Pearson 卡方值為 4.062，但因細格中有 1 單位期望次數小於 5，故採用 Fisher 精確檢定卡方值 3.561。
[22] Pearson 卡方值為 1.213，但因細格中有 2 單位期望次數小於 5，故採用 Fisher 精確檢定卡方值 1.421。

在性別與網路詐欺被害是否報案方面，由下表 4-2-18 可知，不同性別在網路詐欺被害後是否報案未達統計上之顯著水準(χ^2=0.010 ; d.f.=1 ; p>.05)，顯示性別與網路詐欺被害後是否報案未有顯著差異。男性被害者中有 40 位(66.7%)在網路詐欺被害後報案，女性被害者則有 20 位(33.3%)在網路詐欺被害後報案，有關性別與是否與網路詐欺被害後是否報案之差異性分析如下表 4-2-18 所示:

表 4-2-18 性別與是否報案之差異性分析

性別	是否報案(次數/%)		卡方值;自由度（顯著水準）
	是	否	
男性	40(66.7)	54(65.9)	χ^2=0.010[23] d.f.=1
女性	20(33.3)	28(34.1)	

在性別與網路詐欺被害後之報案方式，由下表 4-2-19 可知，不同性別在網路詐欺被害後之報案方式未達統計上之顯著水準(χ^2=2.232 ; d.f.=1 ; p>.05)，其中，男性與女性在網路詐欺被害後親自到警察單位報案者占最多數，但經統計後發現，性別與網路詐欺被害後之各組報案方式未有顯著差異。有關性別與網路詐欺被害後之報案方式之差異性分析如下表 4-2-19 所示:

表 4-2-19 性別與報案方式之差異性分析

性別	報案方式(次數/%)		卡方值;自由度（顯著水準）
	電信報案（含網路、電話、傳真）	親自到警察單位報案	
男性	9(50.0)	31(73.8)	χ^2=2.232[24] d.f.=1
女性	9(50.0)	11(26.2)	

[23] Pearson 卡方值為 0.112，因本表係 2x2 表格，故使用 Yate's 連續校正卡方值 0.010。
[24] Pearson 卡方值為 3.214，因本表係 2x2 表格，故使用 Yate's 連續校正卡方值 2.232。

(二)網路詐欺被害與各變項之差異分析

1.個人基本特性與網路詐欺被害之差異性

在個人基本特性與網路詐欺被害是否有顯著差異性方面,經卡方檢定之分析結果如下表 4-2-20。從表中可以得知,個人基本特性中之性別、年齡、職業、收入、教育程度均與網路詐欺被害有顯著差異性,婚姻狀況與網路詐欺被害則未達統計上之顯著水準,有關個人基本特性與網路詐欺被害之差異性分析茲分述如下:

在性別與網路詐欺被害方面,經卡方檢定分析顯示,不同性別與是否曾有網路詐欺被害經驗之差異,達統計上之顯著水準(χ^2=12.482 ; d.f.=1 ; p<.001),其中,在網路詐欺被害中,男性被害者 94 位(66.2%)顯著大於女性被害者 48 位(33.8%)。

在年齡與網路詐欺被害經驗方面,經卡方檢定分析結果顯示,不同年齡與是否曾有網路詐欺被害經驗之差異,達統計上之顯著水準(χ^2=37.935 ; d.f.=3 ; p<.001),其中,具有網路詐欺被害經驗者之年齡,以 19-39 歲占 64.1%最多、其次為 40-59 歲占 19.0%。

在收入與網路詐欺被害經驗方面,經卡方檢定分析結果顯示,不同收入與是否曾有網路詐欺被害經驗之差異,達統計上之顯著水準(χ^2=59.908 ; d.f.=4 ; p<.001),其中,具有網路詐欺被害經驗者,收入以 1 萬以上至 3 萬未滿占 50.7%最多。

在職業與網路詐欺被害經驗方面,經卡方檢定分析結果顯示,不同職業與是否曾有網路詐欺被害經驗之差異,達統計上之顯著水準(χ^2=36.609 ; d.f.=4 ; p<.001),其中,具有網路詐欺被害經驗者之職業,以學生占 35.3%最多、其次為未就業(退休)占 29.5%。

在教育程度與網路詐欺被害經驗方面,經卡方檢定分析結果顯示,不同教育程度與是否曾有網路詐欺被害經驗之差異,達統計上之顯著水準(χ^2=30.492 ; d.f.=3 ; p<.001),其中,具有網路詐欺被害經驗者之教育程度以大學畢(肄)業占 61.3%最多。

在婚姻狀況與網路詐欺被害經驗方面,雖曾有被害經驗或未曾有被害經驗者,均以單身者占最高比例,但經卡方檢定分析結果顯示,不同婚姻狀況與是否曾有網路詐欺被害經驗之差異,未達統計上之顯著水準(χ^2=4.757 ; d.f.=3 ; p>.05)。

表 4-2-20 個人基本特性與網路詐欺被害之差異性分析(N=870)

變項名稱	組別	網路詐欺被害(次數/百分比)			卡方值;自由度（顯著水準）
		是(%)	否(%)	總計(%)	
性別	男性	94(66.2)	361(49.6)	455(52.3)	χ^2=**12.482*****[25] d.f.=1
	女性	48(33.8)	367(50.4)	415(47.7)	
	總和	142(100.0)	728(100.0)	870(100.0)	
年齡	18 歲以下	11(7.7)	25(3.4)	36(4.1)	χ^2=**37.935***** d.f.=3
	19-39 歲	91(64.1)	302(41.5)	393(45.2)	
	40-59 歲	27(19.0)	322(44.2)	349(40.1)	
	60 歲以上	13(9.2)	79(10.9)	92(10.6)	
	總和	142(100.0)	728(100.0)	870(100.0)	
職業	未就業(退休、家管)	42(29.5)	105(14.4)	105(14.4)	χ^2=**36.609***** d.f.=4
	學生	50(35.3)	181(24.9)	181(24.9)	
	軍警公教人員	10(7.1)	141(19.4)	141(19.4)	
	服務、事務人員	23(16.2)	174(23.9)	174(23.9)	
	技術員及助理人員	17(11.9)	127(17.4)	127(17.4)	
	總和	142(100.0)	728(100.0)	870(100.0)	
收入	未滿 1 萬元	17(11.9)	189(26.0)	204(23.4)	χ^2=**59.908***** d.f.=4
	1 萬以上至 3 萬未滿	72(50.7)	152(20.9)	220(25.3)	
	3 萬以上至 6 萬未滿	27(19.0)	209(28.7)	237(27.2)	
	6 萬以上至 9 萬未滿	16(11.2)	140(19.2)	160(18.4)	
	9 萬元以上	10(7.2)	38(5.2)	49(5.6)	
	總和	142(100.0)	728(100.0)	870(100.0)	
教育程度	國中畢(肄)業以下	12(8.5)	11(1.5)	23(2.6)	χ^2=**30.492*****[26] d.f.=3
	高中專科畢(肄)業	22(15.5)	100(13.7)	122(14.0)	
	大學畢(肄)業	87(61.3)	390(53.6)	477(54.8)	
	研究所畢(肄)業以上	21(14.8)	227(31.2)	248(28.5)	
	總和	142(100.0)	728(100.0)	870(100.0)	
婚姻狀況	單身	77(54.2)	342(47.0)	419(48.2)	χ^2=4.757[27] d.f.=3
	未婚(非單身)	27(19.0)	164(22.5)	191(22.0)	
	已婚(同居、再婚)	31(21.8)	200(27.5)	231(26.6)	
	離婚(分居、喪偶)	7(4.9)	22(3.0)	29(3.3)	
	總和	142(100.0)	728(100.0)	870(100.0)	

註:*p<.05 ; ***p<.001

[25] Pearson 卡方值為 13.140，因本表係 2x2 表格，故使用 Yate's 連續校正卡方值 12.482。
[26] Pearson 卡方值為 34.392,但因細格中有 1 單位期望次數小於 5,故採用 Fisher 精確檢定卡方值 30.492。
[27] Pearson 卡方值為 4.685，但因細格中有 1 單位期望次數小於 5，故採用 Fisher 精確檢定卡方值 4.757。

2.網路使用特性與網路詐欺被害之差異性

在網路使用特性與網路詐欺被害是否有顯著差異性方面，經卡方檢定之分析結果如下表 4-2-21。從表中可以得知，網路使用特性中之每次上網時數、每周上網次數、平日上網時段、假日上網時段、最常上網地點、最常上網原因，均與網路詐欺被害具有顯著差異性，而接觸網路時間與網路詐欺被害則未達統計上之顯著水準。有關網路使用特性與網路詐欺被害之差異性分析內容茲分述如下:

在每次上網時數與網路詐欺被害方面，經卡方檢定分析顯示，每次上網時數與是否曾有網路詐欺被害經驗之差異，達統計上之顯著水準(χ^2=28.270 ; d.f.=2 ; p<.001)，其中，在網路詐欺被害者中，以每次上網 3 至 7 小時（中上網時數）者(69.0%)占最高比例，顯著高於未被害者(46.3%)。

在每周上網次數與網路詐欺被害方面，經卡方檢定分析顯示，每周上網次數與是否曾有網路詐欺被害經驗之差異，達統計上之顯著水準(χ^2=31.923 ; d.f.=2 ; p<.001)，其中，在網路詐欺被害者中，以每周上網 10 次以上（高上網次數）者(58.5%)占最高比例，顯著高於未被害者(14.6%)。

在平日上網時段與網路詐欺被害方面，經卡方檢定分析顯示，平日上網時段與是否曾有網路詐欺被害經驗之差異，達統計上之顯著水準(χ^2=31.270 ; d.f.=2 ; p<.001)，其中，網路詐欺被害及未被害者，雖皆以平日在 16:01 至 00:00（夜間時段）上網者占最高比例，但網路詐欺未被害者平日在 08：01-16：00（白天時段）上網比例(16.2%)顯著高於被害者(3.5%)，而網路詐欺被害者平日在 00：01-08：00（深夜時段）上網之比例(12.7%)則顯著高於未被害者(3.9%)。

在假日上網時段與網路詐欺被害方面，經卡方檢定分析顯示，假日上網時段與是否曾有網路詐欺被害經驗之差異，達統計上之顯著水準(χ^2=107.662 ; d.f.=2 ; p<.001)，其中，網路詐欺被害及未被害者，雖皆以假日在 16:01 至 00:00（夜間時段）上網者占最高比例，但網路詐欺未被害者假日在 08：01-16：00（白天時段）上網比例(25.7%)顯著高於被害者(7.7%)，而網路詐欺被害者假日在 00：01-08：00（深夜時段）上網之比例(31.0%)則顯著高於未被害者(4.8%)。

在接觸網路時間與網路詐欺被害方面，雖曾有被害經驗或未曾有被害經驗者，均以接觸網路 10 年以上占最高比例，但經卡方檢定後發現，接觸網路時間與是否曾有網路詐欺被害經驗之差異，並未達統計上之顯著水準(χ^2=2.212 ; d.f.=3 ; p>.05)。

在最常上網地點與網路詐欺被害方面，經卡方檢定分析顯示，最常上網地點與是否曾有網路詐欺被害經驗之差異，達統計上之顯著水準(χ^2=35.932 ; d.f.=5 ; p<.001)，其中，在網路詐欺被害者中，以最常在家中(租屋處)上網者(36.8%)占最高的被害比例，其次為最常在工作場所上網者(28.8%)。

在最常上網原因與網路詐欺被害方面，經卡方檢定分析顯示，最常上網原因與是否曾有網路詐欺被害經驗之差異，達統計上之顯著水準(χ^2=54.296 ; d.f.=7 ; p<.001)，其中，在網路詐欺被害者中，以最常上網搜尋資料者(22.5%)占最高的被害比例。

表 4-2-21 網路使用特性與網路詐欺被害之差異性分析(N=870)

變項名稱	組別	網路詐欺被害(次數/百分比)			卡方值;自由度（顯著水準）
		是(%)	否(%)	總計(%)	
每次上網時數	未滿 3 小時(低)	19(13.4)	241(33.1)	260(29.9)	**χ^2=28.270***** d.f.=2
	3 至 7 小時(中)	98(69.0)	337(46.3)	435(50.0)	
	7 小時以上(高)	25(17.6)	150(20.6)	175(20.1)	
	總和	142(100.0)	728(100.0)	870(100.0)	
每周上網次數	未滿 7 次(低)	10(7.0)	79(10.9)	89(10.2)	**χ^2=31.923***** d.f.=2
	7 至 9 次(中)	49(34.5)	107(14.6)	156(18.0)	
	10 次以上(高)	83(58.5)	542(74.5)	625(71.8)	
	總和	142(100.0)	728(100.0)	870(100.0)	
平日上網時段	08:01-16:00(白天)	5(3.5)	118(16.2)	123(14.1)	**χ^2=31.270***** d.f.=2
	16:01-00:00(夜間)	119(83.8)	582(79.9)	701(80.6)	
	00:01-08:00(深夜)	18(12.7)	28(3.9)	46(5.3)	
	總和	142(100.0)	728(100.0)	870(100.0)	
假日上網時段	08:01-16:00(白天)	11(7.7)	187(25.7)	198(22.8)	**χ^2=107.662***** d.f.=2
	16:01-00:00(夜間)	87(61.3)	506(69.5)	593(69.2)	
	00:01-08:00(深夜)	44(31.0)	35(4.8)	79(9.0)	
	總和	142(100.0)	728(100.0)	870(100.0)	

接觸網路時間	3 年未滿	3(2.1)	10(1.4)	13(1.5)	χ^2=2.212[28] d.f.=3
	3 年以上 5 年未滿	13(9.2)	46(6.3)	59(6.8)	
	5 年以上 10 年未滿	37(26.0)	184(25.3)	221(25.4)	
	10 年以上	89(62.7)	488(67.0)	577(66.3)	
	總和	142(100.0)	728(100.0)	870(100.0)	
最常上網地點[29]	家中(租屋處)	137(36.8)	649(42.1)	786(41.0)	**χ^2=35.932*[30]** d.f.=5
	學校(圖書館)	43(11.6)	310(20.1)	353(18.4)	
	朋友(同學)家	28(7.5)	71(4.6)	99(5.2)	
	網咖	6(1.6)	14(0.9)	20(1.0)	
	公共場所	51(13.7)	217(14.0)	268(14.1)	
	工作場所	107(28.8)	282(18.3)	389(20.3)	
	總和	372(100.0)	1543(100.0)	1915(100.0)	
最常上網原因[31]	抒發情緒	180(11.8)	229(13.1)	409(12.4)	**χ^2=54.296*** d.f.=7
	搜尋資料	342(22.5)	352(20.1)	694(21.2)	
	買賣東西	215(14.1)	185(10.6)	400(12.2)	
	交友聊天	237(15.6)	246(14.1)	483(14.8)	
	休閒娛樂	223(14.6)	276(15.8)	499(15.3)	
	尋找新奇事物	134(8.8)	162(9.3)	296(9.1)	
	收發信件	171(11.2)	198(11.3)	369(11.3)	
	滿足網愛	21(1.4)	99(5.7)	120(3.7)	
	總和	1523(100.0)	1747(100.0)	3270(100.0)	

註:*p<.05 ; ***p<.001

[28] Pearson 卡方值為 2.610，但因細格中有 1 單位期望次數小於 5，故採用 Fisher 精確檢定卡方值 2.212。
[29] 本題為複選題，故表格中呈現之次數係為各回答題項之統計次數。
[30] Pearson 卡方值為 36.482,但因細格中有 1 單位期望次數小於 5,故採用 Fisher 精確檢定卡方值 35.932。
[31] 本題為複選題，故表格中呈現之次數係為各回答題項之統計次數。

(三)性別、網路詐欺被害與網路使用特性之差異分析

為更深入探究不同性別、網路詐欺被害與否，在各項網路使用特性之差異，故在本分析中以性別為控制變項進行交叉分析，詳細分析敘述如下:

1.每次上網時數

由下表 4-2-22 得知，在男性網路使用者中，被害組與未被害組在每次上網時數之差異性達統計上之顯著水準(χ^2=18.446 ; d.f.=2 ; p<.001)，被害組每次上網 3 至 7 小時比例(69.1%)，顯著高於未被害組比例(47.4%)。在女性網路使用者中，被害組與未被害組在每次上網時數之差異性達統計上之顯著水準(χ^2=9.888 ; d.f.=2 ; p<.01)。被害組每次上網時數在 3 至 7 小時之比例(68.8%)，顯著高於未被害組(45.2%)。

在比較不同性別網路使用者之每次上網時數後，可以得知，無論是男性或女性，被害者上網時數較未被害者上網時數高，在性別部分，男性每次上網時數則高於女性。

2.每周上網次數

在男性網路使用者中，被害組與未被害組在每周上網次數之差異性，達統計上之顯著水準(χ^2=28.332 ; d.f.=2 ; p<.001)，其中，被害組與未被害組每周皆以上網 10 次以上最高。在女性網路使用者中，被害組與未被害組在每周上網次數之差異性達統計上之顯著水準(χ^2=9.008 ; d.f.=2 ; p<.01)。

在比較不同性別網路使用者是否被害之每周上網次數後，可以得知，無論是男性或女性，在是否曾遭受網路詐欺被害部分，均以每周上網 10 次以上最高。

3.平日上網時段

在男性網路使用者中，被害組與未被害組在平日上網時段之差異性達統計上之顯著水準(χ^2=18.729 ; d.f.=2 ; p<.001)。未被害組於平日 08:01 至 16:00(白天時段)上網比例(15.5%)顯著高於被害組(3.2%)，但被害組於平日 00:01 至 08:00(深夜時段)上網之比例(11.7%)則顯著高於未被害組(3.6%)。在女性網路使用者中，被害組與未被害組在平日上網時段之差異性達統計上之顯著水準(χ^2=12.128 ; d.f.=2 ; p<.01)。其中，未被害組於平日 08:01 至 16:00(白天時段)上網比例(16.9%)顯著高於被害組(4.1%)，但被害組於平日 00:01 至 08:00(深夜時段)上網比例(14.6%)則顯著高於未被害組(4.1%)。

在比較不同性別網路使用者是否被害之平日上網時段後，可以得知，在兩性網路使用者中，未被害者平日於 08:01 至 16:00(白天時段)上網者之比例均高於被害者比例，而被害者平日於 00:01 至 08:00(深夜時段)上網之比例，則顯著高於未被害者比例。

表 4-2-22 性別、網路詐欺被害與每次上網時數、每周上網次數之差異性分析

性別	網路使用特性		是否被害			卡方值 自由度 (顯著水準)
	變項名稱	組別	是	否	總和	
男	每次上網時數	未滿 3 小時(低)	12(12.8)	124(34.3)	136(29.9)	χ^2=**18.446***** d.f.=2
		3 至 7 小時(中)	65(69.1)	171(47.4)	236(51.9)	
		7 小時以上(高)	17(18.1)	66(18.3)	83(18.2)	
		總和	94(100.0)	361(100.0)	455(100.0)	
女	每次上網時數	未滿 3 小時(低)	7(14.5)	117(31.9)	124(29.9)	χ^2=**9.888**** d.f.=2
		3 至 7 小時(中)	33(68.8)	166(45.2)	199(48.0)	
		7 小時以上(高)	8(16.7)	84(22.9)	92(22.1)	
		總和	48(100.0)	367(100.0)	415(100.0)	
男	每周上網次數	未滿 7 次(低)	6(6.4)	48(13.3)	54(11.9)	χ^2=**28.332***** d.f.=2
		7 至 9 次(中)	31(33.0)	40(11.1)	71(15.6)	
		10 次以上(高)	57(60.6)	273(75.6)	330(72.5)	
		總和	94(100.0)	361(100.0)	455(100.0)	
女	每周上網次數	未滿 7 次(低)	4(8.3)	31(8.4)	35(8.4)	χ^2=**9.008****[32] d.f.=2
		7 至 9 次(中)	18(37.5)	67(18.3)	85(20.5)	
		10 次以上(高)	26(54.2)	269(73.3)	295(71.1)	
		總和	48(100.0)	367(100.0)	415(100.0)	
男	平日上網時段	08:01-16:00(白天)	3(3.2)	56(15.5)	59(13.0)	χ^2=**18.729*****[33] d.f.=2
		16:01-00:00(夜間)	80(85.1)	292(80.9)	372(81.8)	
		00:01-08:00(深夜)	11(11.7)	13(3.6)	24(5.2)	
		總和	94(100.0)	361(100.0)	455(100.0)	
女	平日上網時段	08:01-16:00(白天)	2(4.1)	62(16.9)	64(15.4)	χ^2=**12.128****[34] d.f.=2
		16:01-00:00(夜間)	39(81.3)	290(79.0)	329(79.3)	
		00:01-08:00(深夜)	7(14.6)	15(4.1)	22(5.3)	
		總和	48(100.0)	367(100.0)	415(100.0)	

註:**p<.01 ; ***p<.001

[32] Pearson 卡方值為 9.861，但因細格中有 1 單位期望次數小於 5，故採用 Fisher 精確檢定卡方值 9.008。
[33] Pearson 卡方值為 18.173，但因細格中有 1 單位期望次數小於 5，故採用 Fisher 精確檢定卡方值 18.729。
[34] Pearson 卡方值為 13.307，但因細格中有 1 單位期望次數小於 5，故採用 Fisher 精確檢定卡方值 12.128。

4.假日上網時段

由表 4-2-23 得知，在男性網路使用者中，被害組與未被害組在假日上網時段之差異性，達統計上之顯著水準(χ^2=75.789 ; d.f.=2 ; p<.001)。未被害組假日在 08:01 至 16:00(白天時段)上網者比例(23.5%)，顯著高於被害組之比例(4.2%)，而被害組假日在 00:01 至 08:00(深夜時段)上網之比例(36.2%)則顯著高於未被害組之比例(3.9%)。

在女性網路使用者中，被害組與未被害組在假日上網時段之差異性達統計上之顯著水準(χ^2=15.819 ; d.f.=2 ; p<.001)。未被害組假日在 08:01 至 16:00(白天時段)上網者比例(27.8%)，顯著高於被害組比例(14.6%)，而被害組假日在 00:01 至 08:00(深夜時段)上網比例(20.8%)則顯著高於未被害組比例(5.7%)。

在比較不同性別網路使用者是否被害之假日上網時段後，可以得知，無論在男性或女性網路使用者中，未被害者假日於 08:01 至 16:00(白天時段)上網者比例均顯著高於被害者比例，而被害者假日於 00:01 至 08:00(深夜時段)上網比例，則顯著高於未被害者比例。

表 4-2-23 性別、網路詐欺被害與假日上網時段之差異性分析

性別	網路使用特性		是否被害			卡方值 自由度 (顯著水準)
	變項名稱	組別	是	否	總和	
男	假日上網時段	08:01-16:00(白天)	4(4.2)	85(23.5)	89(19.6)	**χ^2=75.789*****[35] d.f.=2
		16:01-00:00(夜間)	56(59.6)	262(72.6)	318(69.9)	
		00:01-08:00(深夜)	34(36.2)	14(3.9)	48(10.5)	
		總和	94(100.0)	361(100.0)	455(100.0)	
女	假日上網時段	08:01-16:00(白天)	7(14.6)	102(27.8)	109(26.2)	**χ^2=15.819***** d.f.=2
		16:01-00:00(夜間)	31(64.6)	244(66.5)	275(66.3)	
		00:01-08:00(深夜)	10(20.8)	21(5.7)	31(7.5)	
		總和	48(100.0)	367(100.0)	415(100.0)	

註:***p<.001

[35] Pearson 卡方值為 89.899，但因細格中有 1 單位期望次數小於 5，故採用 Fisher 精確檢定卡方值 75.789。

5.接觸網路時間

由表 4-2-24 得知，在男性網路使用者中，被害組與未被害組在接觸網路時間之差異性，未達統計上之顯著水準(χ^2=3.983 ; d.f.=3 ; p>.05)。被害組接觸網路時間以 10 年以上(66.0%)占最高比例，而未被害組亦以 10 年以上(69.3%)占最高比例，經卡方檢定後發現，被害組與未被害組並未有顯著差異。

在女性網路使用者中，被害組與未被害組在接觸網路時間之差異性，未達統計上之顯著水準(χ^2=1.851 ; d.f.=3 ; p>.05)。由被害組接觸網路時間以 10 年以上(56.3%)占最高比例，而未被害組亦以 10 年以上(64.9%)占最高比例，經卡方檢定後發現，被害組與未被害組並未有顯著差異。

在比較不同性別網路使用者是否被害之接觸網路時間後，可以得知，無論是男性或女性，在是否曾有網路被害經驗部分，皆以接觸網路時間 10 年以上占最高比例，且經卡方檢定後發現，各組間並未有顯著差異。

表 4-2-24 性別、網路詐欺被害與接觸網路時間之差異性分析

性別	網路使用特性		是否被害			卡方值 自由度 （顯著水準）
	變項名稱	組別	是	否	總和	
男	接觸網路時間	3 年未滿	2(2.1)	3(0.8)	5(1.1)	χ^2=3.983[36] d.f.=3
		3 年以上 5 年未滿	9(9.6)	19(5.2)	28(6.1)	
		5 年以上 10 年未滿	21(22.3)	89(24.7)	110(24.2)	
		10 年以上	62(66.0)	250(69.3)	312(68.6)	
		總和	94(100.0)	361(100.0)	455(100.0)	
女	接觸網路時間	3 年未滿	1(2.1)	7(1.9)	8(1.9)	χ^2=1.851[37] d.f.=3
		3 年以上 5 年未滿	4(8.3)	27(7.3)	31(7.5)	
		5 年以上 10 年未滿	16(33.3)	95(25.9)	111(26.7)	
		10 年以上	27(56.3)	238(64.9)	265(63.9)	
		總和	48(100.0)	367(100.0)	415(100.0)	

[36] Pearson 卡方值為 3.677，但因細格中有 2 單位期望次數小於 5，故採用 Fisher 精確檢定卡方值 3.983。
[37] Pearson 卡方值為 1.433，但因細格中有 2 單位期望次數小於 5，故採用 Fisher 精確檢定卡方值 1.851。

6.經常上網地點

由下表 4-2-25 可知，在男性網路使用者中，被害組與未被害組在經常上網地點之差異，達統計上之顯著水準(χ^2=19.088 ; d.f.=5 ; p<.01)。被害組以在家中(租屋處)上網(35.7%)占最高比例，而未被害組亦以在家中(租屋處)上網(42.2%)占最高比例。

在女性網路使用者中，被害組與未被害組在接觸網路時間之差異性，達統計上之顯著水準(χ^2=17.097 ; d.f.=5 ; p<.01)。被害組以在家中(租屋處)上網(39.2%)占最高比例，而未被害組亦以在家中(租屋處)上網(41.7%)占最高比例。

在比較不同性別網路使用者是否被害之接觸網路時間後，可以得知，無論是男性或女性，在是否曾有網路被害經驗部分，各組皆以在家中上網占最高比例，而在性別部分，男性在家中(租屋處)上網比例則低於女性。

表 4-2-25 性別、網路詐欺被害與經常上網地點之差異性分析

性別	網路使用特性		是否被害			卡方值;自由度（顯著水準）
	變項名稱	組別	是	否	總和	
男	經常上網地點[38]	家中(租屋處)	90(35.7)	314(42.4)	404(40.7)	**χ^2=19.088**[**39] d.f.=5
		學校(圖書館)	28(11.1)	137(18.5)	165(16.6)	
		朋友(同學)家	17(6.7)	35(4.7)	52(5.2)	
		網咖	4(1.6)	10(1.4)	14(1.4)	
		公共場所	38(15.1)	99(13.4)	137(13.8)	
		工作場所	75(29.8)	145(19.6)	220(22.3)	
		總和	252(100.0)	740(100.0)	992(100.0)	
女	經常上網地點[40]	家中(租屋處)	47(39.2)	335(41.7)	382(41.4)	**χ^2=17.097**[**41] d.f.=5
		學校(圖書館)	15(12.5)	173(21.5)	188(20.4)	
		朋友(同學)家	11(9.2)	36(4.5)	47(5.0)	
		網咖	2(1.6)	4(0.5)	6(0.7)	
		公共場所	13(10.8)	118(14.7)	131(14.2)	
		工作場所	32(26.7)	137(17.1)	169(18.3)	
		總和	120(100.0)	803(100.0)	923(100.0)	

註:**p<.01

[38] 本題為複選題，故表格中呈現之次數係為各回答題項之統計次數。
[39] Pearson 卡方值為 18.964,但因細格中有 2 單位期望次數小於 5,故採用 Fisher 精確檢定卡方值 19.088。
[40] 本題為複選題，故表格中呈現之次數係為各回答題項之統計次數。
[41] Pearson 卡方值為 17.405,但因細格中有 4 單位期望次數小於 5,故採用 Fisher 精確檢定卡方值 17.097。

7.經常上網原因

由下表 4-2-26 得知，在男性網路使用者中，被害組與未被害組在經常上網原因之差異性，達統計上之顯著水準(χ^2=29.516 ; d.f.=7 ; p<.001)。被害組經常上網原因多為休閒娛樂(19.2%)，而未被害組則為搜尋資料(21.5%)，顯見兩者在上網原因具有顯著差異。

在女性網路使用者中，被害組與未被害組在經常上網原因之差異性，均達統計上之顯著水準(χ^2=23.186 ; d.f.=7 ; p<.001)。被害組經常上網原因大多為抒發情緒(20.2%)，而未被害組則為搜尋資料(23.1%)，顯見兩者在上網原因具有顯著差異。

在比較不同性別網路使用者是否被害之上網原因後，可以得知，未被害者上網原因為搜尋資料，而被害者上網原因則為休閒娛樂或抒發情緒，足見被害者多以網路從事休閒娛樂。此外，在不同性別被害者上網原因中，男性與女性被害上網原因亦有所差異。

表 4-2-26 性別、網路詐欺被害與經常上網原因之差異性分析

性別	網路使用特性		是否被害			卡方值;自由度（顯著水準）
	變項名稱	組別	是	否	總和	
男	經常上網原因[42]	抒發情緒	75(18.7)	154(11.4)	229(13.1)	**χ^2=29.516*** ** d.f.=7
		搜尋資料	63(15.7)	289(21.5)	352(20.1)	
		買賣東西	41(10.2)	144(10.7)	185(10.6)	
		交友聊天	63(15.7)	183(13.6)	246(14.1)	
		休閒娛樂	77(19.2)	199(14.8)	276(15.8)	
		找尋新奇事物	25(6.2)	137(10.2)	162(9.3)	
		收發信件	38(9.5)	160(11.9)	198(11.3)	
		滿足網愛	20(5.0)	79(5.9)	99(5.7)	
		總和	402(100.0)	1345(100.0)	1747(100.0)	
女	經常上網原因	抒發情緒	37(20.2)	143(10.7)	180(11.8)	**χ^2=23.186*** ** d.f.=7
		搜尋資料	32(17.5)	310(23.1)	342(22.5)	
		買賣東西	20(10.9)	195(14.6)	215(14.1)	
		交友聊天	30(16.4)	207(15.4)	237(15.6)	
		休閒娛樂	32(17.5)	191(14.3)	223(14.6)	
		找尋新奇事物	11(6.0)	123(9.2)	134(8.8)	
		收發信件	16(8.7)	155(11.6)	171(11.2)	
		滿足網愛	5(2.7)	16(1.2)	21(1.4)	
		總和	183(100.0)	1340(100.0)	1523(100.0)	

註:***p<.001

[42] 本題為複選題，故表格中呈現之次數係為各回答題項之統計次數。

二、獨立樣本 t 檢定[43]

本部分就性別、網路詐欺被害在研究各連續變項（網路生活型態、被害情境與機會及低自我控制特性)之差異情形進行分析，經以獨立樣本 t 檢定法進行平均數差異分析後，茲將分析結果呈現如下表 4-2-27。

(一)性別在網路生活型態、被害情境與機會及低自我控制特性之差異分析

有關不同性別在網路生活型態、被害情境與機會及低自我控制之差異分析之結果如下表 4-2-27。首先，在網路生活型態構面中，不同性別之網路休閒活動差異，達統計上之顯著差異(t=-3.480 ； p<.01)，且女性從事網路休閒活動程度(平均數為 3.62)顯著高於男性(平均數為 3.53);在網路職業活動部分，不同性別之網路職業活動差異，達統計上之顯著差異(t=-3.750 ； p<.01)，且女性從事網路職業活動程度(平均數為 3.48)顯著高於男性(平均數為 3.35);在網路風險休閒活動部分，不同性別之網路風險休閒活動差異，達統計上之顯著差異(t=6.428 ； p<.001)，但男性從事網路風險休閒活動程度(平均數為 2.16)顯著高於女性(平均數為 1.87);在網路風險職業活動部分，經自然對數轉換後，不同性別之網路風險職業活動差異，達統計上之顯著差異(t=2.497 ; p<.05)，男性從事網路風險職業活動程度(平均數為.31)顯著高於女性(平均數為.25)，由此可知，女性在從事網路休閒或職業活動上之程度雖然顯著高於男性,但男性在從事具風險性之網路休閒或職業活動程度卻顯著高於女性，顯見兩性在網路生活型態上有所差異。

其次，在被害情境與機會構面中，在社會監控部分，不同性別之社會監控差異，達統計上之顯著水準(t=-2.782 ； p<.01)，其中，女性之社會監控程度(平均數為 2.05)顯著高於男性(平均數為 1.93);在物理監控部分，雖然不同性別之物理監控差異未達統計上之顯著差異(t=-.719 ； p>.05)，但女性之物理監控程度(平均數為 2.71)略高於男性(平均數為 2.68)。在網路負面誘因部分，不同性別之網路負面誘因程度差異，達統計上之顯

[43] Mertler 和 Vannatta(2016)、Kennedy 和 Bush(1985)指出，在多數統計工具及多變量分析之基本假設中，資料皆須符合常態分布假設，若未符合基本假設，則統計值及檢驗將產生偏誤，而 Kline(2015)提出量表的得分可經由自然對數、對數、平方根等方式使量表整體分配趨近常態分配。此外，Aron 和 Coups (2006)、Johnson 和 Wichern(2008)均指出，數據轉換僅係將數據以不同單位進行資料的表達，因此不僅不會改變原始資料的特性、對於資料之原始順序及其相對位置亦未受到影響，故受到多數學者肯認並廣泛採用。因此，本研究前節對於各構面之平均得分進行偏態檢定，若呈現偏態分佈，則採用上述方式進行轉換。

著水準(t=5.177 ; p<.001)，其中，男性在網路使用中所接受到的負面誘因訊息(平均數為2.05)顯著高於女性(平均數為 1.80);在網路偏差動機部分，經平方根轉換後，不同性別之網路偏差動機程度差異，達統計上之顯著水準(t=5.906 ; p<.001)，其中，男性在網路使用中的個人偏差動機(平均數為 1.48)顯著高於女性(平均數為 1.28)。由上述數據可知，在監控部分，無論是社會或是物理監控上，女性皆高於男性，而在網路負面誘因及網路偏差動機上，男性則顯著高於女性，顯見男性具有較高的網路負面誘因及偏差動機。

最後，在低自我控制之三個特性中，在衝動性部分，不同性別之衝動性差異，未達統計上之顯著水準(t=1.158 ; p>.05)，但男性之衝動性程度(平均數為 2.04)略高於女性(平均數為 1.99);在冒險性部分,不同性別之冒險性差異,達統計上之顯著水準(t=3.488 ; p<.01)，其中，男性的冒險性程度(平均數為 2.28)顯著高於女性(平均數為 2.13);在投機性部分，不同性別之投機性差異未達統計上之顯著水準(t=-1.011 ; p>.05)，但女性之投機性程度(平均數為 2.45)卻略高於男性(平均數為 2.41)。由上述數據可知，在低自我控制特性之冒險性部分，男性顯著高於女性。

表 4-2-27 性別在各因素面向上之差異分析表

構面名稱	變項	男性(N=455)	女性(N=415)	t 值
		平均數(標準差)	平均數(標準差)	(顯著性)
網路生活型態	網路休閒活動	3.5301(.45998)	3.6275(.36318)	**t=-3.480****
	網路職業活動	3.3574(.55534)	3.4892(.48099)	**t=-3.750****
	網路風險休閒活動	2.1613(.73341)	1.8776(.56385)	**t=6.428*****
	網路風險職業活動(Ln)[44]	.3107(.34944)	.2552(.30594)	**t=2.497***
被害情境與機會	社會監控	1.9376(.61434)	2.0559(.63956)	**t=-2.782****
	物理監控	2.6835(.69375)	2.7157(.62564)	t=-.719
	網路負面誘因	2.0593(.77317)	1.8066(.66607)	**t=5.177*****
	網路偏差動機(Sqrt)[45]	1.4878(.59109)	1.2824(.42850)	**t=5.906*****
低自我控制特性	衝動性	2.0478(.75988)	1.9922(.65647)	t=1.158
	冒險性	2.2835(.62932)	2.1386(.59290)	**t=3.488****
	投機性	2.4159(.58283)	2.4560(.58542)	t=-1.011

註:*p<.05 ; **p<.01 ; ***p<.001

[44] Ln 代表變項經自然對數轉換(Natural logarithm transformation)
[45] Sqrt 代表變項經平方根轉換(Square root transformation)

(二)網路詐欺被害在網路生活型態、被害情境與機會及低自我控制特性之差異分析

是否曾有網路詐欺被害經驗之網路使用者，在網路生活型態(網路休閒活動、網路職業活動、網路風險休閒活動、網路風險職業活動)、被害情境與機會(社會監控、物理監控、網路負面誘因、網路偏差動機)及低自我控制(衝動性、冒險性、投機性)之差異，經獨立樣本 t 檢定分析後，茲將分析結果呈現如下表 4-2-28。

首先,在網路生活型態構面中,是否有網路詐欺被害經驗者在網路休閒活動之差異，達統計上之顯著水準(t=3.135 ; p<.01),其中，未被害者從事網路休閒活動(平均數為 3.60)顯著高於被害者(平均數為 3.45)。在網路職業活動部分，是否有網路詐欺被害經驗者之網路職業活動差異未達統計上之顯著差異(t=4.482 ; p<.001)，其中，未被害者從事網路職業活動程度(平均數 3.46)顯著較被害者高(平均數為 3.21)。在網路風險休閒活動部分，是否有網路詐欺被害經驗者，未達統計上之顯著差異(t=-1.268 ; p>.05)。在網路風險職業活動部分，經自然對數轉換後，是否有網路詐欺被害經驗者之網路風險職業活動達統計上之顯著差異(t=-5.270 ; p<.001)，被害者從事網路風險職業活動程度(平均數為.43)顯著較未被害者高(平均數為.25)。由此可知，未被害者之網路休閒與職業活動顯著高於被害者，但被害者之網路風險職業活動卻顯著高於未被害者。

其次，在被害情境與機會構面中，在社會監控部分，是否曾有網路詐欺被害經驗者在社會監控程度上之差異，達統計上之顯著水準(t=3.487 ; p<.01)，其中，未被害者之社會監控程度(平均數為 2.02)顯著高於被害者(平均數為 1.82);在物理監控部分，是否曾有網路詐欺被害經驗者之物理監控程度差異，達統計上之顯著水準(t=4.690 ; p<.001)，其中，未被害者之物理監控程度(平均數為 2.74)顯著高於被害者(平均數為 2.46)。在網路負面誘因部分，是否曾有網路詐欺被害經驗者之網路負面誘因程度差異，達統計上之顯著水準(t=-2.168 ; p<.05)，其中，被害者在網路使用中所接受到的負面誘因訊息(平均數為 2.08)顯著高於未被害者(平均數為 1.91);在網路偏差動機部分,經平方根轉換後，是否曾有網路詐欺被害經驗者之網路偏差動機程度之差異，達統計上之顯著水準(t=-3.592 ; p<.001)，其中，被害者在網路使用中的個人偏差動機(平均數為 1.57)顯著高於未被害者(平均數為 1.35)。由上述數據可知，在監控部分，未被害者之社會或物理監

控程度均顯著高於被害者，而在網路負面誘因及網路偏差動機部分，被害者則顯著高於未被害者，顯見被害者缺乏物理及社會監控，但卻有較高的網路負面誘因及偏差動機。

最後，在低自我控制之三個特性中，在衝動性部分，是否曾有網路詐欺被害經驗者在衝動性之差異，達統計上之顯著水準(t=-3.828 ; p<.001)，其中，被害者之衝動性程度(平均數為 2.27)顯著高於未被害者(平均數為 1.97);在冒險性部分，是否曾有網路詐欺被害經驗者之冒險性差異，達統計上之顯著水準(t=-5.889 ; p<.001)，其中，被害者的冒險性程度(平均數為 2.48)顯著高於未被害者(平均數為 2.16);在投機性部分，是否曾有網路詐欺被害經驗者之投機性差異，達統計上之顯著水準(t=-5.243 ; p<.001)，其中，被害者之投機性程度(平均數為 2.71)顯著高於未被害者(平均數為 2.38)。由上述數據可知，在低自我控制特性部分，被害者在各項低自我控制之特性中均顯著高於未被害者，顯示被害者具有較低的自我控制程度。

表 4-2-28 網路詐欺被害在各因素面向之差異分析表

構面名稱	變項	未被害(N=728)	被害(N=142)	t 值
		平均數(標準差)	平均數(標準差)	(顯著性)
網路生活型態	網路休閒活動	3.6000(.39334)	3.4563(.51770)	**t=3.135****
	網路職業活動	3.4604(.49568)	3.2141(.61731)	**t=4.482*****
	網路風險休閒活動	2.0121(.65742)	2.0972(.74481)	t=-1.268
	網路風險職業活動(Ln)[46]	.2544(.30884)	.4374(.39077)	**t=-5.270*****
被害情境與機會	社會監控	2.0266(.63368)	1.8268(.57771)	**t=3.487****
	物理監控	2.7448(.65011)	2.4634(.67430)	**t=4.690*****
	網路負面誘因	1.9111(.69970)	2.0810(.88152)	**t=-2.168***
	網路偏差動機(Sqrt)[47]	1.3536(.48073)	1.5754(.70432)	**t=-3.592*****
低自我控制特性	衝動性	1.9715(.65835)	2.2764(.90345)	**t=-3.828*****
	冒險性	2.1611(.61411)	2.4877(.55250)	**t=-5.889*****
	投機性	2.3802(.53551)	2.7165(.72703)	**t=-5.243*****

註:*p<.05 ; **p<.01 ; ***p<.001

[46] Ln 代表變項經自然對數轉換(Natural logarithm transformation)

[47] Sqrt 代表變項經平方根轉換(Square root transformation)

(三)性別、網路詐欺被害在各因素面向之差異分析

為更深入探究不同性別、網路詐欺被害與否在各因素面向上之差異，故在分析中係以獨立樣本 t 檢定法，對於性別及網路詐欺被害在中各因素面向之差異性進行更進一步之交叉分析，詳細分析內容敘述如下表 4-2-29 所示:

1.性別、網路詐欺被害在網路生活型態之差異分析

首先，網路休閒活動部分，在男性網路使用者中，是否曾有網路被害經驗在網路休閒活動上之差異，達統計上之顯著水準(t=2.358 ; p<.05)，其中，未被害者之網路休閒活動(平均數為 3.56)顯著高於被害者(平均數為 3.41)。在女性網路使用者中，未被害者之網路休閒活動(平均數為 3.63)略高於未被害者(平均數為 3.53)，但兩者差異則未達統計上之顯著水準(t=1.581 ; p>.05)。

其次，網路職業活動部分，在男性網路使用者中，是否曾有網路被害經驗在網路職業活動上之差異，達統計上之顯著水準(t=3.623 ; p<.001)，其中，未被害者之網路職業活動(平均數為 3.40)顯著高於被害者(平均數為 3.15)。在女性網路使用者中，是否曾有網路被害被害經驗在網路職業活動上之差異，亦達統計上之顯著水準(t=2.043 ; p<.05)，其中，未被害者之網路職業活動(平均數為 3.51)顯著高於被害者(平均數為 3.32)。

再者，網路風險休閒活動部分，在男性網路使用者中，被害者之網路風險休閒活動(平均數為 2.19)略高於未被害者(平均數為 2.15)，但兩者之差異未達統計上之顯著水準(t=-.497 ; p>.05)。在女性網路使用者中，被害者之網路風險休閒活動(平均數為 1.90)略高於未被害者(平均數為 1.87)，但兩者之差異未達統計上之顯著水準(t=-.292 ; p>.05)。

最後，網路風險職業活動部分，經自然對數轉換後，在男性網路使用者中，是否曾有網路被害經驗在網路風險職業活動上之差異，達統計上之顯著水準(t=-3.582 ; p<.001)，其中，被害者之網路風險職業活動(平均數為.43)顯著高於未被害者(平均數為.27)，而在女性網路使用者中，是否曾有網路被害被害經驗在網路風險職業活動上之差異，亦達統計上之顯著水準(t=-3.705 ; p<.001)，其中，被害者之網路風險職業活動(平均數為.43)顯著高於未被害者(平均數為.23)。

2.性別、網路詐欺被害在被害情境與機會之差異分析

首先，社會監控部分，在男性網路使用者中，是否曾有網路被害經驗在社會監控程度之差異，達統計上之顯著水準(t=2.875 ; p<.01)，其中，未被害者之社會監控程度(平均數為 1.97)顯著高於被害者(平均數為 1.77)。在女性網路使用者中，是否曾有網路被害經驗在社會監控程度之差異，則未達統計上之顯著水準(t=1.510 ; p>.05)，其中，未被害者之社會監控程度(平均數為 2.07)略高於被害者(平均數為 1.92)。

其次，物理監控部分，在男性網路使用者中，是否曾有網路被害經驗在物理監控程度之差異，達統計上之顯著水準(t=3.593 ; p<.001)，其中，未被害者之物理監控程度(平均數為 2.74)顯著高於被害者(平均數為 2.45)。在女性網路使用者中，是否曾有網路被害經驗在物理監控程度之差異，亦達統計上之顯著水準(t=2.858 ; p<.01)，其中，未被害者之物理監控程度(平均數為 2.74)顯著高於被害者(平均數為 2.47)。

再者，網路負面誘因部分，在男性網路使用者中，被害者之網路負面誘因程度(平均數為 2.18)略高於未被害者(平均數為 2.02)，但兩者之差異未達統計上之顯著水準(t=-1.615 ; p>.05)。在女性網路使用者中，被害者之網路負面誘因程度(平均數為 1.86)略高於未被害者(平均數為 1.79)，但兩者之差異亦未達統計上之顯著水準(t=-.594 ; p>.05)。

最後，網路偏差動機部分，在男性網路使用者中，是否曾有網路被害經驗在網路偏差動機程度之差異，達統計上之顯著水準(t=-3.582 ; p<.001)，其中，被害者之網路偏差動機程度(平均數為 1.66)顯著高於未被害者(平均數為 1.44)。在女性網路使用者中，是否曾有網路詐欺被害經驗在網路偏差動機程度之差異，達統計上之顯著水準(t=-1.590 ; p<.05)，其中，被害者之網路偏差動機程度(平均數為 1.39)顯著高於未被害者(平均數為 1.26)。

表 4-2-29 性別、網路詐欺被害在網路生活型態、被害情境機會之差異分析表

變項名稱	性別	組別	平均數(標準差)	t 值(顯著性)
網路休閒活動	男性 (N=455)	未被害組(N=361)	3.5601(.42735)	**t=2.358***
		被害組(N=94)	3.4149(.55590)	
	女性 (N=415)	未被害組(N=367)	3.6392(.35295)	t=1.581
		被害組(N=48)	3.5375(.42708)	
網路職業活動	男性 (N=455)	未被害組(N=361)	3.4089(.52908)	**t=3.623****
		被害組(N=94)	3.1596(.61001)	
	女性 (N=415)	未被害組(N=367)	3.5112(.45552)	**t=2.043***
		被害組(N=48)	3.3208(.62397)	
網路風險休閒活動	男性 (N=455)	未被害組(N=361)	2.1518(.70915)	t=-.497
		被害組(N=94)	2.1979(.82305)	
	女性 (N=415)	未被害組(N=367)	1.8747(.57067)	t=-.292
		被害組(N=48)	1.9000(.51364)	
網路風險職業活動(Ln)[48]	男性 (N=455)	未被害組(N=361)	.2772(.32529)	**t=-3.582****
		被害組(N=94)	.4395(.40669)	
	女性 (N=415)	未被害組(N=367)	.2319(.29046)	**t=-3.705****
		被害組(N=48)	.4333(.36169)	
社會監控	男性 (N=455)	未被害組(N=361)	1.9795(.61889)	**t=2.875****
		被害組(N=94)	1.7766(.57163)	
	女性 (N=415)	未被害組(N=367)	2.0730(.64538)	t=1.510
		被害組(N=48)	1.9250(.58291)	
物理監控	男性 (N=455)	未被害組(N=361)	2.7424(.67660)	**t=3.593****
		被害組(N=94)	2.4574(.71580)	
	女性 (N=415)	未被害組(N=367)	2.7471(.62387)	**t=2.858****
		被害組(N=48)	2.4750(.59161)	
網路負面誘因	男性 (N=455)	未被害組(N=361)	2.0256(.73234)	t=-1.615
		被害組(N=94)	2.1888(.90599)	
	女性 (N=415)	未被害組(N=367)	1.7984(.64751)	t=-.594
		被害組(N=48)	1.8698(.79892)	
網路偏差動機(Sqrt)[49]	男性 (N=455)	未被害組(N=361)	1.4407(.52714)	**t=-3.582****
		被害組(N=94)	1.6687(.76699)	
	女性 (N=415)	未被害組(N=367)	1.2679(.41338)	**t=-1.590***
		被害組(N=48)	1.3926(.52214)	

註:*p<.05 ; **p<.01 ; ***p<.001

[48] Ln 代表變項經自然對數轉換(Natural logarithm transformation)

[49] Sqrt 代表變項經平方根轉換(Square root transformation)

3.性別、網路詐欺被害在低自我控制特性之差異分析

有關性別、網路詐欺被害在低自我控制特性之差異分析如下表 4-2-30 所示。首先，衝動性部分，男性網路使用者中，網路詐欺被害與否在衝動性之差異，達統計上之顯著水準(t=-4.212 ; p<.001)，其中，被害者之衝動性(平均數為 2.39)顯著高於未被害者(平均數為 1.95)，但女性網路使用者之衝動性則未達統計上之顯著水準(t=-.672 ; p>.05)。

其次,冒險性部分,在男性網路使用者中,網路詐欺被害與否在冒險性程度之差異，達統計上之顯著水準(t=-4.924 ; p<.001)，其中，被害者之冒險性程度(平均數為 2.56)顯著高於未被害者(平均數為 2.21)。在女性網路使用者中，網路詐欺被害與否在冒險性程度之差異，亦達統計上之顯著水準(t=-2.567 ; p<.01)，其中，被害者之冒險性程度(平均數為 2.34)顯著高於未被害者(平均數為 2.11)。

最後，投機性部分，在男性網路使用者中，網路詐欺被害與否在投機性程度上之差異,達統計上之顯著水準(t=-3.649 ; p<.001),其中,被害者之投機性程度(平均數為 2.64)顯著高於未被害者(平均數為 2.35)。在女性網路使用者中，是否曾有網路詐欺被害經驗在投機性程度之差異，亦達統計上之顯著水準(t=-4.091 ; p<.001)，其中，被害者之投機性程度(平均數為 2.86)顯著高於未被害者(平均數為 2.40)。

表 4-2-30 性別、網路詐欺被害在低自我控制特性之差異分析表

變項名稱	性別	組別	平均數(標準差)	t 值;(顯著性)
衝動性	男性(N=455)	未被害組(N=361)	1.9584(.68161)	**t=-4.212*** **
		被害組(N=94)	2.3910(.93294)	
	女性(N=415)	未被害組(N=367)	1.9843(.63531)	t=-.672
		被害組(N=48)	2.0502(.80550)	
冒險性	男性(N=455)	未被害組(N=361)	2.2112(.63510)	**t=-4.924*** **
		被害組(N=94)	2.5612(.52323)	
	女性(N=415)	未被害組(N=367)	2.1117(.58946)	**t=-2.567** **
		被害組(N=48)	2.3438(.58488)	
投機性	男性(N=455)	未被害組(N=361)	2.3573(.53302)	**t=-3.649*** **
		被害組(N=94)	2.6410(.70287)	
	女性(N=415)	未被害組(N=367)	2.4026(.53773)	**t=-4.091*** **
		被害組(N=48)	2.8646(.75786)	

註:**p<.01 ; ***p<.001

第三節 性別、網路詐欺被害與各變項之相關分析

一、個人特性與各因素構面間之相關性

(一)個人基本特性與網路詐欺被害之相關性

在個人基本特性與網路詐欺被害之皮爾森積差相關結果，如表 4-3-1 所示。在個人基本特性部分，經皮爾森積差相關分析後可發現，網路詐欺被害與收入(r=.247 ; p<.001)呈現顯著正相關，但卻與性別(r=-.123 ; p<.001)、年齡(r=-.135 ; p<.001)及職業(r=-.190 ; p<.001)及教育程度(r=-.199 ; p<.001)呈現顯著負相關，顯示男性、年齡越低者、未就業者、收入較高及教育程度較低者，網路詐欺被害之機會較高。

(二)個人基本特性與網路生活型態之相關性

有關個人基本特性與網路生活型態之皮爾森積差相關結果，如表 4-3-1 所示。首先，在網路休閒活動構面中，經皮爾森積差相關分析後可發現，網路休閒活動與性別(r=.116 ; p<.01)、年齡(r=.068 ; p<.01)、職業(r=.100 ; p<.01)及教育程度(r=.211 ; p<.001)呈現顯著正相關，顯示女性、年齡較長、就業者及教育程度較高者從事網路休閒活動之程度較高。

其次，在網路職業活動構面中，經皮爾森積差相關分析後可發現，網路職業活動與性別(r=.125 ; p<.001)、職業(r=.083 ; p<.05)及教育程度(r=.361 ; p<.01)呈現顯著正相關，顯示女性、就業者及教育程度較高者，其從事網路職業活動之程度較高。

再者，在網路風險休閒活動構面中，經皮爾森積差相關分析後可發現，網路風險休閒活動與性別(r=-.211 ; p<.001)、教育程度(r=-.091 ; p<.01)及婚姻狀況(r=-.118 ; p<.001)呈現顯著負相關，顯示男性、教育程度較低者及未婚者從事風險休閒活動之程度較高。

最後，在網路風險職業活動構面中，經皮爾森積差相關分析後可發現，網路風險職業活動僅與性別(r=-.092 ; p<.05)呈現顯著負相關，顯示男性從事網路風險休閒活動之程度較高。

(三)個人基本特性與被害情境與機會之相關性

有關個人基本特性與被害情境與機會之皮爾森積差相關結果，如下表 4-3-1 所示。首先，在社會監控構面中，經皮爾森積差相關分析後可發現，社會監控與性別(r=.094 ;

p<.01)、收入(r=.130 ; p<.001)及婚姻狀況(r=.096 ; p<.01)呈現顯著正相關，顯示女性、高收入者、已婚者，其社會監控程度較高。

其次，在物理監控構面中，經皮爾森積差相關分析後可發現，物理監控與職業(r=.176 ; p<.001)、收入(r=.123 ; p<.001)及教育程度(r=.170 ; p<.01)呈現顯著正相關，顯示就業者、收入較高者及教育程度較高者，其物理監控程度較高。

再者，在網路負面誘因構面中，經皮爾森積差相關分析後可發現，網路負面誘因與性別(r=-.172 ; p<.001)及年齡(r=-.106 ; p<.01)呈現顯著負相關，顯示男性及年齡較低者其網路負面誘因誘因程度較高。

最後，在網路偏差動機構面中，經皮爾森積差相關分析後可發現，網路偏差動機與性別(r=-.185 ; p<.001)、年齡(r=-.077 ; p<.05)及教育程度(r=-.110 ; p<.01)呈現顯著負相關，顯示男性、年齡較低及教育程度較低者，在網路使用過程中有較高的偏差動機。

(四)個人基本特性與低自我控制特性之相關性

有關個人基本特性與低自我控制特性之皮爾森積差相關結果，如下表 4-3-1 所示。首先，在衝動性構面中，經皮爾森積差相關分析後可發現，衝動性與年齡(r=-.068 ; p<.05)、職業(r=.102 ; p<.01)、收入(r=-.082 ; p<.05)、教育程度(r=-.076 ; p<.05)及婚姻狀況(r=-.093 ; p<.01)呈現顯著負相關，顯示年齡較低、未就業者、收入較低、教育程度較低及未婚者其衝動性程度較高。

其次，在冒險性構面中，經皮爾森積差相關分析後可發現，冒險性與性別(r=-.118 ; p<.01)、職業(r=-.070 ; p<.05)、教育程度(r=-.078 ; p<.05)及婚姻狀況(r=-.073 ; p<.05)呈現顯著負相關，顯示男性、未就業者、教育程度較低者及未婚者其冒險性程度較高。

最後，在投機性構面中，經皮爾森積差相關分析後可發現，投機性與職業(r=-.119 ; p<.001)及教育程度(r=-.076 ; p<.05) 呈現顯著負相關，顯示未就業者及教育程度較低者其投機性程度較高。

二、網路使用特性與各因素構面間之相關性

有關網路使用特性與各因素構面之皮爾森積差相關結果，如表 4-3-1 所示。首先，在每次上網時數方面，經皮爾森積差相關分析後可發現，每次上網時數與網路詐欺被害與否(r=.244 ; p<.001)、網路休閒活動(r=.126 ; p<.001)及網路職業活動(r=.073 ; p<.05)、網路風險休閒活動(r=.125 ; p<.001)及衝動性(r=.094 ; p<.01)呈現顯著正相關，顯示每次上網時數較長者，其網路詐欺被害機會較高、從事網路休閒活動、網路職業活動、網路風險休閒活動之程度較高，個人之衝動性程度亦較高。

其次，在每周上網次數方面，經皮爾森積差相關分析後可發現，每周上網次數與網路詐欺被害與否(r=.192 ; p<.001)、網路休閒活動(r=.285 ; p<.001)及網路職業活動(r=.181 ; p<.001)呈現顯著正相關，但卻與網路風險職業活動(r=-.112 ; p<.001)、網路負面誘因(r=-.097 ; p<.01)、網路偏差動機(r=-.129 ; p<.001)、衝動性(r=-.075 ; p<.05)、冒險性(r=-.098 ; p<.01)呈現顯著負相關，顯示網路使用者每周上網次數較頻繁者，其遭受網路詐欺被害之機會較高，且其從事網路休閒活動及網路職業活動之機會較高，但其從事網路風險職業活動程度較低，而個人的網路負面誘因、網路偏差動機、衝動性及冒險性程度亦較低。

最後，在接觸網路時間方面，經皮爾森積差相關分析後可發現，接觸網路時間與網路休閒活動(r=.263 ; p<.001)、網路職業活動(r=.262 ; p<.001)及物理監控(r=.145 ; p<.001)呈現顯著正相關，但卻與網路風險職業活動(r=-.089 ; p<.05)及網路偏差動機(r=-.078 ; p<.05)呈現顯著負相關，顯示接觸網路時間較長者，其從事網路休閒活動及網路職業活動之程度較高且其物理監控程度亦較高，但其從事網路風險職業活動程度較低，且個人在網路使用時的網路偏差動機程度較低。

三、網路詐欺被害與各因素構面間之相關性

有關網路詐欺被害與各因素構面之皮爾森積差相關結果，如表 4-3-1 所示。首先，在網路生活型態方面，經皮爾森積差相關分析後可發現，網路詐欺被害與網路休閒活動(r=-.127 ; p<.001)、網路職業活動(r=-.174 ; p<.001)呈顯著負相關，但卻與網路風險職業活動(r=.211 ; p<.01)呈顯著正相關，顯示在網路生活型態變項中，當網路使用者從事越少網路休閒活動、網路職業活動，從事較高網路風險職業活動者，其遭受網路詐欺被害的機會較高。

其次，在被害情境與機會方面，經皮爾森積差相關分析後可發現，網路詐欺被害與社會監控(r=-.118 ; p<.001)、物理監控(r=-.157 ; p<.001)呈顯著負相關，但卻與網路負面誘因(r=.086 ; p<.05)及網路偏差動機(r=.183 ; p<.01)呈顯著正相關，顯示在被害情境與機會中，當網路使用者具有較低物理監控、社會監控、接受較多網路負面誘因及具有較高網路偏差動機時，其網路詐欺被害機會較高。

最後，在低自我控制特性方面，經皮爾森積差相關分析後可發現，網路詐欺被害與衝動性(r=.158 ; p<.001)、冒險性(r=.196 ; p<.001)及投機性(r=.213 ; p<.001)皆呈顯著正相關，顯示在低自我控制特性方面，當網路使用者具有較高的衝動性、冒險性及投機性者，其網路詐欺被害機會較高。

綜合上述皮爾森積差相關分析之結果後可以發現，當網路使用者從事較少網路休閒活動、網路職業活動、缺乏社會監控及物理監控，從事較多網路風險職業活動、接收較多網路負面誘因及較高網路偏差動機、衝動性、冒險性及投機性者，其遭受網路詐欺被害之可能性也較高。

四、網路詐欺被害次數與各因素構面間之相關性

(一)個人基本特性與網路詐欺被害次數之相關性

有關個人基本特性與網路詐欺被害次數之皮爾森積差相關結果，如表 4-3-1 所示。網路詐欺被害次數與性別(r=-.361 ; p<.001)、年齡(r=-.331 ; p<.001)、職業(r=-.211 ; p<.001)及教育程度(r=-.371 ; p<.001)呈顯著負相關，顯示男性、年齡較低者、無職業者及教育程度較低者，其網路詐欺被害次數較高。

(二)網路使用特性與網路詐欺被害次數之相關性

有關網路使用特性與網路詐欺被害次數之皮爾森積差相關結果，如表 4-3-1 所示。網路詐欺被害次數僅與網路接觸時間(r=.197 ; p<.05)呈顯著正相關，顯示網路接觸時間較高者，其網路詐欺被害次數較高。

(三)網路詐欺被害次數與各因素構面之相關性

有關網路詐欺被害次數與各因素構面之皮爾森積差相關結果，如表 4-3-1 所示。首先，在網路生活型態方面，網路詐欺被害次數與網路休閒活動(r=-.460 ; p<.001)、網路職業活動(r=-.362 ; p<.001)呈顯著負相關，但卻與網路風險休閒活動(r=.557 ; p<.001)、網路風險職業活動(r=.392 ; p<.001)呈顯著正相關，顯示從事越少網路休閒活動、網路職業活動，從事較高網路風險休閒與職業活動者，其網路詐欺被害次數較高。

其次，在被害情境與機會方面，經皮爾森積差相關分析後可發現，網路詐欺被害次數與社會監控(r=-.406 ; p<.001)、物理監控(r=-.545 ; p<.001)呈顯著負相關，但卻與網路負面誘因(r=.607 ; p<.001)及網路偏差動機(r=.589 ; p<.001)呈顯著正相關，顯示當網路使用者具有較低物理監控及社會監控程度，並接受較多網路負面誘因及較高網路偏差動機時，其網路詐欺被害次數較高。

最後，在低自我控制特性方面，經皮爾森積差相關分析後可發現，網路詐欺被害與冒險性(r=.292 ; p<.001)及投機性(r=.214 ; p<.05)呈顯著正相關，顯示在低自我控制特性方面，當網路使用者具有較高的冒險性及投機性者，其網路詐欺被害次數較高。

表 4-3-1 個人基本特性、網路生活型態及網路詐欺被害在各因素之相關分析表

		是否被害	被害次數	網路休閒活動	網路職業活動	網路風險休閒活動	網路風險職業活動 (Ln)[50]	社會監控	物理監控	網路負面誘因	網路偏差動機 (Sqrt)[51]	衝動性	冒險性	投機性
個人基本特性	性別[52]	**-.123*****	**-.361*****	**.116****	**.125*****	**-.211*****	**-.092***	**.094****	.024	**-.172*****	**-.185*****	-.039	**-.118****	-.034
	年齡	**-.135*****	**-.331*****	**.068****	.028	-.046	-.024	.011	.019	**-.106****	**-.077***	**-.068***	-.040	-.039
	職業[53]	**-.190*****	**-.211*****	**.100****	**.083***	-.032	-.038	.013	**.176*****	-.045	-.056	**-.102****	**-.070***	**-.119*****
	收入	**.247*****	.152	.027	.048	-.019	.023	**.130*****	**.123*****	.044	-.020	**-.082***	.013	-.058
	教育程度	**-.199*****	**-.371*****	**.211*****	**.361****	**-.091****	-.054	.010	**.170****	-.034	**-.110****	**-.076***	**-.078***	**-.076***
	婚姻狀況[54]	-.047	-.058	-.031	-.031	**-.118*****	-.057	**.096****	.009	-.046	-.056	**-.093****	**-.073***	-.041
網路使用特性	每次上網時數	**.244*****	-.134	**.126*****	**.073***	**.125*****	-.004	-.007	-.010	.043	.031	**.094****	.047	.037
	每周上網次數	**.192*****	-.064	**.285*****	**.181*****	-.026	**-.112*****	-.019	.062	**-.097****	**-.129*****	**-.075***	**-.098****	-.007
	接觸網路時間	.070	**.197***	**.263*****	**.262*****	.048	**-.089***	-.044	**.145*****	.014	**-.078***	-.027	-.037	-.005
網路詐欺被害與否[55]		–	–	**-.127*****	**-.174*****	.047	**.211****	**-.118*****	**-.157*****	**.086***	**.183****	**.158*****	**.196*****	**.213*****
網路詐欺被害次數		–	–	**-.460*****	**-.362*****	**.557*****	**.392*****	**-.406*****	**-.545*****	**.607*****	**.589*****	-.089	**.292*****	**.214***

註:*p<.05 ; **p<.01 ; ***p<.001

[50] Ln 代表變項經自然對數轉換(Natural logarithm transformation)
[51] Sqrt 代表變項經平方根轉換(Square root transformation)
[52] 性別(0=男、1=女)
[53] 職業(0=無業/未就業組、1=就業組)
[54] 婚姻狀況(0=未婚組、1=已婚組)
[55] 網路詐欺被害與否(0=否、1=是)

五、網路詐欺各因素構面間之相關性

(一)網路生活型態與各因素構面之相關性

有關網路生活型態與各態度量表之皮爾森積差相關結果，如表 4-3-2 所示。首先，在網路休閒活動構面中，網路休閒活動與網路職業活動(r=.443 ; p<.001)、社會監控(r=.115 ; p<.01)、物理監控(r=.285 ; p<.001)均呈現顯著正相關，因此，當網路使用者所從事之網路休閒活動程度越高，其網路職業活動、社會監控及物理監控之程度也越高。此外，網路休閒活動與網路風險職業活動(r=-.122 ; p<.001)、網路負面誘因(r=-.108 ; p<.01)、網路偏差動機(r=-.286 ; p<.01)、冒險性(r=-.096 ; p<.01)及投機性(r=-.117 ; p<.01)呈現顯著負相關，亦即網路使用者從事之網路休閒活動程度越高，則個人的網路風險職業活動、網路負面誘因、網路偏差動機、冒險性及投機性程度越低。

其次，在網路職業活動構面中，經皮爾森積差相關分析後可發現，網路職業活動與社會監控(r=.129 ; p<.001)及物理監控(r=.119 ; p<.001) 均呈現顯著正相關，因此，當網路使用者所從事之網路職業活動程度越高，其社會監控及物理監控之程度也越高。此外，網路職業活動與網路風險職業活動(r=-.129 ; p<.001)、網路偏差動機(r=-.219 ; p<.001)、衝動性(r=-.093 ; p<.01)、冒險性(r=-.088 ; p<.01)及投機性(r=-.160 ; p<.001)呈顯著負相關，亦即網路使用者從事之網路職業活動程度越高，則個人之網路風險職業活動、網路偏差動機、衝動性、冒險性及投機性程度越低。

再者，在網路風險休閒活動構面中，經皮爾森積差相關分析後可發現，網路風險休閒活動與網路風險職業活動(r=.362 ; p<.001)、網路負面誘因(r=.378 ; p<.001)、網路偏差動機(r=.422 ; p<.001)、衝動性(r=.082 ; p<.05)、冒險性(r=.189 ; p<.001)及投機性(r=.181 ; p<.001)均呈現顯著正相關，因此，當網路使用者所從事之網路風險休閒活動程度越高，其網路風險職業活動、網路負面誘因、網路偏差動機、衝動性、冒險性及投機動性之程度也越高。此外，網路風險休閒活動與社會監控(r=-.091 ; p<.01)及物理監控(r=-.106 ; p<.01)呈現顯著負相關，亦即網路使用者從事之風險性網路休閒活動程度越高，則個人的社會監控及物理監控程度越低。

最後，在網路風險職業活動構面中，經皮爾森積差相關分析後可發現，網路風險職業活動與網路負面誘因(r=.219 ; p<.001)、網路偏差動機(r=.413 ; p<.001)、衝動性(r=.161 ; p<.001)、冒險性(r=.226 ; p<.001)、投機性(r=.208 ; p<.001)均呈現顯著正相關，因此，當網路使用者所從事之網路風險職業活動程度越高，其網路負面誘因、網路偏差動機、衝動性、冒險性及投機性之程度也越高。此外，網路風險職業活動與社會監控(r=-.067 ; p<.05)及物理監控(r=-.198 ; p<.001)呈現顯著負相關，亦即網路使用者從事之風險性網路職業活動程度越高，則個人的社會監控及物理監控之程度越低。

(二)被害情境與機會與各因素構面之相關性

有關被害情境與機會與各態度量表之皮爾森積差相關結果，如表 4-3-2 所示。首先，在社會監控構面中，社會監控與物理監控(r=.175 ; p<.001)呈現顯著正相關，故網路使用者在網路使用過程中的社會監控程度越高，則其物理監控程度亦越高。

其次，在物理監控構面中，物理監控與網路偏差動機(r=-.152 ; p<.001)、衝動性(r=-.113 ; p<.001)及投機性(r=-.161 ; p<.001)呈現顯著負相關，亦即網路使用者在網路使用過程中之物理監控程度越高，則個人的網路偏差動機、衝動性及冒險性之程度越低。

再者，在網路負面誘因構面中，網路負面誘因與網路偏差動機(r=.441 ; p<.001)、冒險性(r=.217 ; p<.001)及投機性(r=.115 ; p<.01)呈現顯著正相關，亦即網路使用者之網路負面誘因程度越高，則個人之網路偏差動機、冒險性及投機性之程度越高。

最後，在網路偏差動機構面中，經皮爾森積差相關分析後可發現，網路偏差動機與衝動性(r=.132 ; p<.001)、冒險性(r=.284 ; p<.001)及投機性(r=.262 ; p<.001)呈現顯著正相關，亦即網路使用者之網路偏差動機程度越高，其衝動性、冒險性及投機性之程度越高。

(三)低自我控制與各因素構面之相關性

在低自我控制部分，在衝動性方面，衝動性與冒險性(r=.282 ; p<.001)及投機性(r=.252 ; p<.001)呈現顯著正相關，當網路使用者之衝動性程度越高，則其冒險性及投機性程度也越高。在冒險性方面，冒險性與投機性(r=.133 ; p<.001)呈現顯著正相關，當網路使用者之冒險性程度越高，則其投機性程度也越高。

表 4-3-2 網路詐欺各因素構面之相關分析表

	網路休閒活動	網路職業活動	網路風險休閒活動	網路風險職業活動 (Ln)[56]	社會監控	物理監控	網路負面誘因	網路偏差動機 (Sqrt)[57]	衝動性	冒險性	投機性
網路休閒活動	–										
網路職業活動	**.443*****	–									
網路風險休閒活動	-.037	-.034	–								
網路風險職業活動	**-.122*****	**-.129*****	**.362*****	–							
社會監控	**.115****	**.129*****	**-.091****	**-.067***	–						
物理監控	**.285*****	**.119*****	**-.106****	**-.198*****	**.175*****	–					
網路負面誘因	**-.108****	-.056	**.378*****	**.219*****	-.025	-.030	–				
網路偏差動機	**-.286****	**-.219*****	**.422*****	**.413*****	-.004	**-.152*****	**.441*****	–			
衝動性	-.003	**-.093****	**.082***	**.161*****	-.060	**-.113*****	.019	**.132*****	–		
冒險性	**-.096****	**-.088****	**.189*****	**.226*****	-.011	-.049	**.217*****	**.284*****	**.282*****	–	
投機性	**-.117****	**-.160*****	**.181*****	**.208*****	-.019	**-.161*****	**.115****	**.262*****	**.252*****	**.133*****	–

註:*p<.05 ; **p<.01 ; ***p<.001

[56] Ln 代表變項經自然對數轉換(Natural logarithm transformation)

[57] Sqrt 代表變項經平方根轉換(Square root transformation)

第四節 性別與網路詐欺被害影響因素及理論模式分析

本研究目的在於探討不同性別間網路詐欺被害影響因素，為深入探究影響不同性別網路詐欺被害之影響因素，故根據前述二節各變項對於網路詐欺被害之差異、相關分析結果，對於本研究所設計之依變項，包括「是否被害」及「被害次數」進行多變量分析，藉以深入了解影響不同性別網路詐欺被害之重要因素，並據此建立有效解釋兩性間網路詐欺被害差異之理論模型架構。

在本研究所設計之依變項中，以是否曾有網路詐欺被害經驗以及網路詐欺被害次數兩個重要變項來建構網路詐欺被害之概念，自變項則為研究架構中所建構之各因素構面。在是否曾有網路詐欺被害經驗部分，因本變項為二分類之間斷變項，故採用二元邏輯斯迴歸(Binary Logistic Regression)進行分析，而在被害次數部分，因此變項係為計數型之資料，故對於單位時間內事件發生次數之預測及解釋則採用廣義線性模型(Generalized Linear Models)中之卜瓦松迴歸(Poisson Regression)進行分析。

綜合上述分析內容，本節分析內容共包括兩個部分，第一部分以二元 Logistic 迴歸進行不同性別網路詐欺被害影響因素之理論模式解釋，並探究對依變項具有重要影響力及解釋力之自變項，第二部分則以卜瓦松迴歸對於被害次數進行分析，茲分述如後:

一、網路詐欺被害經驗之二元 Logistic 迴歸分析

為探究不同性別間網路詐欺之被害差異因素及各自變項與依變項間之差異因素，故根據前述卡方檢定、獨立樣本 t 檢定、單因子變異數分析及相關分析等差異性分析、相關分析後，對於與依變項(是否被害)具有顯著關聯性之自變項投入二元 Logistic 迴歸方程式中進行分析，經檢視前述分析結果，篩選出與依變項有顯著關聯性之自變項包括:「性別」、「年齡」、「職業」、「收入」、「教育程度」、「每次上網時數」、「每周上網次數」、「平日上網時段」、「假日上網時段」、「網路休閒活動」、「網路職業活動」、「網路風險休閒活動」、「網路風險職業活動」、「社會監控」、「物理監控」、「網路負面誘因」、「網路偏差動機」、「衝動性」、「冒險性」及「投機性」等 20 個變項全數投入二元 Logistic 迴歸方程式中，以了解各自變項對於依變項之解釋及影響力。

(一)二元 Logistic 迴歸模型配適度檢驗

本研究考量研究之依變項為是否被害之二分類間斷變項，為避免殘差未符合常態性分配及依變項預測機率值無法介於 0 至 1 之間，故係採用二元 Logistic 迴歸進行分析。在二元 Logistic 迴歸模型中，自變項可為類別變項或連續變項，但若為類別變項，則需先轉化為虛擬變項(dummy variable)始可投入迴歸方程式中，故本研究先就「性別」、「職業」、「每次上網時數」、「每周上網次數」、「平日上網時段」、「假日上網時段」等變項，轉化為虛擬變項，並依據各組中平均數最低者列為參考組，以進行迴歸模型之解釋。

在模型之配適度檢驗中，首先，由於自變項間之多元共線性會導致迴歸模型中之迴歸係數產生正負號與期望者相反之衝突現象，並導致迴歸係數及標準誤過度膨脹，從而導致迴歸估計不正確，故本研究對於投入迴歸方程式中的自變項是否具有多元共線性(multicollinearity)之問題進行檢視及診斷。在多元共線性之診斷部分，本研究先就相關矩陣中之皮爾森積差相關係數進行檢視，一般認為變項間之相關係數在 0.8 以上即具有多元共線性之問題，此外，雖然二元 Logistic 迴歸無法進行多元共線性診斷，但可透過線性迴歸模式，將前述自變項及依變項投入一般線性迴歸模式中進行檢驗，而本研究除以變異數膨脹係數，或稱 VIF 值(Variance inflation factor, VIF)作為共線性問題之診斷依據外，亦根據特徵值(Eigenvalue)及條件指數(Conditional index, CI)進行共線性判斷。

在共線性之診斷方面，容忍值係為 VIF 值之倒數，一般認為容忍值小於 0.2 代表該自變項與其他自變項間存在共線性問題，而 VIF 值大於 5 時，則可認為自變項間已具有較高相關，若 VIF 值大於 10 時，表示共線性問題嚴重。在特徵值與條件指數方面，特徵值越小，則代表各解釋變項間具有相關性，而條件指數(CI 值)越高表示共線性問題嚴重，一般係認為 CI 值介於 30 至 100 間，迴歸模式具有中度至高度之共線性問題，若大於 100，則顯示迴歸模式具有嚴重的共線性問題(邱皓政，2010)，而經共線性診斷後，本研究之自變項間並未有共線性之情形。

其次，本研究在進行二元 Logistic 迴歸部分，分別就全體樣本、男性樣本及女性樣本進行網路詐欺被害與否之分析，以了解各分組樣本中，對於影響網路詐欺被害與否之因素是否具有差異。在迴歸模型之配適度檢驗方面，除了以 Hosmer-Lemeshow 檢定及

Omnibus 檢定對於整體模型進行配適度之考驗外，亦在不同解釋模式中加入不同觀察變項，比較各模型間-2LL 值(-2 對數概似值)、χ^2 值之改變程度及 Cox & Snell R^2、Nagelkerke R^2 值之高低，以建構最合適的被害解釋模型。

有關本研究所建構之二元 Logistic 迴歸模型之配適度綜合檢驗如下表 4-4-1 所示。首先，經 Omnibus 檢定後，三個迴歸模型達統計上極為顯著之水準，顯示投入迴歸方程式之變項確實對於依變項(網路詐欺被害與否)有顯著影響力。其次，經 Hosmer 與 Lemeshow 檢定後，三個迴歸模型均未達統計上之顯著水準，顯示本研究所建構之整體解釋模型與資料之整體擬合程度高。再者，在模型之分類正確性部分，在全體樣本中，在未將任何變項投入迴歸方程式時，該模型之初步預測正確率為 83.7%，俟投入各變項後，整體模型之預測正確性提升至 89.5%。在男性樣本中，在未將任何變項投入迴歸方程式時，該模型之初步預測正確率為 79.3%，俟投入各變項後，整體模型之預測正確性提升至 88.1%。在女性樣本中，在未將任何變項投入迴歸方程式時，該模型之初步預測正確率為 88.4%，俟投入各變項後，整體模型之預測正確性提升至 92.5%。

綜合上述二元 Logistic 迴歸模型之配適度檢驗指標後，本研究建構之三個解釋模型皆具有良好的配適度，整體模型與資料之擬合程度高、投入迴歸方程式中之自變項確實對於依變項具有解釋能力，而在變項投入迴歸方程式後，模型之卡方值均顯著下降，且各模型之整體預測正確性均較未投入變項前提升，顯示本研究投入迴歸方程式中的變項確實提升整體預測正確性。

表 4-4-1 網路詐欺被害二元邏輯斯(logistic)迴歸模型之整體配適度檢定

迴歸模型	Omnibus 檢定		-2 對數	Hosmer 與 Lemeshow 檢定		分類正確性
	卡方值	顯著性	概似值	卡方值	顯著性	（前/後）
全體樣本 (N=870)	**271.100*****		495.817	χ^2=3.744 ; p=.879		83.7% ; 89.5%
男性 (N=455)	**206.457*****		257.105	χ^2=9.051 ; p=.338		79.3% ; 88.1%
女性 (N=415)	**110.882*****		186.418	χ^2=5.046 ; p=.753		88.4% ; 92.5%

註:***p<.001

(二)二元 Logistic 迴歸分析結果

經前述模型配適度檢定、模型解釋力考驗及迴歸模型預測正確率之分析後，接下來將探究迴歸模型中各預測變項與依變項間之關係。本研究係以 Wald 檢驗法對於各預測變項之迴歸係數值進行檢驗，檢視迴歸係數值是否達統計上之顯著水準。其次，對於各預測變項之事件預測機率倍數係以 Exp(B)，亦即勝算比(Odds Ratio)作為解釋依據，以了解各預測變項與各自對照組間預測依變項機率之倍數概率。最後，在模型中各變項之相對重要性係以 Wald 值作為判斷依據，故解釋變項之 Wald 值越大，則顯示該變項在二元邏輯斯迴歸模型中對於依變項有較高的解釋能力。本研究為探究不同性別網路詐欺被害之影響因素，故將分析模型以全體樣本、男性及女性進行分析，以了解各組中影響網路詐欺被害因子之差異，相關分析結果如下表 4-4-2 所示。

1.全體樣本

模式一係以二元邏輯斯迴歸對於全體樣本進行分析，以了解網路詐欺被害影響因素。首先，在個人基本特性方面，經迴歸分析之結果後，性別、年齡、職業、收入及教育程度均達統計上之顯著水準($p<.05$)，顯示個人基本特性變項對於網路詐欺被害與否均具有解釋力。

在性別部分，網路詐欺被害發生機率與性別呈正相關，男性較女性更容易遭受網路詐欺被害(B=.604 ; Wald=5.764*)。在年齡部分，年齡與網路詐欺被害呈負相關，顯示年齡較低者相較於年齡較長者，有較高的網路詐欺被害之機率(B=-.561 ; Wald=10.112**)。在職業部分，網路詐欺被害發生機率與職業呈正相關，無業者較就業者有較高的網路詐欺被害機率(B=1.265 ; Wald=15.985***)。在收入部分，收入與網路詐欺被害呈正相關，顯示收入較高者相較於收入較低者，有較高的網路詐欺被害之機率(B=.486 ; Wald=12.851***)。在教育程度部分，教育程度與網路詐欺被害呈負相關，顯示教育程度較低者相較於教育程度較高者，有較高的網路詐欺被害之機率(B=-.405 ; Wald=5.578*)，綜合上述結果顯示，男性、年齡較低者、無業者、收入較高者、教育程度較低者有較高的網路詐欺被害可能性。

其次，在網路使用特性部分，經迴歸分析之結果後，每次上網時數、每周上網次數、平日上網時段及假日上網時段中之部分變項達統計上之顯著水準(p<.05)，顯示網路使用特性變項對於是否網路詐欺被害具有解釋力。在每次上網時數部分，經轉化為虛擬變項後，中上網時數(3-7 小時)及高上網時數(7 小時以上)均達統計上之顯著水準(p<.05)。其中，中上網時數(3-7 小時)相較於低上網時數(未滿 3 小時)有較高被害機率(B=1.466 ; Wald=19.836***)，而高上網時數(7 小時以上)相較於低上網時數(未滿 3 小時)亦有較高的被害機率(B=.929 ; Wald=5.442*)。在每周上網次數部分，經轉化為虛擬變項後，僅有中上網次數達統計上之顯著水準(p<.05)，中上網次數(7-9 次)相較於低上網次數(未滿 7 次)有較高的被害機率(B=1.286 ; Wald=7.499**)。

在平日上網時段部分，經轉化為虛擬變項並投入迴歸方程式後，平日夜間上網時段(16-24 時)及平日深夜上網時段(0-8 時)均達統計上之顯著水準(p<.05)，其中，平日夜間上網時段(16-24 時)相較於平日白天上網時段(8-16 時)有較高的被害機率(B=1.403 ; Wald=6.964**)，而平日深夜上網時段(0-8 時)相較於平日白天上網時段(8-16 時)有較高的被害機率(B=1.689 ; Wald=5.893*)。在假日上網時段部分，經轉化為虛擬變項後，僅有假日深夜上網時段(0-8 時)達統計上之顯著水準(p<.05)，其中，假日深夜上網時段(0-8 時)相較於假日白天上網時段(8-16 時)有較高的被害機率(B=1.822 ; Wald=18.193***)。綜合上述結果顯示，每次上網 3-7 小時及 7 小時以上、每周上網 7-9 次、平日夜間、深夜時段上網者及假日深夜時段上網者，有較高的網路詐欺被害機率。

再者，在網路生活型態方面，僅有網路風險職業活動達統計上顯著水準(p<.05)，其餘變項則未達統計上之顯著水準，其中，網路風險職業活動與網路詐欺被害呈正相關，顯示從事較多網路風險職業活動者相較於從事較少網路風險職業活動者，有較高的網路詐欺被害之機率(B=1.230 ; Wald=11.024**)。在被害情境與機會方面，社會監控及網路負面誘因達統計上顯著水準(p<.05)，其餘變項則未達統計上之顯著水準，其中，社會監控與網路詐欺被害呈負相關，顯示社會監控較低者相較於社會監控較高者，有較高的網路詐欺被害之機率(B=-.426 ; Wald=4.529*)，而網路負面誘因則與網路詐欺被害呈正相關，顯示接收較多網路負面誘因者相較於接收較少網路負面誘因者，有較高的網路詐欺被害

之機率(B=1.443 ; Wald=8.077**)，綜上可知，在網路使用過程中，從事較多網路風險職業活動、社會監控程度較低及接收較多網路負面誘因者，有較高的網路詐欺被害機率。

最後，在低自我控制方面，衝動性、冒險性及投機性等三個變項均達統計上顯著水準(p<.05)。在衝動性部分，衝動性與網路詐欺被害呈正相關，顯示衝動性程度較高者相較於衝動性程度較低者，具有較高的網路詐欺被害之機率(B=1.436 ; Wald=10.890***)。在冒險性部分，冒險性與網路詐欺被害呈正相關，顯示冒險性程度較高者相較於冒險性程度較低者，具有較高的網路詐欺被害之機率(B=.675 ; Wald=9.863**)，而在投機性部分，投機性與網路詐欺被害呈正相關，顯示投機性程度較高者相較於投機性程度較低者，具有較高的網路詐欺被害之機率(B=.759 ; Wald=11.752**)，綜上可知，具有較高衝動性、冒險性及投機性程度者，有較高的網路詐欺被害機率。

由上述分析可得知，在二元邏輯斯迴歸方程式中，與依變項（是否被害）有顯著關聯性之變項包括:性別、年齡、職業、收入、教育程度、每次上網 3-7 小時、每次上網 7 小時以上、每周上網 7-9 次、平日夜間時段上網、平日深夜時段上網、假日深夜時段上網、網路風險職業活動、社會監控、網路負面誘因、衝動性、冒險性及投機性等變項。在解釋全體樣本網路詐欺被害與否之重要性依序為假日深夜上網時段、其次為職業（無業組），最後則為收入。此外，經全體變項投入迴歸方程式後，整體模型解釋能力介於 26.8%至 45.7%(Cox & Snell R^2=.268 ; Nagel Kerke R^2=.457)，整體模型預測率從原本的 83.7%提升至 89.5%。

2.男性樣本

模式二係以二元邏輯斯迴歸對於男性樣本進行分析，以了解網路詐欺被害影響因素。首先，在個人基本特性方面，經迴歸分析後，年齡及收入變項達統計上之顯著水準(p<.05)，顯示個人基本特性變項對於網路詐欺被害與否具有部分解釋能力。在年齡部分，年齡與網路詐欺被害呈負相關，顯示年齡較低者相較於年齡較長者，有較高的網路詐欺被害之機率(B=-.660 ; Wald=7.437**)。在職業部分，網路詐欺被害發生機率與職業呈正相關，無業者較就業者有較高網路詐欺被害機率(B=1.224 ; Wald=9.227**)。綜合上述結果顯示，年齡較低者及無業者有較高的網路詐欺被害可能性。

其次，在網路使用特性部分，經迴歸分析之結果後，每次上網時數、每周上網次數、平日上網時段及假日上網時段中之部分變項達統計上之顯著水準(p<.05)，顯示網路使用特性變項對於是否網路詐欺被害具有解釋力。在每次上網時數部分，經轉化為虛擬變項後，中上網時數(3-7 小時)及高上網時數(7 小時以上)均達統計上之顯著水準(p<.05)。其中，中上網時數(3-7 小時)相較於低上網時數(未滿 3 小時)有較高網路詐欺被害機率(B=1.662 ; Wald=13.162**)，而高上網時數(7 小時以上)相較於低上網時數(未滿 3 小時)亦有較高的被害機率(B=1.092 ; Wald=4.114*)。在每周上網次數部分，僅有中上網次數(7-9 次)達統計上之顯著水準(p<.05)，中上網次數(7-9 次)相較於低上網次數(未滿 7 次)有較高的被害機率(B=1.687 ; Wald=7.452**)。

在平日上網時段部分，經轉化為虛擬變項並投入迴歸方程式後，平日夜間上網時段(16-24 時)及平日深夜上網時段(0-8 時)均達統計上之顯著水準(p<.05)。其中，平日夜間上網時段(16-24 時)相較於平日白天上網時段(8-16 時)有較高的被害機率(B=1.550 ; Wald=4.896*)，而平日深夜上網時段(0-8 時)相較於平日白天上網時段(8-16 時)有較高的被害機率(B=1.925 ; Wald=4.213*)。在假日上網時段部分，經轉化為虛擬變項後，僅有假日深夜上網時段(0-8 時)達統計上之顯著水準(p<.05)，其中，假日深夜上網時段(0-8 時)相較於假日白天上網時段(8-16 時)有較高的被害機率(B=1.540 ; Wald=16.276***)。綜合上述結果顯示，每次上網 3-7 小時及 7 小時以上、每周上網 7-9 次、平日夜間及深夜時段上網者、假日深夜時段上網者，有較高的網路詐欺被害機率。

再者，在網路生活型態方面，經迴歸分析之結果後，網路休閒活動、網路職業活動及網路風險職業活動等三個變項達統計上之顯著水準(p<.05)，顯示多數網路生活型態變項對於網路詐欺被害與否具有解釋力。在網路休閒活動部分，網路休閒活動與網路詐欺被害呈負相關，顯示從事較多網路休閒活動者相較於從事較少網路休閒活動者，其網路詐欺被害機率較低(B=-1.506 ; Wald=4.387*)。在網路職業活動部分，網路職業活動與網路詐欺被害呈負相關，顯示從事較多網路職業活動者相較於從事較少網路職業活動者，其網路詐欺被害機率較低(B=-2.951 ; Wald=8.230**)。在網路風險職業活動部分，網路風

險職業活動與網路詐欺被害呈正相關，顯示從事較多網路風險職業活動者相較於從事較少網路風險職業活動者，有較高的網路詐欺被害之機率(B=1.017 ; Wald=4.308**)。

在被害情境與機會方面，經迴歸分析之結果後，社會監控及網路負面誘因達統計上顯著水準(p<.05)，其中，社會監控與網路詐欺被害呈負相關，顯示社會監控較低者相較於社會監控較高者，有較高的網路詐欺被害之機率(B=-.824 ; Wald=8.465**)，而網路負面誘因與網路詐欺被害呈正相關，顯示接收較多網路負面誘因者相較於接收較少網路負面誘因者，有較高的網路詐欺被害之機率(B=1.576 ; Wald=5.514*)。綜合上述分析可知，在網路使用過程中，從事較少網路休閒活動及網路職業活動、從事較多網路風險職業活動、社會監控程度較低及接收較多網路負面誘因者，有較高的網路詐欺被害機率。

最後，在低自我控制方面，經迴歸分析之結果後，衝動性及冒險性等二個變項均達統計上顯著水準(p<.05)，顯示多數低自我控制變項對於是否網路詐欺被害具有解釋力。在衝動性部分，衝動性與網路詐欺被害呈正相關，顯示衝動性程度較高者相較於衝動性程度較低者，有較高的網路詐欺被害之機率(B=1.798 ; Wald=9.746**)。在冒險性部分，冒險性與網路詐欺被害呈正相關，顯示冒險性程度較高者相較於冒險性程度較低者，有較高的網路詐欺被害之機率(B=.940 ; Wald=10.581**)，綜上可知，網路使用者具有較高衝動性及冒險性程度者，有較高的網路詐欺被害機率。

綜合上述分析可得知，在男性樣本之二元邏輯斯迴歸方程式中，與依變項(網路詐欺被害與否)具有顯著關聯性之變項包括:年齡、職業、每次上網 3-7 小時、每次上網 7 小時以上、每周上網 7-9 次、平日夜間時段上網、平日深夜時段上網、假日深夜時段上網、網路休閒活動、網路職業活動、網路風險職業活動、社會監控、網路負面誘因、衝動性及冒險性等變項。在解釋男性網路詐欺被害與否之重要性依序為假日深夜上網時段、其次為每次上網 3-7 小時，最後則為冒險性。此外，經全體變項投入迴歸方程式後，整體模型解釋能力介於 36.5%至 57.1%(Cox & Snell R^2=.365 ; Nagel Kerke R^2=.571)，整體模型預測率從原本 79.3%提升至 88.1%。

3.女性樣本之二元邏輯斯迴歸分析

模式三係以二元邏輯斯迴歸對於女性樣本進行分析，以了解影響網路詐欺被害之因素。首先，在個人基本特性方面，經迴歸分析之結果後，職業及收入變項達統計上之顯著水準($p<.05$)，顯示個人基本特性變項對於是否網路詐欺被害具有部分解釋力。其中，在職業部分，網路詐欺被害發生機率與職業呈正相關，無業者較就業者有較高的網路詐欺被害機率($B=2.008$; $Wald=10.933^{**}$)。在收入部分，收入與網路詐欺被害呈正相關，顯示收入較高者相較於收入較低者，有較高網路詐欺被害之機率($B=.990$; $Wald=14.662^{***}$)。綜合上述結果顯示，無業者及收入較高者，有較高的網路詐欺被害可能性。

其次，在網路使用特性部分，經迴歸分析之結果後，每次上網時數、平日上網時段及假日上網時段中之部分變項達統計上之顯著水準($p<.05$)，但每周上網次數則未達統計上之顯著水準，顯示網路使用特性變項對於是否網路詐欺被害具有部分解釋力。在每次上網時數部分，中上網時數(3-7 小時)達統計上之顯著水準($p<.05$)，而中上網時數(3-7 小時)相較於低上網時數(未滿 3 小時)有較高的被害機率($B=1.588$; $Wald=6.044^{**}$)。

在平日上網時段部分，經轉化為虛擬變項並投入迴歸方程式後，僅有平日深夜上網時段(0-8 時)達統計上之顯著水準($p<.05$)，其中，平日深夜上網時段(0-8 時)相較於平日白天上網時段(8-16 時)有較高的被害機率($B=1.990$; $Wald=4.430^{*}$)。在假日上網時段部分，經轉化為虛擬變項後，僅有假日深夜上網時段(0-8 時)達統計上之顯著水準($p<.05$)，其中，假日深夜上網時段(0-8 時)相較於假日白天上網時段(8-16 時)有較高的被害機率($B=1.824$; $Wald=5.954^{*}$)，綜合上述結果顯示，每次上網 3-7 小時、平日深夜時段及假日深夜時段上網者，有較高的網路詐欺被害機率。

再者，在網路生活型態方面，經迴歸分析之結果後，網路休閒活動及網路風險職業活動等二個變項達統計上之顯著水準($p<.05$)，顯示部分網路生活型態變項對於網路詐欺被害與否具有解釋力。在網路休閒活動部分，網路休閒活動與網路詐欺被害呈負相關，顯示從事較多網路休閒活動者相較於從事較少網路休閒活動者，其網路詐欺被害機率較低($B=-4.916$; $Wald=4.912^{*}$)。在網路風險職業活動部分，網路風險職業活動與網路詐欺

被害呈正相關，顯示從事較多網路風險職業活動者相較於從事較少網路風險職業活動者，有較高的網路詐欺被害之機率(B=1.298 ; Wald=9.773**)。

在被害情境與機會方面，經迴歸分析之結果後，僅有網路負面誘因達統計上之顯著水準(p<.05)，其餘變項則未達統計上之顯著水準。其中，網路負面誘因與網路詐欺被害呈正相關，顯示接收較多網路負面誘因者相較於接收較少網路負面誘因者，有較高網路詐欺被害之機率(B=1.988 ; Wald=5.223**)。綜合上述分析可知，在網路使用之過程中，從事較少網路休閒活動、從事較高網路風險職業活動及接收較多網路負面誘因者，有較高的網路詐欺被害機率。

最後，在低自我控制方面，經迴歸分析之結果後，衝動性及投機性等二個變項均達統計上顯著水準(p<.05)，顯示多數低自我控制變項對於是否網路詐欺被害具有解釋力。在衝動性部分，衝動性與網路詐欺被害呈正相關，顯示衝動性程度較高者相較於衝動性程度較低者，有較高的網路詐欺被害之機率(B=1.684 ; Wald=5.156*)。在投機性部分，投機性與網路詐欺被害呈正相關，顯示投機性程度較高者相較於投機性程度較低者，有較高的網路詐欺被害之機率(B=1.335 ; Wald=12.976*)，綜上可知，網路使用者具有較高衝動性及投機性程度者，有較高的被害機率。

綜合上述分析可得知，在女性樣本之二元邏輯斯迴歸方程式中，與依變項(網路詐欺被害與否)具有顯著關聯性之變項包括:職業、收入、每次上網 3-7 小時、平日深夜時段上網、假日深夜時段上網、網路休閒活動、網路風險職業活動、網路負面誘因、衝動性及投機性等變項。在迴歸模型中解釋依變項之重要性係以 Wald 值作為判斷依據，故在解釋女性網路詐欺被害與否之重要性依序為收入、其次為投機性，最後則為職業。此外，經全體變項投入迴歸方程式後，整體模型解釋能力介於 23.4%至 45.8%(Cox & Snell R^2=.234 ; Nagel Kerke R^2=.458)，整體模型預測率從原本模型之 88.4%提升至 92.5%，代表本模型具有較高的解釋力及預測力。

4.各分組樣本二元邏輯斯迴歸之綜合分析

本研究前述對於全體樣本、男性及女性樣本分別進行二元邏輯斯迴歸分析。經迴歸分析結果發現，首先，影響全體樣本網路詐欺被害與否之重要因子包括:性別、年齡、職業、收入、教育程度、每次上網 3-7 小時(中上網時數)、每次上網 7 小時以上(高上網時數)、每周上網 7-9 次(高上網次數)、平日夜間時段上網(16-24 時)、平日深夜時段上網(0-8 時)、假日深夜時段上網(0-8 時)、網路風險職業活動、社會監控、網路負面誘因、衝動性、冒險性及投機性等變項。

其次，影響男性樣本網路詐欺被害與否之重要因子包括:年齡、職業、每次上網 3-7 小時(中上網時數)、每次上網 7 小時以上(高上網時數)、每周上網 7-9 次(高上網次數)、平日夜間時段上網(16-24 時)、平日深夜時段上網(0-8 時)、假日深夜時段上網(0-8 時)、網路休閒活動、網路職業活動、網路風險職業活動、社會監控、網路負面誘因、衝動性及冒險性等變項。

最後，影響女性樣本網路詐欺被害與否之重要因子包括: 職業、收入、每次上網 3-7 小時(中上網時數)、平日深夜時段上網(0-8 時)、假日深夜時段上網(0-8 時)、網路休閒活動、網路風險職業活動、網路負面誘因、衝動性及投機性等變項。

綜合上述迴歸分析結果後一致發現，在各分組受試者中，影響網路詐欺被害與否之重要共通性因子包括:職業(無業組)、每次上網 3-7 小時(中上網時數)、平日深夜時段上網(0-8 時)、假日深夜時段上網(0-8 時)、網路風險職業活動、網路負面誘因及衝動性等七個重要變項。換言之，當網路使用者為無業者、每次上網 3-7 小時(中上網時數)、平日在深夜時段(0-8 時)上網、假日在深夜時段(0-8 時)上網、從事較多的網路風險職業活動，具有較高的網路負面誘因及衝動性者，無論在全體樣本、男性或女性樣本中，網路詐欺被害之機率皆較高。

表 4-4-2 網路詐欺被害之二元邏輯斯(logistic)迴歸分析

變　項	全體樣本(N=870)			男性(N=455)			女性(N=415)		
	B	Wald	Exp(B)	B	Wald	Exp(B)	B	Wald	Exp(B)
個人基本特性									
性別(男)	.604	**5.764***	1.830						
年齡	-.561	**10.112****	.570	-.660	**7.437****	.517	-.479	2.227	.619
職業(無業組)	1.265	**15.985*****	3.542	1.224	**9.227****	3.400	2.008	**10.933****	7.452
收入	.486	**12.851*****	1.626	.225	1.592	1.253	.990	**14.662*****	2.692
教育程度	-.405	**5.578***	.667	-.160	.455	.852	-.541	2.915	.582
網路使用特性									
每次上網時數									
中上網時數(3-7 小時)	1.466	**19.836*****	4.332	1.662	**13.162****	5.268	1.588	**6.044****	4.076
高上網時數(7 小時以上)	.929	**5.442***	2.531	1.092	**4.114***	2.981	.545	.567	1.713
每周上網次數									
中上網次數(7-9 次)	1.286	**7.499****	3.681	1.687	**7.452****	6.214	-.070	.158	.720
高上網次數(10 次以上)	.356	1.342	.421	1.117	1.147	1.852	-.714	.596	.547
平日上網時段									
夜間上網時段(16-24 時)	1.403	**6.964****	4.068	1.550	**4.896***	4.713	1.790	3.756	5.988
深夜上網時段(0-8 時)	1.689	**5.893***	5.414	1.925	**4.213***	6.854	1.990	**4.430***	6.908
假日上網時段									
夜間上網時段(16-24 時)	.654	3.057	1.923	1.073	3.198	2.923	.155	.089	1.168
深夜上網時段(0-8 時)	1.822	**18.193*****	6.809	1.540	**16.276*****	5.471	1.824	**5.954***	6.197
網路生活型態									

網路休閒活動	-1.805	3.150	.165	-1.506	**4.387***	.222	-4.916	**4.912***	.007
網路職業活動	-.342	1.997	.710	-2.951	**8.230****	.052	.079	.030	1.082
網路風險休閒活動	.973	2.083	2.646	.325	1.496	1.873	1.154	.513	3.172
網路風險職業活動(Ln)[58]	1.230	**11.024****	3.397	1.017	**4.308***	2.764	1.298	**9.773****	3.663
被害情境與機會									
社會監控	-.426	**4.529***	.653	-.824	**8.465****	.440	.073	.048	1.076
物理監控	-2.048	1.470	.129	-.074	.074	.933	-6.878	3.731	.001
網路負面誘因	1.443	**8.077****	4.231	1.576	**5.514***	4.673	1.988	**5.223****	7.303
網路偏差動機(Sqrt)[59]	.365	1.759	1.937	.162	1.170	1.186	.748	.849	2.113
低自我控制特性									
衝動性	1.436	**10.890*****	4.203	1.798	**9.746****	6.036	1.684	**5.156***	5.385
冒險性	.675	**9.863****	1.965	.940	**10.581****	2.560	.168	.213	1.183
投機性	.759	**11.752****	2.137	.485	2.407	1.624	1.335	**12.976***	3.799
常數(Constant)	-3.987	**1.892*****	.019	-2.218	.851	.051	3.412	.155	3.323
模型摘要									
-2 log likehood(對數概似值)		495.817			257.105			186.418	
模型卡方值(χ^2)及顯著性		**271.100*****			**206.457*****			**110.882*****	
H-L 檢定統計量及顯著性		χ^2=3.744 ; p=.879			χ^2=9.051 ; p=.338			χ^2=5.046 ; p=.753	
Pseudo R^2									
Cox & Snell R^2		.268			.365			.234	
Nagelkerke R^2		.457			.571			.458	

註: *p<.05 ; **p<.01 ; ***p<.001

註:性別:對照組=女性、職業:對照組=就業組、每次上網時數:對照組=低上網時數(未滿 3 小時)

每周上網次數:對照組=低上網次數(未滿 7 次)、平(假)日上網時段:對照組=白天上網時段(8-16 時)

[58] Ln 代表變項經自然對數轉換(Natural logarithm transformation)

[59] Sqrt 代表變項經平方根轉換(Square root transformation)

二、網路詐欺被害次數之 Poisson 迴歸分析

(一)離散計數型資料

在進行統計分析時,若依變項係為計算次數之變項,稱為計數型資料(Count Data),而在社會科學之研究中,多數計數型資料因其分布並非連續(Non-continous)、非常態分佈,且具有間斷性(Discrete)、稀少性(Rare)及非負整數(Nonnegative integer)之特性,故又稱為「離散型計數資料」(Discrete Count Data)。

在離散型計數資料中,因資料多為不連續、分布多為偏態且取值範圍小,故又被稱為受限的依變項(Limited Dependent),並經常被認為是分類變項的一種型態(Powers et al., 2000; Long et al., 2001; Long, 2011)。由於離散型計數資料服從於離散機率分配而非常態分配,故若將其視為連續、常態分布資料進行多變量分析(Multivariate statistical)則將因嚴重違反常態、線性及均方差之重要基本假設,而導致估計值產生嚴重的偏差,相應之統計推論值及檢驗亦無效(郭志剛,1999 ; Mertler & Vannatta, 2016; White et al., 2005)。有鑑於離散計數型資料無法適用於一般線性迴歸,故在 1980 年代後,在計量經濟學、社會科學領域研究中就逐漸發展出一套專門用以分析離散計數型資料之統計模型,稱為「離散選擇模型」或「計數變項模型」,而在離散選擇模型中,由於資料並不需假設符合常態分布,故可對於特定時間、空間中事件發生之次數進行較精確的分析及預測。

在離散選擇模型中,一般常見用以分析離散型計數資料之迴歸模式包括卜瓦松迴歸(Poisson Regression, PR)、廣義卜瓦松迴歸(Generalized Poisson Regression, GPR)、負二項迴歸(Negative Binomial Regression, NBR),以及當資料中有過多零值存在時所使用之零膨脹卜瓦松迴歸(Zero-Inflated Poisson Regression, ZIP)及零膨脹負二項迴歸(Zero-Inflated Negative Binomial Regression, ZINB)等模式。

本研究在網路詐欺被害次數之分析部分,考量此依變項係為偏態、非連續之分布,且具有間斷性、稀少性及非負整數之特性,係為離散計數型資料(Discrete Count Data)、資料服從離散機率分配,且對於單位時間內事件發生次數之分配服從卜瓦松分配(Poisson Distribution),故採用離散型計數資料之迴歸模式進行資料分析。在本研究模型建構之過程中,係以廣義線性模型(Generalized Linear Models)中對於單位時間或空間中

事件發生之數量能進行有效之預測及判斷之卜瓦松迴歸(Poisson Regression, PR)模型進行資料之分析。

在卜瓦松迴歸分析的過程中，本研究根據前述自變項與網路詐欺被害與否之卡方檢定、獨立樣本 t 檢定、單因子變異數分析及相關分析等差異及相關分析後，對於前揭具有顯著關聯性之自變項全數投入 Poisson 迴歸方程式中進行分析，經檢視前述分析結果，投入迴歸方程式中之自變項包括:「性別」、「年齡」、「職業」、「收入」、「教育程度」、「每次上網時數」、「每周上網次數」、「平日上網時段」、「假日上網時段」、「網路休閒活動」、「網路職業活動」、「網路風險休閒活動」、「網路風險職業活動」、「社會監控」、「物理監控」、「網路負面誘因」、「網路偏差動機」、「衝動性」、「冒險性」及「投機性」等 20 個變項，以了解各自變項對於依變項(網路詐欺被害次數)之解釋及預測力。

(二)網路詐欺被害次數 Poisson 迴歸模型之配適度檢驗

首先，在進行 Poisson 迴歸分析前，因類別變項需先轉化為虛擬變項，始可投入迴歸方程式中，故對於本研究先就「性別」、「職業」、「每次上網時數」、「每周上網次數」、「平日上網時段」、「假日上網時段」等類別變項，轉化為虛擬變項，並依據各組中平均數最低者列為參考組，以進行迴歸模型之分析與解釋。

其次，在模型之配適度檢驗中，由於自變項間之多元共線性會導致迴歸模型中之迴歸係數產生正負號與期望者相反之衝突現象，並導致迴歸係數及標準誤過度膨脹，從而導致迴歸估計不正確，故本研究對於投入迴歸方程式中的自變項是否具有多元共線性之問題進行檢視及診斷。在多元共線性之診斷部分，本研究除先檢視相關矩陣中之皮爾森積差相關係數值是否在 0.8 以上外，亦將所有自變項與依變項(網路詐欺被害次數)投入線性迴歸方程式中，並根據變異數膨脹係數(VIF 值)、特徵值及條件指數進行共線性之判斷，經共線性診斷後，本研究投入迴歸方程式中之自變項間並未有共線性之情形。

再者，在離散計數型資料之分析中，包括 Poission 迴歸模型、零膨脹 Poission 迴歸模型、廣義 Poission 迴歸模型、零膨脹廣義 Poission 迴歸模型、負二項迴歸模型及零膨脹負二項迴歸模型等迴歸分析模型。在諸多離散計數模型中，係根據資料之特性及資料

之離散程度，而選擇不同之迴歸分析模型，故對於離散模型之選擇，必須先就資料是否呈現過度離散(over-dispersion)之狀況，進行資料離散性檢定。

本研究為檢定資料是否呈現過度離散之狀況，先利用偏差值/自由度(deviance / d.f.)及皮爾森卡方值/自由度(Pearson χ^2/ d.f.)之值來進行資料離散性檢定，若該檢定值大於 1，則資料呈現過度離散(over-dispersion)情況，此時須採用負二項迴歸模型，但若檢定值小於 1，則資料呈現低度離散(under-dispersion)的情況，此時則採用卜瓦松迴歸模型（徐郁婷，2017 ; Hilbe, 2017）。經資料離散性檢定結果，由下表 4-4-3 所示，從表中可以得知，本研究依變項（網路詐欺被害次數）之偏差值/自由度及皮爾森卡方值/自由度均小於 1，可知本研究之離散計數型資料呈現低度離散(under-dispersion)之情況，故係採用卜瓦松迴歸模型進行迴歸分析。

此外，本研究除以偏差值/自由度(deviance / d.f.)及皮爾森卡方值/自由度(Pearson/ d.f.)之值來進行資料離散性檢定外，在模型之選擇部分，亦採用 Lagrange 乘數（子）檢定來進行輔助判斷，對於資料是否具有過大變異及應使用何種離散迴歸模型進行檢定，在 Lagrange 乘數（子）檢定之過程中，係採用離散輔助參數 θ(Theta)值對於負二項迴歸式進行檢定，若檢定結果 θ 值大於零之結果顯著時，則代表資料存在過度離散之狀況，此時必須採用負二項迴歸分析進行分析，反之則採用 Poisson 迴歸進行分析。經 Lagrange 乘數檢定結果，如下表 4-4-3 所示，從表中可以得知，將負二項式分配之輔助參數 0 作為虛無假設，則檢定結果不顯著(p>.05)，故必須採用 Poisson 迴歸進行分析。經過上述模型判斷準則後，確認本研究之依變項係以 Poission 迴歸進行資料之分析。

最後，在模型之配適度檢定部分，下表 4-4-3 呈現有關本研究所建構之 Poisson 迴歸模型之各項配適度(goodness-of-fit)。在配適度部分，因模型配適度指標卡方值(χ^2)並未達統計上之顯著水準(χ^2=108.487 ; d.f.=115 ; p>.05)，代表模型與資料之擬和度佳，兩者一致性高，此模型適用於預測被害次數。在 Omnibus 檢定部分，因檢定卡方值(χ^2)達統計上之顯著水準(χ^2=139.611 ; d.f.=21 ; p<.001)，代表本 Poisson 迴歸模型中至少有一迴歸係數不為零，亦即本模型中至少有一變項適合解釋依變項，因此投入迴歸方程式之自變項確實對於依變項有解釋及預測能力，而在模型的選擇上，本研究係以赤池信息量

準則(Akaike information criterion, AIC)為模型選擇準則，以避免因變數過多而誤判過度配適(overfitting)結果為較佳之模型，並以 AIC 值較小者做為較佳模型之選擇。

此外，雖然 Poisson 迴歸模型係離散計數型資料之標準模型，但 Poisson 迴歸分析有一個非常重要的特徵，假定資料之平均數與標準差相等，亦即資料須呈均等離散分布(Equi-dispersion)，然而就實際離散計數型之資料而言，因資料係由不同子群體所組成，因此造成母體產生異質性之狀況，從而使資料呈現過度離散(over-dispersion)或低度離散(under-dispersion)之狀況（張紹勳、林秀娟，2017）。

Mertler 和 Vannatta(2016)指出，在使用統計分析工具時，必須充分評估該樣本數據滿足統計假設的程度，而當資料輕微違反統計假設時，可採用穩健性(Robust)統計假設，以減少資料輕微違反基本假設之敏感程度，此種方法亦被肯認係精準且可靠的統計方式(Kennedy & Bush, 1985)。有鑑於此，本研究採用 Mertler 和 Vannatta(2016)、Cameron 與 Trivedi(2013)及張紹勳、林秀娟(2017)所建議之統計方法，在迴歸模型之估計方程式中採用穩健迴歸估計量(Robust Estimator)來控制輕微違反 Poisson 分布假設，以求得正確估計值，使整體迴歸方程式符合 Poisson 分布。

表 4-4-3 網路詐欺被害次數卜瓦松(Poisson)迴歸模型之配適度摘要

模型摘要	檢定值
Omnibus 檢定	
對數概似值/自由度/顯著性	**139.611***** ; d.f.=21
模型適合度檢定	
偏差值(Deviance) ; 自由度	109.670 ; d.f.=115
Pearson's 卡方值 ; 自由度	108.487 ; d.f.=115
偏差值/自由度 ;	.953
卡方值/自由度	.943
AIC ; BIC 值	502.249 ; 582.057
Lagrange 檢定	參數<0 (P<.001)

註:***p<.001

(三)網路詐欺被害次數影響因素之 Poission 迴歸分析[60]

下表 4-4-4 係以 Poission 迴歸對於全體樣本進行分析，以了解網路詐欺被害次數之影響因素。首先，在個人基本特性方面，經迴歸分析之結果後，僅有性別及年齡達統計上之顯著水準，顯示個人基本特性變項對於依變項(網路詐欺被害次數)具有部分解釋力。在性別部分，網路詐欺被害次數與性別呈正相關，男性相較女性有較高的網路詐欺被害次數(B=.269 ; Wald=22.762***)，且男性被害次數之發生率為女性被害次數發生率之 1.309 倍。在年齡部分，年齡與網路詐欺被害次數呈負相關，顯示年齡較低者相較於年齡較長者，有較高的網路詐欺被害次數(B=-.039 ; Wald=4.488*)，且年齡每增加 1 單位，則預期的網路詐欺被害對數計數值(log count)就會減少.039。綜合上述結果顯示，男性、年齡較低者、其網路詐欺被害次數較高。

其次，在網路使用特性部分，每次上網時數、每周上網次數、平日上網時段及假日上網時段均未達統計上之顯著水準，顯示網路使用特性未顯著預測網路詐欺被害次數。

再者，在網路生活型態方面，網路休閒活動及網路風險休閒活動達統計上顯著水準($p<.05$)，其餘變項則未達統計上之顯著水準，顯示網路生活型態變項對於依變項(網路詐欺被害次數)具有部分解釋力。在網路休閒活動部分，網路休閒活動與網路詐欺被害次數呈負相關，顯示從事較少網路休閒活動者相較於從事較多網路休閒活動者，有較高的網路詐欺被害次數(B=-.189 ; Wald=9.907**)，且網路休閒活動每增加 1 單位，則預期的網路詐欺被害對數計數值(log count)就會減少.189。在網路風險休閒活動部分，網路風險休閒活動與網路詐欺被害次數呈正相關，顯示從事較多網路風險休閒活動者相較於從事較少網路風險休閒活動者，有較高的網路詐欺被害次數(B=.097 ; Wald=6.895**)，且網路風險休閒活動每增加 1 單位，則預期的網路詐欺被害對數計數值(log count)就會增加.189。綜合上述結果顯示，在網路使用的過程中，有較少網路休閒活動，而有較多網路風險休閒活動者，其網路詐欺被害次數較高。

[60]Kutner 等人(2019)指出，由於樣本數太少、資訊欠佳，將造成迴歸方程式之結果產生偏誤。由於樣本數過少，預測變項過多，可能形成迴歸方程式雖整體達到顯著，但各預測變項之迴歸係數卻不顯著之情況，亦即在自變項過多而樣本數過少之情況下，各別變項之預測效率將低落，而造成迴歸方程式產生偏誤。在本研究之網路詐欺被害樣本中，若將樣本劃分為全體(N=142)、男性(N=94)、女性(N=48)，則將因自變項過多，男性、女性組樣本數過少，而無法形成迴歸預測方程式，故本研究僅以全體樣本進行迴歸分析。

在被害情境與機會方面，社會監控、物理監控及網路負面誘因均達統計上顯著水準($p<.05$)，顯示被害情境與機會之多數變項對於依變項（網路詐欺被害次數）具有解釋能力。在社會監控部分，社會監控與網路詐欺被害次數呈負相關，顯示社會監控較低者相較於社會監控較高者，有較高的網路詐欺被害次數(B=-.127 ; Wald=7.613**)，且社會監控每增加 1 單位，則預期的網路詐欺被害對數計數值(log count)就會減少.127。在物理監控部分，物理監控與網路詐欺被害次數呈負相關，顯示物理監控較低者相較於物理監控較高者，有較高的網路詐欺被害次數(B=-.228 ; Wald=22.720***)，且物理監控每增加 1 單位，則預期的網路詐欺被害對數計數值(log count)就會減少.228。在網路負面誘因部分，網路負面誘因與網路詐欺被害次數呈正相關，顯示接收較多網路負面誘因者相較於接收較少網路負面誘因者，有較高的網路詐欺被害次數(B=.129 ; Wald=7.254**)。綜上可知，在網路使用過程中，個人社會監控、物理監控程度較低及接收較多網路負面誘因者，具有較高的網路詐欺被害次數。

最後，在低自我控制特性部分，冒險性及投機性達統計上顯著水準，顯示部分變項對於網路詐欺被害次數具有預測能力。在冒險性部分，冒險性與網路詐欺被害呈正相關，顯示冒險性程度較高者相較於冒險性程度較低者，有較高的網路詐欺被害次數(B=.393 ; Wald=6.910**)，且冒險性每增加 1 單位，則預期的網路詐欺被害對數計數值(log count)就會增加.393，而在投機性部分，投機性與網路詐欺被害呈正相關，顯示投機性程度較高者相較於投機性程度較低者，有較高網路詐欺被害次數(B=.136 ; Wald=9.958**)，且投機性每增加 1 單位，則預期的網路詐欺被害對數計數值(log count)就會增加.136，綜上可知，具有較高冒險性及投機性程度者，有較高的被害機率。

綜合上述分析可得知，在全體樣本之 Poisson 迴歸方程式中，與依變項（網路詐欺被害次數）具有顯著關聯性之變項包括:性別、年齡、網路休閒活動、網路風險休閒活動、社會監控、物理監控、網路負面誘因、冒險性及投機性等變項。在迴歸模型中用以預測依變項之重要性係以 Wald 值作為判斷依據，故在預測網路詐欺被害次數之重要性依序為性別、其次為物理監控，最後則為投機性。

表 4-4-4 網路詐欺被害次數之卜瓦松(Poisson)迴歸模型分析(N=142)

變　項	B	RSE[61]	Wald	IRR[62]
個人基本特性				
性別(男)	.269	.0564	**22.762*****	1.309
年齡	-.039	.0182	**4.488***	.962
職業(無業組)	.047	.0559	.709	1.048
收入	.028	.0304	.829	1.028
教育程度	-.012	.0354	1.854	.949
網路使用特性				
每次上網時數				
中上網時數(3-7 小時)	.158	.0819	3.736	1.172
高上網時數(7 小時以上)	.008	.0647	.015	1.008
每周上網次數				
中上網次數(7-9 次)	.118	.1308	.817	1.125
高上網次數(10 次以上)	.043	.1142	.140	1.044
平日上網時段				
夜間上網時段(16-24 時)	.070	.1136	.377	1.072
深夜上網時段(0-8 時)	.032	.1010	.099	1.032
假日上網時段				
夜間上網時段(16-24 時)	.127	.0794	2.556	1.135
深夜上網時段(0-8 時)	.082	.0578	2.039	1.086
網路生活型態				
網路休閒活動	-.189	.0600	**9.907****	.828
網路職業活動	-.032	.1010	.099	.732
網路風險休閒活動	.097	.0368	**6.895****	1.101
網路風險職業活動(Ln)[63]	.070	.0374	3.535	1.073
被害情境與機會				
社會監控	-.127	.0459	**7.613****	.881
物理監控	-.228	.0479	**22.720*****	.796
網路負面誘因	.129	.0478	**7.254****	1.137
網路偏差動機(Sqrt)[64]	.348	.2296	2.296	1.416
低自我控制特性				
衝動性	.094	.1225	.583	1.098
冒險性	.393	.1496	**6.910****	1.482
投機性	.136	.0431	**9.958****	1.146
截距(Intercept)	.695	.5822	1.425	2.004

註:*p<.05 ; **p<.01 ; ***p<.001

註:性別:對照組=女性、職業:對照組=就業組、每次上網時數:對照組=低上網時數(未滿 3 小時)
每周上網次數:對照組=低上網次數(未滿 7 次)、平(假)日上網時段:對照組=白天上網時段(8-16 時)

[61] RSE 代表穩健標準誤估計量(Robust standard errors)
[62] IRR 代表事件發生比率(Incident rate ratios)
[63] Ln 代表變項經自然對數轉換(Natural logarithm transformation)
[64] Sqrt 代表變項經平方根轉換(Square root transformation)

第五節 網路詐欺重複被害影響因素分析

在網路詐欺被害風險因素之研究中，除了了解影響網路詐欺被害之風險因素外，必須更進一步深入探究影響網路詐欺重複被害可能性之因素為何、網路使用者具有何種個人弱點特質進而重複成為網路詐欺被害之標的，以及如何有效降低網路詐欺重複被害之風險外，更重要的是，透過重複被害現象之理解，可針對重複被害可能再次發生之情況。因此，本研究除了依據前述網路日常活動理論及自我控制理論之架構，分別對於網路詐欺是否被害以及被害次數分別進行二元邏輯斯迴歸及卜瓦松迴歸分析，以瞭解網路詐欺被害影響因素外，本節將進一步根據上述理論基礎，對於網路詐欺重複被害次數之影響因素進行深入分析，以探究影響網路詐欺重複被害次數之影響因素。

本節共分為二個部分，第一部分就網路詐欺被害次數進行描述性統計，以次數分配及百分比來對於調查樣本之重複被害與非重複被害者進行分析，其次則就網路詐欺重複被害次數進行卜瓦松迴歸分析，以期了解在網路詐欺被害重複次數之影響因素中，具有關鍵性之重要影響因子為何。

一、網路詐欺重複被害與非重複被害分析

(一)網路詐欺被害次數分析

本研究之全體調查樣本共計 870 位，在重複被害之分析部分，茲將全體樣本劃分為無被害經驗、單次被害經驗(被害次數為 1)以及重複被害經驗(被害次數 2 次以上)三組。無被害經驗者共計 728 位(占全體樣本 83.7%)、單次被害經驗者共計共計 41 位(占全體樣本 4.7%)、重複被害經驗者共計 101 位(占全體樣本 11.6%)，有關全體調查樣本分析如下表 4-5-1 所示:

表 4-5-1 網路詐欺被害次數分析表(N=870)

組別	人數	百分比(%)
無被害經驗(被害次數=0)	728	83.7
單次被害經驗(被害次數=1)	41	4.7
重複被害經驗(被害次數>1)	101	11.6

(二)網路詐欺重複被害次數分析

有關本研究調查樣本在網路詐欺被害次數分布如下圖 4-5-1 所示,從圖中可以得知,在網路詐欺被害次數中(N=142),以單次被害共計 41 位(占 28.9%)最高、被害 2 次共計 31 位(占 21.8%)次之,兩者總計占全體被害樣本 50.7%,亦即被害次數在 2 次以下者合計超過全體被害樣本之半數。在網路詐欺被害次數部分,平均數為 3.15、標準差為 2.295、最小值為 1、最大值為 12、峰度係數 1.252、偏態係數 1.257,整體呈現右偏之高狹分布。

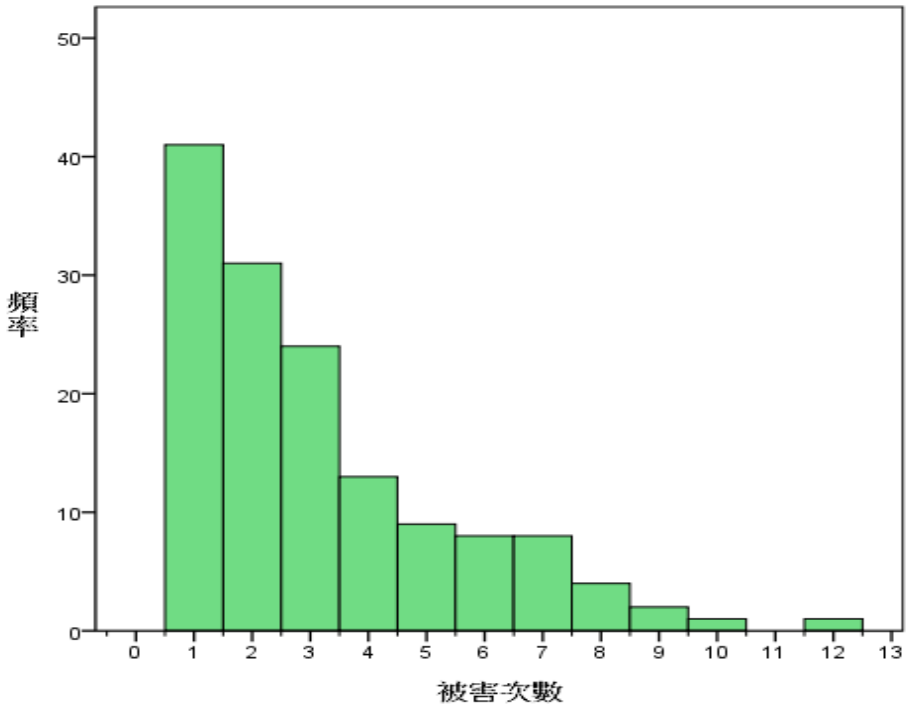

圖 4-5-1 網路詐欺被害次數分布圖

二、網路詐欺重複被害次數影響因素之 Poisson 迴歸分析

(一)網路詐欺重複被害次數 Poisson 迴歸模型配適度檢驗

在網路詐欺重複被害次數之分析部分,本研究係採用卜瓦松(Poisson)迴歸進行被害次數之分析。經資料離散性檢定結果,由下表 4-5-2 所示,從表中可以得知,網路詐欺重複被害次數之偏差值/自由度及皮爾森卡方值/自由度均小於 1,可得知本研究之離散計數型資料呈現低度離散之情況,故採用卜瓦松迴歸模型進行分析。

在模型之配適度檢定部分,下表 4-5-2 呈現有關本研究所建構之 Poisson 迴歸模型之各項配適度。在配適度部分,因模型配適度指標卡方值(χ^2)並未達統計上之顯著水準(χ^2=63.460 ; d.f.=74 ; p>.05),代表模型與資料之擬和度佳,此模型適用於預測被害次數。

在 Omnibus 檢定部分，因檢定卡方值(χ^2)達統計上之顯著水準(χ^2=93.115 ; d.f.=21 ; p<.001)，故本 Poisson 迴歸模型中至少有一迴歸係數不為零，亦即在本模型中至少有一變項適合預測依變項，換言之，本研究投入之自變項確實對於依變項具有預測力。

表 4-5-2 網路詐欺重複被害次數之卜瓦松(Poisson)迴歸模型配適度摘要

模型摘要	檢定值
Omnibus 檢定	
對數概似值/自由度/顯著性	**93.115***** ; d.f.=21
模型適合度檢定	
偏差值(Deviance) ; 自由度	63.419 ; d.f.=74
Pearson's 卡方值 ; 自由度	63.460 ; d.f.=74
偏差值/自由度	.857
卡方值/自由度	.857
AIC ; BIC 值	386.101 ; 456.710
Lagrange 檢定	參數<0 (P<.001)

註:***p<.001

(二)網路詐欺重複被害次數影響因素之 Poisson 迴歸分析

經前述網路詐欺被害之次數分配後可知,全體網路詐欺重複被害者為101位,其中，男性樣本計有 85 位、女性樣本計有 16 位。為避免樣本過少，而投入迴歸方程式之預測變項過多,導致自變項之預測效率低落,個別變項之迴歸係數未達顯著水準之情況產生,本研究在網路詐欺重複被害次數之迴歸建構中，僅就全體樣本進行迴歸分析。

下表 4-5-3 係以 Poission 迴歸對全體樣本進行分析，以了解網路詐欺重複被害次數之影響因素。首先，在個人基本特性方面，經迴歸分析之結果後，僅有性別達統計上之顯著水準。在性別部分，網路詐欺重複被害次數與性別呈正相關，男性相較女性有較高的網路詐欺重複被害次數(B=.415 ; Wald=27.933***)，且男性網路詐欺重複被害次數之發生率為女性重複被害次數發生率之 1.514 倍。在網路使用特性部分，各變項均未達統計上之顯著水準，顯示網路使用特性並未顯著預測網路詐欺重複被害次數。

其次，在網路生活型態方面，僅有網路風險休閒活動達統計上顯著水準，網路風險休閒活動與網路詐欺重複被害次數呈正相關，顯示從事較多網路風險休閒活動者，有較高網路詐欺重複被害次數(B=.094 ; Wald=5.496***)。

在被害情境與機會方面，物理監控及網路負面誘因均達統計上顯著水準，在物理監控部分，物理監控與網路詐欺重複被害次數呈負相關，顯示物理監控較低者，網路詐欺被害次數較高(B=-.277 ; Wald=40.890***)。在網路負面誘因部分，網路負面誘因與網路詐欺重複被害次數呈正相關，顯示接收較多網路負面誘因者，有較高的網路詐欺重複被害次數(B=.225 ; Wald=7.121**)。

最後，在低自我控制特性部分，僅有投機性達統計上之顯著水準，在投機性部分，投機性與網路詐欺重複被害次數呈正相關，顯示投機性較高者，有較高的網路詐欺重複被害次數(B=.222 ; Wald=17.382***)。

綜合上述分析後可得知，男性、從事較多網路風險休閒活動、物理監控程度較低、接收的網路負面誘因較高及有較高投機性程度者，具有較高的網路詐欺重複被害次數。在迴歸模型中解釋依變項之重要性係以 Wald 值作為判斷依據，故在解釋網路詐欺重複被害次數之重要性依序為物理監控、其次為性別，最後則為投機性。

(三)網路詐欺被害、重複被害次數影響因素之 Poisson 迴歸綜合分析

本研究對於網路詐欺被害樣本(N=142)及網路詐欺重複被害樣本(N=101)，分別進行 Poisson 迴歸分析。綜合兩個預測網路詐欺被害次數、重複被害次數之 Poisson 迴歸模型後可以發現，影響網路詐欺被害次數、重複被害次數之共通性預測因素包括:性別、網路風險休閒活動、物理監控及投機性等四個重要變項。

換言之，當網路使用者為男性、從事較高網路風險休閒活動、具有較低物理監控及較高衝動性特質者，其在網路詐欺之被害次數及重複被害次數皆越高。

表 4-5-3 網路詐欺重複被害次數之卜瓦松(Poisson)迴歸模型分析(N=101)

變　項	B	RSE[65]	Wald	IRR[66]
個人基本特性				
性別(男)	.415	.0785	**27.933*****	1.514
年齡	-.032	.0230	1.875	.969
職業(無業組)	.063	.0913	.473	1.065
收入	.007	.0462	.022	1.007
教育程度	-.012	.0431	.076	.988
網路使用特性				
每次上網時數				
中上網時數(3-7 小時)	.183	.1062	2.969	1.201
高上網時數(7 小時以上)	.164	.1045	2.474	1.179
每周上網次數			.	
中上網次數(7-9 次)	.119	.0794	2.233	1.126
高上網次數(10 次以上)	.118	.0717	2.708	1.125
平日上網時段			.	
夜間上網時段(16-24 時)	.068	.1193	.323	1.070
深夜上網時段(0-8 時)	.088	.1160	.573	1.092
假日上網時段				
夜間上網時段(16-24 時)	.173	.1439	1.447	1.189
深夜上網時段(0-8 時)	.138	.0674	4.186	1.148
網路生活型態				
網路休閒活動	-.080	.0478	2.788	.923
網路職業活動	-.036	.0415	1.730	.836
網路風險休閒活動	.094	.0402	**5.496*****	1.099
網路風險職業活動(Ln)[67]	.049	.0428	1.302	1.050
被害情境與機會				
社會監控	-.022	.0426	.279	.978
物理監控	-.277	.0434	**40.890*****	.758
網路負面誘因	.225	.0844	**7.121****	1.253
網路偏差動機(Sqrt)[68]	.118	.1773	.444	1.125
低自我控制特性				
衝動性	.034	.1511	.050	1.034
冒險性	.196	.1304	2.254	1.216
投機性	.222	.0533	**17.382*****	1.249
截距(Intercept)	.467	.6468	.521	1.595

註: **p<.01 ; ***p<.001

註:性別:對照組=女性、職業:對照組=就業組、每次上網時數:對照組=低上網時數(未滿 3 小時)
每周上網次數:對照組=低上網次數(未滿 7 次)、平(假)日上網時段:對照組=白天上網時段(8-16 時)

[65] RSE 代表穩健標準誤估計量(Robust standard errors)
[66] IRR 代表事件發生比率(Incident rate ratios)
[67] Ln 代表變項經自然對數轉換(Natural logarithm transformation)
[68] Sqrt 代表變項經平方根轉換(Square root transformation)

第六節 綜合分析

本研究依據研究架構進行分析，分析之核心除著重於網路詐欺被害之性別差異外，亦深入探究網路詐欺重複被害之影響因素，經前述分析後，發現網路使用者之個人基本特性、網路生活型態、被害情境與機會及低自我控制特性等面向，對於網路詐欺被害及網路詐欺重複被害影響因素具有顯著解釋力及預測力，故本節將對於前述幾節之差異性分析、相關分析、邏輯斯迴歸分析及卜瓦松迴歸分析等結果，綜合歸納整理如下:

一、差異性分析結果

(一)不同性別在網路使用特性及各態度面向具有顯著差異

有關不同性別網路使用者在各因素面向之差異分析摘要如下表 4-6-1 所示。首先，不同性別之假日上網時段及經常上網原因具有顯著差異，其中，在假日上網時段部分，女性在假日白天時段上網者顯著高於男性，但男性在假日深夜時段上網者則高於女性。不同性別在網路使用特性部分，不同性別經常上網原因具有顯著差異，其中，不同性別在經常上網原因部分，男性經常上網原因係為抒發情緒之比例，顯著高於女性。

其次，不同性別在網路生活型態之各因素面向均有顯著差異。從表中可以得知，在從事非風險性之一般網路休閒與網路職業活動部分，女性網路使用者均顯著高於男性，但在從事具風險性之網路風險休閒與職業活動部分，男性網路使用者則顯著高於女性，顯示男性所從事之網路風險休閒與職業活動皆顯著高於女性。

再者，在被害情境與機會部分，不同性別網路使用者在社會監控、網路負面誘因及網路偏差動機等變項均有顯著差異。在社會監控部分，女性網路使用者顯著高於男性，但在網路負面誘因及網路偏差動機部分，男性網路使用者則顯著高於女性，顯示在網路使用過程中，女性具有較高社會監控，而男性則具有較高網路負面誘因及網路偏差動機。在低自我控制特性部分，不同性別網路使用者僅在冒險性程度上存在顯著差異，其中，男性在網路使用的過程中，其冒險性程度顯著高於女性。

最後，在網路詐欺被害部分，不同性別網路使用者在是否被害、被害類型、是否與加害者互動及與加害者互動方式皆有顯著差異。是否被害部分，男性網路使用者其網路

詐欺被害機率顯著高於女性。在被害類型部分，各組雖然皆以遭受網路購物詐欺被害之比例最高，但被害者在各類型的網路詐欺被害比例，顯著高於未被害者。在是否與加害者進行互動部分，男性網路使用者與加害者互動之比例顯著高於女性。在與加害者互動方式部分，各組則以使用網路社群網站與加害人接觸比例最高，顯著高於其他接觸管道。綜上所述，不同性別之網路使用者在網路使用特性、網路生活型態、被害情境與機會、低自我控制及網路詐欺被害面向有部分顯著差異。

表 4-6-1 不同性別網路使用者在各因素面向之差異分析摘要表

主構面名稱	次構面名稱	男性	女性
		（顯著性/差異性）	（顯著性/差異性）
網路使用特性	每次上網時數	N.S.	
	每周上網次數	N.S.	
	平日上網時段	N.S.	
	假日上網時段	男性深夜上網時段顯著高於女性	
	接觸網路時間	N.S.	
	經常上網地點	N.S.	
	經常上網原因	男性以網路抒發情緒比例顯著高於女性	
網路生活型態	網路休閒活動	女>男	
	網路職業活動	女>男	
	網路風險休閒活動	男>女	
	網路風險職業活動	男>女	
被害情境與機會	社會監控	女>男	
	物理監控	N.S.	
	網路負面誘因	男>女	
	網路偏差動機	男>女	
低自我控制	衝動性	N.S.	
	冒險性	男>女	
	投機性	N.S.	
網路詐欺被害	是否被害	男性>女性	
	被害類型	各組以網路詐欺被害比例最高	
	交易方式	N.S.	
	是否與加害者互動	男性>女性	
	與加害者互動方式	各組以網路社群網站比例最高	
	是否報案	N.S.	
	是否再次從事網路活動	N.S.	

註:N.S.代表未達統計上之顯著水準(Non-Significant)

(二)網路詐欺被害與否在個人基本特性、網路使用特性及各態度面向具有顯著差異

有關網路詐欺被害與否在各因素面向之差異分析摘要如下表 4-6-2 所示。首先，網路詐欺被害在個人基本特性部分具有部分顯著差異。在年齡部分，網路詐欺被害者以 19-39 歲占最高比例，顯著高於其他被害年齡層，而未被害者則以 40-59 歲占最高比例，顯著高於其他年齡層。在職業部分，網路詐欺被害者與未被害者皆以學生占最高比例。在收入部分，網路詐欺被害者以收入介於 1 至 3 萬占最高比例，顯著高於其他收入組別，而未被害者收入則介於 3 至 6 萬占最高比例，顯著高於其他收入組別。在教育程度部分，各組則皆以大學畢(肄)業占最高比例，顯著高於其他教育程度組別。

其次，網路詐欺被害在網路使用特性部分，網路詐欺被害在每次上網時數、每周上網次數、平日上網時段、假日上網時段、經常上網地點及經常上網原因具有顯著差異。在網路詐欺被害之每次上網時數，網路詐欺被害者每周上網 3 至 7 小時之比例，顯著高於未被害者。在每周上網次數部分，各組皆以每周上網 10 次以上占最高比例，顯著高於其他組別。在平日及假日上網時段部分，未被害者在白天上網之比例顯著高於被害者，而被害者在深夜上網之比例均顯著高於未被害者。在經常上網地點部分，被害者在不同地點上網之比例，顯著高於未被害者，而在經常上網原因部分，各組雖均以搜尋資料占最高比例，但被害者以網路從事休閒娛樂活動之比例則顯著高於未被害者。

再者，在網路生活型態部分，網路詐欺被害與否在網路休閒活動、網路職業活動及網路風險職業活動均有顯著差異。在網路休閒活動與職業活動部分，網路詐欺未被害者在從事非風險性之網路休閒及職業活動部分，均顯著高於網路詐欺被害者。在網路風險職業活動部分，網路詐欺被害者所從事具風險性之網路職業活動則顯著高於未被害者，顯示在網路使用的過程中，從事較高非風險性之網路休閒或職業活動，則網路詐欺被害之可能性較低。

在被害情境與機會部分，網路詐欺被害與否在社會監控、物理監控、網路負面誘因及網路偏差動機均有顯著差異。在社會監控及物理監控部分，網路詐欺未被害者均顯著高於被害者，而在網路負面誘因及偏差動機部分，網路詐欺被害者則顯著高於未被害者，顯示網路詐欺未被害者有較高的物理監控及社會監控，網路詐欺被害者則有較高的網路

負面誘因及偏差動機。

最後，在低自我控制部分，網路詐欺被害與否在衝動性、冒險性及投機性程度，均有顯著差異。在衝動性、冒險性及投機性部分，網路詐欺被害者均顯著高於未被害者，顯示在網路使用的過程中，網路詐欺被害者具有較高的衝動性、冒險性及投機性程度。綜上所述，網路詐欺被害與否在個人基本特性、網路使用特性及各因素面向上具有部分顯著差異。

表 4-6-2 網路詐欺被害與否在各因素面向之差異分析摘要表

主構面名稱	次構面名稱	網路詐欺被害者（顯著性/差異性）	網路詐欺未被害者（顯著性/差異性）
個人基本特性	年齡	以 19-39 歲比例最高	以 40-59 歲比例最高
	職業	各組以學生比例最高	
	收入	以 1 至 3 萬比例最高	以 3 至 6 萬比例最高
	教育程度	各組以大學畢(肄)業比例最高	
	婚姻	N.S.	
網路使用特性	每次上網時數	每周上網 3-7 小時比例，被害者顯著高於未被害者	
	每周上網次數	每周上網 10 次以上比例，被害者顯著高於未被害者	
	平日上網時段	被害者深夜時段上網比例顯著高於未被害者	
	假日上網時段	被害者深夜時段上網比例顯著高於未被害者	
	接觸網路時間	N.S.	
	經常上網地點	被害者在各地點上網比例顯著高於未被害者	
	經常上網原因	被害者以網路從事休閒娛樂比例高於未被害者	
網路生活型態	網路休閒活動	未被害者>被害者	
	網路職業活動	未被害者>被害者	
	網路風險休閒活動	N.S.	
	網路風險職業活動	被害者>未被害者	
被害情境與機會	社會監控	未被害者>被害者	
	物理監控	未被害者>被害者	
	網路負面誘因	被害者>未被害者	
	網路偏差動機	被害者>未被害者	
低自我控制	衝動性	被害者>未被害者	
	冒險性	被害者>未被害者	
	投機性	被害者>未被害者	

註:N.S.代表未達統計上之顯著水準(Non-Significant)

(三)性別、網路詐欺被害與否在網路使用特性及各態度面向具有顯著差異

有鑑於前述分析係以「性別」及「網路詐欺被害與否」，作為各分組差異分析依據，此部分則以性別做為控制變項，更進一步對於不同性別網路詐欺被害者在網路使用特性及各態度面向上之差異進行交叉分析。

有關不同性別、網路詐欺被害與否在各因素面向之差異分析摘要如下表 4-6-3 所示。首先，在網路使用特性部分，各分組在每次上網次數、每周上網次數、平日上網時段、假日上網時段、經常上網地點及經常上網原因部分具有顯著差異。在每周上網次數部分，男性各組均以每周上網 3-7 小時占最高比例，女性亦以每周上網 3-7 小時占最高比例。在每周上網次數部分，各組均以每周上網 10 次以上占最高比例，顯著高於其他組別。在平日及假日上網時段部分，各組皆以在 16-24 時上網占最高比例，顯著高於其他組別。在經常上網地點部分，各組均以在家中(租屋處)上網占最高比例，顯著高於其他組別。在經常上網原因部分，男性經常上網原因以搜尋資料比例最高、女性則以休閒娛樂比例最高，顯著高於其他組別。

其次，在網路生活型態部分，各組在網路休閒活動、網路職業活動及網路風險職業活動具有顯著差異。在網路休閒活動部分，男性未被害組網路休閒活動顯著高於被害組。在網路職業活動部分，無論是男性或女性，未被害組之網路職業活動均顯著高於被害組。在網路風險職業活動部分，男性及女性各分組之被害組均顯著高於未被害組。綜上分析發現，無論是男性或女性，在非風險性網路休閒及職業活動上，未被害組均高於被害組，但在風險性網路職業活動上，被害組則顯著高於未被害組。

再者，在被害情境與機會部分，各組在社會監控、物理監控及網路偏差動機等變項具有部分顯著差異。在社會監控部分，男性未被害組之社會監控程度顯著高於被害組。在物理監控部分，在男性及女性各分組中，未被害組之物理監控程度均顯著高於被害組。在網路偏差動機部分，男性及女性被害各分組之網路偏差動機亦皆顯著高於未被害組，綜合上述分析後發現，無論是男性或女性，在社會監控及物理監控程度上，未被害組均高於被害組，但在網路偏差動機程度上，被害組則顯著高於未被害組。

最後,在低自我控制特性部分,各組在衝動性、冒險性及投機性變項具有顯著差異。在衝動性部分，男性被害組之衝動性程度顯著高於未被害組，而在冒險性部分，男性及女性被害組之冒險性程度亦均顯著高於未被害組。在投機性部分，男性及女性被害組之投機性程度亦顯著高於未被害組,顯示無論是男性或女性,在低自我控制三個特性部分,被害組均顯著大於未被害組，亦即，被害組相較於未被害組具有較低的自我控制程度。綜上所述，將性別做為控制變項，對於網路詐欺被害與否進行交叉分析後發現，性別及網路詐欺被害與否在網路使用特性、網路生活型態、被害情境與機會及低自我控制特性部分均存在部分顯著差異。

表 4-6-3 性別、網路詐欺被害與否在各因素面向之差異分析摘要表

主構面名稱	次構面名稱	性別、是否被害分組			
		男性被害	男性未被害	女性被害	女性未被害
		（顯著性/差異性）		（顯著性/差異性）	
網路使用特性	每次上網時數	各組以 3-7 小時比例最高			
	每周上網次數	各組以 10 次以上比例最高			
	平日上網時段	各組以 16-24 時比例最高			
	假日上網時段	各組以 16-24 時比例最高			
	接觸網路時間	N.S.			
	經常上網地點	各組以在家中(租屋處)上網比例最高			
	經常上網原因	以搜尋資料比例最高		以休閒娛樂比例最高	
網路生活型態	網路休閒活動	男性未被害>男性被害		N.S.	
	網路職業活動	男性未被害>男性被害		女性未被害>女性被害	
	網路風險休閒活動	N.S.		N.S.	
	網路風險職業活動	男性被害>男性未被害		女性被害>女性未被害	
被害情境與機會	社會監控	男性未被害>男性被害		N.S.	
	物理監控	男性未被害>男性被害		女性未被害>女性被害	
	網路負面誘因	N.S.		N.S.	
	網路偏差動機	男性被害>男性未被害		女性被害>女性未被害	
低自我控制	衝動性	男性被害>男性未被害		N.S.	
	冒險性	男性被害>男性未被害		女性被害>女性未被害	
	投機性	男性被害>男性未被害		女性被害>女性未被害	

註:N.S.代表未達統計上之顯著水準(Non-Significant)

二、相關分析結果

本研究旨在探究不同性別網路詐欺被害影響因素，經皮爾森積差相關分析後發現，個人基本特性與網路詐欺被害與否、網路詐欺被害次數、網路使用特性及各因素面項等具有部分顯著相關，故以下茲對於相關分析所得之結果，綜合歸納如下表 4-6-4 所示:

(一)個人基本特性在網路詐欺被害與否、被害次數與各態度面向具有顯著相關

在個人特性與網路詐欺被害部分，從表中可知，當網路使用者為男性、無職業者、年齡較低者、收入較高者、教育程度較低者，其網路詐欺被害機率越高。

在個人基本特性與各態度面向相關分析部分，從表中可知，在性別與網路生活型態部分，女性從事網路休閒活動、網路職業活動程度較高，而男性從事網路風險休閒活動及網路風險職業活動之程度較高。在被害情境與機會部分，女性在網路使用的過程中，具有較高的社會監控程度，而男性則接收較高的網路負面誘因並具有較高網路偏差動機。在低自我控制部分，男性在網路使用的過程中，具有較高的冒險性程度。

在年齡與網路生活型態部分，年齡較高之網路使用者，其網路休閒活動程度較高。在被害情境與機會部分，年齡較低之網路使用者其接收到的網路負面誘因及個人在網路使用過程中的偏差動機程度較高。在低自我控制部分，年齡較低者其衝動性程度較高。在職業與網路生活型態部分，就業者所從事之網路休閒活動及網路職業活動程度較高。在被害情境與機會部分，就業者之物理監控程度較未就業者高。在低自我控制部分，未就業者其衝動性、冒險性及投機性程度均較高於就業者。

在收入與網路生活型態部分，未有顯著相關。在被害情境與機會部分，收入較低者，其社會監控及物理監控程度較低。在低自我控制部分，收入較低者其衝動性程度較高。在教育程度與網路生活型態部分，教育程度較高者，其從事網路休閒活動與職業活動之程度較高、其從事之網路風險休閒活動程度較低。在教育程度與被害情境與機會部分，教育程度較高者，其物理監控程度較高，但其網路偏差程度較低。在低自我控制部分，教育程度較高者其衝動性及冒險性程度較低。在婚姻狀況與網路生活型態部分，未婚者從事網路風險休閒活動程度較高。在被害情境與機會部分，未婚者其社會監控程度較低。在低自我控制部分，未婚者其衝動性及冒險性程度較高。

(二)網路使用特性與網路詐欺被害與否與各態度面向具有顯著相關

在網路使用特性與網路詐欺被害部分，每次上網時數較高、每周上網次數較高者，其網路詐欺被害機率較高。在網路使用特性與網路生活型態部分，每次上網時數較高者，其網路休閒活動、網路職業活動及網路風險休閒活動程度皆較高。在低自我控制部分，每周上網時數越高者，其衝動性程度越高。

在每周上網次數與網路生活型態部分，每周上網次數越高者，其網路休閒與職業之活動程度較高。在被害情境與機會部分，每周上網次數越高者，其網路負面誘因及偏差動機程度越高。在低自我控制部分，每周上網次數越高者，其衝動性及冒險性程度越高。

在接觸網路時間與網路生活型態部分，接觸網路時間越早者，其網路休閒活動及網路職業活動程度較高，但其網路風險職業活動程度較低。在被害情境與機會部分，接觸網路時間越早者，其物理監控程度越高、網路偏差動機程度越低。在低自我控制部分，接觸網路時間與低自我控制特性則未有顯著相關。

(三)網路詐欺被害與否與各態度面向具有顯著相關

網路詐欺被害與各因素面向具有顯著相關，網路詐欺被害與網路生活型態部分，在網路使用的過程中，從事較少非風險性之網路休閒活動及網路職業活動、從事較高網路風險職業活動，其網路詐欺被害機率較高。在被害情境與機會部分，在網路使用過程中，社會監控及物理監控程度較低者、所接收到的網路負面誘因及個人偏差動機程度較高者，其網路詐欺被害機率較高。在網路詐欺被害與低自我控制部分，在網路使用的過程中，個人的衝動性、冒險性及投機性程度較高者，其網路詐欺被害之機率較高。

(四)網路詐欺被害次數與各態度面向具有顯著相關

在網路詐欺被害次數與網路生活型態部分，從事較少網路休閒活動、網路職業活動，並從事較多網路風險休閒活動及網路風險職業活動者，其網路詐欺被害之次數較高。在網路詐欺被害次數與被害情境與機會方面，具有較低社會監控及物理監控程度，並具有較高網路負面誘因及網路偏差動機者，其網路詐欺被害之次數較高。在網路詐欺被害次數與低自我控制特性部分，具有較高冒險性及衝動性程度之低自我控制者，其網路詐欺被害之次數較高。

(五)各態度面向間具有顯著相關

在網路休閒活動與各態度面向部分，網路休閒活動與網路職業活動、社會監控、物理監控呈顯著正相關，但與網路風險職業活動、網路負面誘因、網路偏差動機、冒險性及投機性均呈顯著負相關，顯示當網路使用者從事較多的網路休閒活動時，其網路職業活動、社會監控及物理監控程度均較高，但其網路風險職業活動、網路負面誘因、網路偏差動機、冒險性及投機性程度則較低。

在網路職業活動與各態度面向部分，網路職業活動與社會監控及物理監控均呈顯著正相關，但與網路風險職業活動、網路偏差動機、衝動性、冒險性及投機性呈負相關。顯示當網路使用者從事較多的網路職業活動時，其社會監控及物理監控程度均較高，但其網路風險職業活動、網路偏差動機、衝動性、冒險性及投機性程度則較低。

在網路風險休閒活動與各態度面向部分，網路風險休閒活動與網路風險職業活動、網路負面誘因、網路偏差動機、衝動性、冒險性及投機性呈顯著正相關，但與社會監控及物理監控則呈顯著負相關，顯示當網路使用者從事較多的網路風險休閒活動時，其網路風險職業活動、網路負面誘因、網路偏差動機、衝動性、冒險性及投機性程度均越高，而個人的社會監控與物理監控程度則相關較低。

在網路風險職業活動與各態度面向部分，網路風險職業活動與網路負面誘因、網路偏差動機、衝動性、冒險性及投機性呈顯著正相關，但與社會監控及物理監控則呈顯著負相關，顯示當網路使用者從事較多的網路風險職業活動時，其網路負面誘因、網路偏差動機、衝動性、冒險性及投機性程度越高，但個人的社會監控與物理監控程度則越低。

在社會監控與各態度面向部分，社會監控與物理監控呈顯著正相關，亦即當網路使用者有較高的社會監控時，相對也有較高的物理監控程度。在物理監控與各態度面向部分，物理監控與網路偏差動機、衝動性及投機性呈顯著負相關，顯示當網路使用者有較高的物理監控程度時，其網路偏差動機、衝動性及投機性程度相對越低。

在衝動性與各態度面向部分，衝動性與冒險性及投機性呈顯著正相關，亦即當網路使用者有較高的衝動性程度，其冒險性及投機性程度亦越高，而冒險性亦與投機性程度呈顯著正相關，顯示個人的冒險性程度越高，其投機性程度亦越高。

表 4-6-4 個人特性、網路生活型態與各因素構面之相關分析摘要表

變項	是否被害	被害次數	網路休閒活動	網路職業活動	網路風險休閒活動	網路風險職業活動	社會監控	物理監控	網路負面誘因	網路偏差動機	衝動性	冒險性	投機性
性別(1=女性)	-***	-***	+**	+***	-***	-*	+**		-***	-***		-**	
年齡	-***	-***	+**						-**	-*	-*		
職業(1=就業)	-***	-***	+**	+*				+***			-**	-*	-***
收入	+***						+***	+***			-*		
教育程度	-***	-***	+***	+**	-**			+**		-**	-*	-*	-*
婚姻狀況(1=已婚)					-***		-**				-**	-*	
每次上網時數	+***		+***	+*	+***						+**		
每周上網次數	+***		+***	+***		+***			+**	+***	+*	+**	
接觸網路時間		+*	+***	+***		-*		+***		-*			
被害與否(1=被害)			-***	-***		+**	-***	-***	+*	+**	+***	+***	+***
網路詐欺被害次數			-***	-***	+***	+***	-***	-***	+***	+***		+***	+*
網路休閒活動				+***		-***	+**	+***	-**	-**		-**	-**
網路職業活動						-***	+***	+***		-***	-**	-**	-***
網路風險休閒活動						+***	-**	-**	+***	+***	+*	+***	+***
網路風險職業活動							-*	-***	+***	+***	+***	+***	+***
社會監控								+***					
物理監控										-***	-***		-***
網路負面誘因										+***		+***	+**
網路偏差動機											+***	+***	+***
衝動性												+***	+***
冒險性													+***
投機性													

註:*p<.05 ; **p<.01 ; ***p<.001

三、多變量分析結果

本研究在多變量分析(Multivariate analysis)部分，共包括兩個部分，第一部分係以二元 logistic 迴歸對於本研究之二分類間斷依變項(網路詐欺被害與否)進行分析，藉以了解影響網路詐欺被害重要因素、不同性別網路詐欺被害影響因素。第二部分則分別就網路詐欺被害次數及重複被害次數，進行 Poisson 迴歸分析，以了解網路詐欺被害次數及重複被害次數之重要影響因素，相關分析內容茲分述如下:

(一)二元 logistic 迴歸分析

本研究在二元 logistic 迴歸分析部分，先對於全體調查樣本進行分析，以了解全體網路使用者之網路詐欺被害影響因素,其次,將樣本劃分為男性及女性網路使用者兩組,並分別進行二元logistic迴歸分析,藉以了解及比較不同性別網路詐欺被害之影響因素，相關分析內容茲詳細分述如下:

1.全體調查樣本網路詐欺被害影響因素

有關全體調查樣本網路詐欺被害影響因素二元 logistic 迴歸分析摘要結果如下表 4-6-5 所示。在全體調查樣本中(N=870)，經迴歸分析後發現，個人基本特性、網路使用特性、網路生活型態、被害情境與機會及低自我控制之部分變項對於網路詐欺被害具有顯著影響力及解釋力。

經迴歸分析後可知，當網路使用者為男性、年齡越低者、無職業者、收入較高者、教育程度較低者、每次上網 3-7 小時(中上網時數)、每次上網 7 小時以上(高上網時數)、每周上網 7-9 次(高上網次數)、在平日夜間時段(16-24 時)上網、平日深夜時段(0-8 時)上網、假日深夜時段(0-8 時)上網,以及在網路使用過程中從事較多網路風險職業活動、接收到較高網路負面誘因、有較高衝動性、冒險性及投機性,且其社會監控程度較低者，其網路詐欺被害風險較高。

2.男性網路使用者之網路詐欺被害影響因素

在男性網路使用者之網路詐欺被害影響因素二元 logistic 迴歸分析後，研究發現，在男性樣本中(N=455)，經迴歸分析後發現，個人基本特性、網路使用特性、網路生活型態、被害情境與機會及低自我控制變項對於網路詐欺被害有顯著影響力及解釋力。

當男性網路使用者年齡越低、無職業者、每次上網 3-7 小時(中上網時數)、每次上網 7 小時以上(高上網時數)、每周上網 7-9 次(高上網次數)、在平日夜間時段(16-24 時)上網、平日深夜時段(0-8 時)上網、假日深夜時段(0-8 時)上網者，在網路使用過程中從事較少網路休閒活動、網路職業活動、社會監控程度較低，且從事網路風險職業活動、接收較高網路負面誘因、有較高衝動性及冒險性者，其網路詐欺被害風險較高。

3.女性網路使用者之網路詐欺被害影響因素

在女性網路使用者之網路詐欺被害影響因素二元 logistic 迴歸分析後，研究發現，在女性樣本中(N=415)，經迴歸分析後發現，個人基本特性、網路使用特性、網路生活型態、被害情境與機會及低自我控制變項對於網路詐欺被害有顯著影響力及解釋力。

當女性網路使用者為無職業者、收入較低者、每次上網 3-7 小時(中上網時數)、在平日深夜時段(0-8 時)上網、假日深夜時段(0-8 時)上網者，以及網路使用過程中從事較少網路職業活動，且其從事之網路風險職業活動、接收較高網路負面誘因、具有較高衝動性及投機性者，其網路詐欺被害風險較高。

在綜合比較不同性別網路使用者之迴歸分析後，可知影響不同性別網路詐欺被害之重要共通因素中包括，職業、每次上網 3-7 小時(中上網時數)、平日深夜時段(0-8 時)上網、假日深夜時段(0-8 時)上網、網路職業活動、網路風險職業活動、網路負面誘因及衝動性，其中，無職業者、每次上網 3-7 小時、平日深夜時段(0-8 時)上網、假日深夜時段(0-8 時)上網，從事較低網路職業活動、從事較多網路風險職業活動且具有較高網路負面誘因及衝動性者，無論男性或女性，其成為網路詐欺被害者之可能性較高。

4.影響網路詐欺被害之共通性因素

本研究就全體樣本、男性及女性網路使用者分別建構三組二元 logistic 迴歸模型，經綜合分析後發現，上述各組中，共同影響網路詐欺被害之共通性解釋因素分別為職業、每次上網 3-7 小時(中上網時數)、假日深夜時段(0-8 時)上網、網路風險職業活動、網路負面誘因及衝動性，亦即在各分組中，無業者、每次上網 3-7 小時(中上網時數)、平日深夜時段(0-8 時)上網、假日深夜時段(0-8 時)上網及從事較多網路風險職業活動，並具有較多網路負面誘因及衝動性者為各組之網路詐欺共通被害因素。

表 4-6-5 網路詐欺被害影響因素之二元 logistic 迴歸分析摘要表

依變項 / 自變項	網路詐欺被害分組		
	全體樣本(N=870)	男性(N=455)	女性(N=415)
個人基本特性			
性別(男)	+*		
年齡	-**	-**	
職業(無業組)	+***	+**	+**
收入	+***		+***
教育程度	-*		
網路使用特性			
每次上網時數			
中上網時數(3-7 小時)	+**	+**	+**
高上網時數(7 小時以上)	+**	+*	
每周上網次數			
中上網次數(7-9 次)	+**	+**	
高上網次數(10 次以上)			
平日上網時段			
夜間上網時段(16-24 時)	+**	+*	
深夜上網時段(0-8 時)	+*	+*	+*
假日上網時段			
夜間上網時段(16-24 時)			
深夜上網時段(0-8 時)	+***	+***	+*

網路生活型態			
網路休閒活動		-*	-*
網路職業活動		-**	
網路風險休閒活動			
網路風險職業活動	+**	+*	+**
被害情境與機會			
社會監控	-*	-**	
物理監控			
網路負面誘因	+**	+*	+**
網路偏差動機			
低自我控制特性			
衝動性	+***	+**	+*
冒險性	+**	+**	
投機性	+**		+*
模型摘要			
-2 log likehood(對數概似值)	495.817	257.105	186.418
模型卡方值(χ^2)及顯著性	**271.100*****	**206.457*****	**110.882*****
H-L 檢定統計量及顯著性	χ^2=3.744 ; p=.879	χ^2=9.051 ; p=.338	χ^2=5.046 ; p=.753
Pseudo R^2			
Cox & Snell R^2	.268	.365	.234
Nagelkerke R^2	.457	.571	.458
分類正確率(前;後)	83.7% ; 89.5%	79.3% ; 88.1%	88.4% ; 92.5%

註:*p<.05 ; **p<.01 ; ***p<.001

註:性別:對照組=女性、職業:對照組=就業組、每次上網時數:對照組=低上網時數(未滿 3 小時)、每周上網次數:對照組=低上網次數(未滿 7 次)、平(假)日上網時段:對照組=白天上網時段(8-16 時)

(二) Poisson 迴歸分析

本研究在 Poisson 迴歸分析部分，共分為兩個部分，第一部分就網路詐欺被害次數進行分析，以了解影響網路詐欺被害次數之因子，第二部分則依據網路詐欺被害次數，將全體樣本分為非重複被害(被害次數1次以下)及重複被害(被害次數2次以上)兩組，並對於重複被害者進行分析，以了解網路詐欺重複被害次數之影響因素，相關內容如下:

1.網路詐欺被害次數影響因素

在網路詐欺被害次數之影響因素部分，經 Poisson 迴歸分析後如下表 4-6-6 所示。由下表可知，在網路詐欺被害者中(N=142)，個人基本特性、網路生活型態、被害情境與機會及低自我控制特性均對於網路詐欺被害次數具有顯著影響力，但網路使用特性則未具有顯著影響力存在。

其中，當網路使用者為男性、年齡較低者、在網路使用過程中從事較少網路休閒活動、具有較低社會監控及物理監控程度，且從事較多網路風險休閒活動、接收較多網路負面誘因、有較高冒險性及投機性之低自我控制者，其網路詐欺被害次數較高。

2.網路詐欺重複被害影響次數分析

在網路詐欺重複被害次數之影響因素部分，經Poisson迴歸分析後如下表4-6-6所示。由下表可知，在網路詐欺重複被害者中(N=101)，個人基本特性、網路生活型態、被害情境與機會及低自我控制特性對於網路詐欺被害次數具有部分顯著影響力，但網路使用特性變項則未具有顯著影響力存在。

其中，當網路使用者為男性、在網路使用過程中從事較多網路風險休閒活動、接收較多網路負面誘因、並具有較高投機性之低自我控制者，同時缺乏有效之物理監控者，其網路詐欺重複被害次數較高。

3.性別、網路風險休閒活動、物理監控、網路負面誘因及投機性，係網路詐欺被害次數與重複被害次數之重要預測因子

綜合上述迴歸分析後，影響網路詐欺被害次數及重複被害次數之重要共通性因素，包括性別、網路風險休閒活動、物理監控、網路負面誘因及投機性。

表 4-6-6 網路詐欺被害次數之 Poisson 迴歸分析摘要表

依變項 / 自變項	網路詐欺被害次數 全體樣本(N=142)	網路詐欺重複被害次數 全體樣本(N=101)
個人基本特性		
性別(男)	+***	+***
年齡	-*	
職業(就業)		
收入		
教育程度		
網路使用特性		
每次上網時數		
中上網時數(3-7 小時)		
高上網時數(7 小時以上)		
每周上網次數		
中上網次數(7-9 次)		
高上網次數(10 次以上)		
平日上網時段		
夜間上網時段(16-24 時)		
深夜上網時段(0-8 時)		
假日上網時段		
夜間上網時段(16-24 時)		
深夜上網時段(0-8 時)		
網路生活型態		
網路休閒活動	-**	
網路職業活動		
網路風險休閒活動	+**	+***
網路風險職業活動		
被害情境與機會		
社會監控	-**	
物理監控	-***	-***
網路負面誘因	+**	+**
網路偏差動機		
低自我控制特性		
衝動性		
冒險性	+**	
投機性	+**	+***

註: *p<.05 ; **p<.01 ; ***p<.001

註:性別:對照組=女性、職業:對照組=無職業者、每次上網時數:對照組=低上網時數(未滿 3 小時)
每周上網次數:對照組=低上網次數(未滿 7 次)、平(假)日上網時段:對照組=白天上網時段(8-16 時)

四、網路詐欺被害影響因素與相關理論驗證

(一)網路詐欺被害影響因素之分析結果與理論驗證

有關本研究網路詐欺被害影響因素之各組分析結果如下表 4-6-7 所示,由表中可知,在全體樣本、男性及女性網路使用者中，以職業(無業)、每次上網 3-7 小時、平日深夜時段上網(0-8 時)、假日深夜時段上網(0-8 時)、網路風險職業活動、網路負面誘因及衝動性為網路詐欺被害之共同影響因素，而在此上述變項中，均係依據犯罪學相關理論建構而成,故驗證了生活型態理論、日常活動理論、網路日常活動理論及自我控制理論。

由此可知,網路詐欺各分組被害者之共同特徵為職業為無業者、每周上網3-7小時、平日深夜時段上網(0-8 時)、假日深夜時段上網(0-8 時)、從事較多網路風險職業活動、且在網路使用過程中具有較高的網路負面誘因、衝動性。

表 4-6-7 網路詐欺被害影響因素之分析結果與理論驗證

	網路詐欺被害影響因素		
	全體樣本(N=870)	男性(N=455)	女性(N=415)
個別影響因素	性別、年齡、職業 收入、教育程度 每次上網時數 每周上網次數 平日上網時段 假日上網時段 網路風險職業活動 社會監控 網路負面誘因 衝動性、冒險性 投機性	年齡、職業 每次上網時數 每周上網次數 平日上網時段 假日上網時段 網路休閒活動 網路職業活動 網路風險職業活動 網路負面誘因 衝動性、冒險性	職業、收入 每次上網時數 平日上網時段 假日上網時段 網路休閒活動 網路風險職業活動 網路負面誘因 衝動性、投機性
共同影響因素	職業(無業)、每次上網 3-7 小時(中上網時數) 平日深夜時段上網(0-8時)、假日深夜時段上網(0-8時) 網路風險職業活動、網路負面誘因、衝動性		
理論驗證	生活型態理論 日常活動理論 網路日常活動理論 自我控制理論	生活型態理論 日常活動理論 網路日常活動理論 自我控制理論	生活型態理論 日常活動理論 網路日常活動理論 自我控制理論

(二)網路詐欺重複被害影響因素之分析結果與理論驗證

有關本研究網路詐欺被害次數及重複被害次數影響因素分析結果如下表 4-6-8 所示，由表中可知，在全體網路使用者中，以性別(男性)、年齡、職業(無業)、每周上網 3-7 小時、假日深夜時段上網(0-8 時)、網路職業活動、網路風險職業活動、網路負面誘因衝動性及投機性為網路詐欺被害次數之影響因素。

在網路詐欺重複被害次數之影響因素部分，則包括性別、網路風險休閒活動、物理監控、網路負面誘因及投機性，在兩者之共同影響因素部分，則包括性別(男性)、網路負面誘因、投機性等三個因素。由此可知，網路詐欺被害次數及重複被害次數最重要之預測因素為男性、在網路使用過程中具有較高網路負面誘因及偏差動機者。

在理論之驗證部分，網路詐欺被害次數影響因素驗證生活型態理論、日常活動理論網路日常活動理論、自我控制理論等四個理論，而網路詐欺重複被害次數影響因素則驗證網路日常活動理論及自我控制理論。

表 4-6-8 網路詐欺被害次數影響因素之分析結果與理論驗證

	網路詐欺被害次數影響因素	網路詐欺重複被害次數影響因素
	網路詐欺被害者(N=142)	網路詐欺重複被害者(N=101)
個別影響因素	性別、年齡、職業 每次上網時數 每周上網次數 假日上網時段 網路職業活動 網路風險職業活動 社會監控 網路負面誘因 衝動性 投機性	性別 網路風險休閒活動 物理監控 網路負面誘因 投機性
共同影響因素	性別(男性)、網路負面誘因、投機性	
理論驗證	生活型態理論、日常活動理論 網路日常活動理論、自我控制理論	網路日常活動理論 自我控制理論

五、研究假設之驗證分析

本研究根據研究架構，於第三章第一節提出共七點之研究假設，經本章各節之分析結果後，茲將研究分析結果與研究假設逐一進行驗證，相關驗證結果如下表 4-6-9 所示。

有關本研究假設一、二，經差異分析後，部分驗證本研究之假設，即男性及女性在「低自我控制」、「被害情境與機會」及「網路詐欺犯罪被害」等面向有顯著差異存在。

有關本研究假設三，經相關分析後，部分驗證本研究之假設，「網路生活型態」、「被害情境與機會」、「低自我控制特性」與「網路詐欺犯罪被害」有顯著相關性存在。

有關本研究假設四、五，經由二元 logistic 迴歸分析後，部分驗證本研究之假設，研究發現「個人基本特性」、「網路生活型態」、「被害情境與機會」、「低自我控制特性」，對於「網路詐欺被害」有顯著解釋力，而不同性別之「低自我控制特性」、「網路生活型態」、「被害情境與機會」對於不同性別之「網路詐欺被害」，有顯著影響力。

有關本研究假設六、七，經由 Poisson 迴歸分析後，部分驗證本研究之假設，研究發現「個人基本特性」、「網路生活型態」、「被害情境與機會」、「低自我控制特性」，部分對於「網路詐欺被害次數」及「網路詐欺重複被害次數」有顯著預測力存在。

表 4-6-9 本研究假設之驗證分析表

研究假設	內容	驗證結果
假設一	不同性別之網路使用者其「個人基本特性」在「低自我控制」、「被害情境與機會」及「網路詐欺被害」有顯著差異。	部分支持假設
假設二	不同性別網路使用者之「低自我控制特性」、「網路生活型態」、「被害情境與機會」及「網路詐欺被害」有顯著差異。	部分支持假設
假設三	「網路生活型態」、「被害情境與機會」、「低自我控制特性」與「網路詐欺被害」有顯著關聯性。	部分支持假設
假設四	「個人基本特性」、「低自我控制特性」、「網路生活型態」與「被害情境與機會」對於「網路詐欺被害」有顯著影響力。	部分支持假設
假設五	「個人基本特性」、「低自我控制特性」、「網路生活型態」與「被害情境與機會」對於不同性別之「網路詐欺被害經驗」，有顯著影響力。	部分支持假設
假設六	「個人基本特性」、「低自我控制特性」、「網路生活型態」與「被害情境與機會」對於「網路詐欺被害次數」有顯著影響力。	部分支持假設
假設七	「個人基本特性」、「低自我控制特性」、「網路生活型態」與「被害情境與機會」對「網路詐欺重複被害次數」有顯著影響力。	部分支持假設

第五章 結論與建議

本研究基於過往網路詐欺被害研究之基礎，除將過往文獻所列述與網路詐欺有關之個人特質納入本研究架構外，亦援引 Choi 於 2008 年結合 Hindelang(1978)生活方式暴露理論及 Cohen 與 Felson(1979)之日常活動理論後提出之網路日常活動理論(Cyber-Routine Activities Theory，簡稱 Cyber-RAT)，將網路使用者之網路生活型態、網路安全監控及被害情境與機會因素納入本研究之架構中，並依據 Gottfredson 與 Hirschi(1990)提出之自我控制理論(Self-Control Theory)，將個人自我控制程度列為研究之重要變項，以建構網路詐欺被害風險理論解釋模式，並進一步建構網路詐欺被害者未來再次遭受網路詐欺被害及重複被害次數之預測模式。

有鑑於多數學者對於以往解釋物理、實體場域之傳統犯罪學理論，是否能有效適用於虛擬網路場域之犯罪與被害行為之解釋存有廣泛之爭議，故本研究除了檢驗以往解釋實體、現實生活環境之傳統犯罪學理論(生活方式暴露理論、日常活動理論、自我控制理論)外，再整合解釋虛擬世界人們互動之理論(網路日常活動理論)以解釋並預測虛擬網路場域之詐欺犯罪被害之行為，並依據研究結果提出重要結論與具體犯罪預防之政策建議，期望能藉由本研究之發現，以強化社會大眾對於網路詐欺犯罪行為及被害風險之理解，並進一步為未來網路詐欺犯罪被害研究領域提供研究方向，是一個頗具前瞻性的整合性理論之研究。

綜上所述，本章共可分為四節，第一節係針對前章所得之研究發現進行綜合分析、歸納，據以得出本研究之重要發現及結論。第二節係依據第一節所提出之重要研究結論，具體轉化為可行之有效政策意涵，並提供有關單位擬定合宜之犯罪預防對策。第三節則根據過往文獻探討所得之重要發現及綜合歸納本研究之研究成果，提供未來研究之重要方向。最後一節則根據本研究建構之研究架構與整體研究之實施設計，分點列述本研究之研究限制。

第一節 結論與討論

本研究係以網路日常活動理論及自我控制理論為研究架構,綜合網路使用者之個人基本特性、低自我控制程度及被害情境與機會因素,藉由差異、相關及迴歸分析等方式，深入探究不同性別網路使用者間網路詐欺被害之差異因素。此外，有鑑於網路詐欺重複被害研究之重要性，本研究復依循前述理論架構，對於網路詐欺重複被害次數影響因素進行深入探討，以了解網路詐欺重複被害次數之重要影響及預測因子。

本研究依據個人特性、自我控制程度與被害情境因素，先以二元 logistic 迴歸分析對於全體調查樣本、男性及女性網路使用者，分別建構網路詐欺被害影響因素之模型，復以 Poisson 迴歸分析建構網路詐欺被害次數及重複被害次數之預測模型。研究發現則更進一步支持以網路日常活動及自我控制理論來解釋並預測網路詐欺被害風險,因此，本研究根據前章之研究發現，共歸納出 11 點重要結論與發現，茲分點列述如下:

一、性別係網路詐欺被害之重要解釋及預測因子

經由差異分析後發現，在網路詐欺被害者中，男性被害比例(66.2%)顯著高於女性(33.8%)，此研究發現不僅符合我國網路詐欺被害官方統計資料，亦與過往國內外多數研究發現(王秋惠,2007； 黃俊祥,2006； 黃珮如,2010； 張耀中,2009； 葉雲宏,2008；簡鳳容，2018; Holt et al., 2008; Holtfreter et al., 2008; Kerstens & Jansen, 2016; Trahan, Marquart, & Mullings, 2005)一致。

此外，經相關分析發現，性別與網路詐欺存在顯著相關性;另外，經二元 logistic 迴歸分析結果發現，性別係網路詐欺被害之重要解釋因子;經由 Poisson 迴歸分析後更進一步發現，性別在網路詐欺被害次數及重複被害次數，具有重要之預測能力，確實能有效預測並推估個人未來網路詐欺被害之次數機率,這些研究結果證實過往實證研究之發現，亦即性別為解釋網路詐欺被害之重要影響因素(溫怡婷，2008； 葉雲宏，2008； 蔡田木，2009； 簡鳳容，2018; Mesch & Dodel, 2018; Reyns, 2015)，其中，男性網路詐欺之被害風險又高於女性(王秋惠,2007； 黃珮如,2010； 葉雲宏,2008； 蔡田木,2009；簡鳳容，2018; Mesch & Dodel, 2018; Holtfreter et al., 2008; Kerstens & Jansen, 2016)。

二、部分個人基本特性確實與網路詐欺被害息息相關

Wilsem(2013)指出，網路犯罪者依據網路使用者在網路上所揭露之個人訊息，來設計個人化網路詐欺訊息，並鎖定具有易被害特質者作為其遂行網路詐欺犯罪之標的物，而多數被害者學理論亦指出，被害並非隨機，而是針對特定個人特質進行犯罪行為，因此，具有某些個人弱點特質者，較容易成為被害的標的物。

經差異、相關及迴歸分析後發現，在個人特性中，男性、年齡較低、無業者、收入較高、教育程度較低者，其網路詐欺被害機會較高，此一研究結果不僅與過往多數國內外文獻相符（王秋惠，2007；陳佳玉，2007；黃祥益，2006；葉雲宏，2008；蔡佳瑜，2010; Kigerl, 2012; Leukfeldt & Yar, 2016; Mesch & Dodel, 2018; Pratt et al., 2010; Van & Mason, 2001），這也進一步顯示，網路詐欺被害者確實具有部分個人弱點特質，導致其網路詐欺被害之可能性增加，這不僅證實被害者學理論，亦與 Bossler 和 Holt(2009)、Holt 等人(2018)、Holt 和 Bossler(2009)及 Wilsem(2013)之研究發現一致。

三、不同性別網路使用者其網路詐欺被害因素確實存在顯著差異

本研究以網路日常活動理論與自我控制理論之指標對於不同性別網路使用者進行差異及二元 logistic 迴歸分析後發現，不同性別網路使用者不僅在網路使用特性（平日上網時段、假日上網時段、經常上網原因）有所差異，在網路休閒活動、網路職業活動、網路風險休閒活動、網路風險職業活動、社會監控、網路負面誘因、網路偏差動機以及冒險性具有顯著差異，在網路詐欺被害影響因素，亦皆存在顯著差異，此結果證實過往研究發現（葉雲宏，2008；蔡佳瑜，2010；Holt & Bossler, 2009; Bossler & Holt,2010），這也同時證實男性與女性確實在網路生活型態上有所差異(Chang & Samuel, 2004)。

經由差異分析後發現，在兩性網路詐欺被害影響因素之差異中，男性從事較多網路風險休閒與職業活動，此一研究發現與蔡佳瑜(2010)及 Holt 和 Bossler(2009)研究一致。在被害情境與機會因素中，男性較缺乏有效的社會監控，並接收較高的網路負面誘因、具有較多網路偏差動機，此研究發現與葉雲宏(2008)、蔡佳瑜(2010)、簡鳳容(2018)、Zaykowski 和 Gunter(2013)及 Garbarino 和 Strahilevitz(2004)發現相同。在低自我控制特性方面，研究發現兩性在衝動性方面具有顯著差異，且男性衝動性程度顯著高於女性。

四、網路生活方式而非僅為網路使用頻率決定網路詐欺被害風險

經差異分析後可得知，網路詐欺被害者與未被害者在網路使用特性上具有顯著差異。經相關分析後則發現，網路詐欺被害與否與每周上網時數、每次上網時間呈顯著正相關，但進一步以二元 logistic 迴歸分析後發現，各組網路詐欺被害之影響因素中，每次上網 3-7 小時（中上網時數）者其網路詐欺被害機率卻高於每次上網 7 小時以上（高上網時數），而每周上網 7-9 次者（中上網次數）則具有最高的網路詐欺被害機率，亦即網路詐欺被害風險最高者並非上網時數最長抑或上網次數最頻繁者。

國內林清榮(2006)研究發現，從被害者角度觀點，平時較未接觸良好資訊或網路訊息者較容易被害。Mustaine 與 Tewskbury(1998)認為個人被害係與其所參與之活動及所去的地方有關，並非僅是空間因素，而 Holt 和 Bossler(2009)研究亦指出，僅擁有電腦並花費大量時間上網及高頻率上網者，並不一定會顯著增加其網路被害風險，網路被害風險程度取決於個人網路使用時所從事的活動及環境。此一分析結果證實上述學者觀點，雖然網路使用時間較長或頻率較高者，相較於低網路使用時間或頻率者，有較高的網路詐欺被害風險，但決定網路詐欺被害風險因素之重要預測因子，端視個人網路使用過程中所參與之網路風險休閒及職業活動程度，而非僅為網路使用時間之長短或頻率高低。

五、經常從事網路風險生活型態確實顯著增加網路詐欺被害可能性

經差異分析後發現，被害者與未被害者在網路休閒活動、網路職業活動及網路風險職業活動變項確實存有顯著差異，其中，被害者從事具風險性網路生活型態則顯著高於未被害者，此一研究結果與過往文獻一致（葉雲宏，2008；簡鳳容，2018；廖釗頡，2010; Choi, 2008; Marcum, 2008; Pratt el al., 2010; Ross & Smith, 2011; Wilsem, 2011）。

經相關及迴歸分析後亦發現，當網路使用者從事高風險之網路職業活動時，其網路詐欺被害可能性亦隨之增加，此一結果不僅證實網路日常活動理論指標確實足以解釋網路詐欺之被害風險，更誠如 Bossler 和 Holt(2010)、Chen 等人(2017)、Holt 和 Bossler(2009)、Holtfreter 等人(2008)所言，網路偏差行為及風險因素與網路被害間之關係不僅存在顯著關聯性，彼此間更呈現重要的顯著正相關，當網路使用者參與多種形式的網路風險生活型態，則個人暴露於有動機犯罪者之風險增加，其網路犯罪被害可能性也隨之提升。

六、網路安全監控係網路詐欺被害之重要解釋及預測因子

經差異分析發現，未被害者之物理及社會監控程度較高，而女性之物理及社會監控程度亦高於男性。經相關分析後發現，物理、社會監控程度與網路詐欺被害之可能性呈顯著負相關，亦即網路安全監控(物理監控、社會監控)較低者，將增加其網路詐欺被害可能性。此研究發現不僅支持 Choi(2008)網路日常活動理論，並與過往國內溫怡婷(2008)、蔡佳瑜(2010)、葉雲宏(2008)，國外 Grabosky 和 Smith(2001)、Yar(2005)之研究發現一致。

此外，經迴歸分析結果後發現，社會監控係全體及男性樣本網路詐欺被害之重要解釋因子，此一研究發現與過往國內外文獻一致(葉雲宏，2008；溫怡婷，2008；陳永鎮，2007；蔡佳瑜，2010; Grabosky & Smith, 2001; Lwin et al., 2008)，而物理監控則係網路詐欺被害次數、重複被害次數之重要預測因子，亦與過往國內外相關研究一致(葉雲宏，2008；廖釗頡 2010；蔡佳瑜，2010; Bossler & Holt, 2010; Chen et al., 2017; Choi, 2008; Choi, 2017; Holt & Bossler, 2010; Ngo & Paternoster, 2011)。

七、低自我控制者確實增加網路詐欺被害可能性

Holt 等人(2008)指出，經常尋求風險並有衝動性特質者，更容易顯現出低自我控制之行為，而 Holtfreter 等人(2010)則指出，低自我控制與詐欺被害暴露風險呈正相關，低自我控制程度越高者，越可能從事高詐欺被害風險之行為。

本研究經相關及迴歸分析結果均發現，自我控制程度與網路詐欺被害呈顯著負相關，研究進一步發現，在網路詐欺被害風險影響因子中，尤其以衝動性為最重要之解釋因子。此研究結果證實 Gottfredson 與 Hirschi(1990)自我控制理論確實具有解釋網路詐欺被害風險之能力，並支持自我控制理論之概念架構，亦即缺乏自我控制能力者，傾向做出與負面生活型態相關之衝動性決定，並增加其成為被害者之可能性，以及 Schreck(1999)認為自我控制能力決定個人被害程度之發現。此外，本研究發現亦與過往之研究指出，自我控制係解釋網路詐欺之重要因素(蔡田木，2009；Benson & Moore, 1992; Chen et al., 2017; Langton et al., 2006; Pratt & Cullen, 2000; Reisig et al., 2009; Simpson & Piquero, 2002; Smith, 2004)觀點一致，低自我控制確實顯著增加並預測個人網路詐欺被害可能性(Bossler & Holt, 2010; Chen et al., 2017; Holt el al., 2008; Holtfreter et al., 2010)。

八、偏差(風險)生活方式及自我控制皆係網路詐欺被害之重要解釋因素

由於網路詐欺犯罪係「情境」、「機會」、「監控」、「個人特質」等多重犯罪因子交互作用下所產生之負面結果,因此在網路詐欺被害之研究,必須將這些因子綜合納入考量。經前述研究結論後可知,以生活方式暴露理論、日常活動理論所建構之情境、機會指標,以及低自我控制特質所建構之指標,確實皆係網路詐欺被害之重要解釋及預測因素。此研究發現除支持 Choi(2008)之網路日常活動理論外,亦證實過往多數實證研究之發現,亦即具有低自我控制特質及經常從事偏差風險網路生活型態者,其暴露於網路詐欺風險之可能性確實顯著增加(王秋惠,2007; 陳佳玉,2007; 黃祥益,2006; 葉雲宏,2008; 蔡佳瑜,2010; Chen et al., 2017; Holt et al., 2008; Holt et al., 2018; Holtfreter et al., 2010; Mesch & Dodel, 2018; Schreck, 1999; Yu, 2014)。

此外,Turanovic 和 Pratt(2012)指出,低自我控制特質顯著地增加個人與有動機之犯罪者接觸之機會,並使個人從事高風險的生活方式,進而增加其重複被害之可能性。Gottfredson 與 Hirschi(1990)觀點認為,缺乏自我控制者傾向做出衝動的決定,並從事與不良生活方式相關的危險行為,而多數研究亦指出,自我控制與偏差生活型態不僅皆係網路詐欺被害之重要解釋及預測因素,低自我控制與偏差生活型態間更存有重要關聯性(葉雲宏,2008; 蔡佳瑜,2010; Bossler & Holt, 2010; Holt & Bossler, 2009; Chen et al., 2017; Franklin et al., 2015; Leukfeldt & Yar, 2016; Mesch & Dodel, 2018; Pratt et al., 2014; Ren, He, Zhao & Zhang, 2016; Schreck et al., 2002; Wilcox & Cullen, 2017; Yu, 2014)。

本研究在自我控制與生活方式之關聯性部分,雖然無法以研究所得之橫斷性資料就彼此間之因果關係進行檢驗,但經由相關分析後可知,兩者間呈現顯著正相關,當個人低自我控制程度越高時,其從事之網路風險休閒與職業活動程度亦隨之增加。換言之,低自我控制程度與偏差生活型態之間存在顯著關聯性,自我控制程度較低者較容易從事高風險的網路社交活動,而此一研究發現亦與過往國內黃祥益(2006)、葉雲宏(2008)、蔡佳瑜(2010),以及國外學者之多數研究發現相符(Choi, 2008; Donner et al., 2014; Holt & Bossler, 2009; Franklin, 2011; Franklin, 2015; Stewart et al., 2004; Turanovic & Pratt, 2012; Turanovic & Pratt, 2014)。

九、日常活動與自我控制理論彼此具有相容性，且均適用於虛擬網路場域之被害解釋

Grabosky(2001)指出，網路犯罪行為僅係「裝在新瓶中的舊酒」，在其研究中指出，雖然虛擬網路空間是一個全新的犯罪場域，犯罪者會依據環境的不同而調整其策略，但在網路空間中，犯罪的本質卻未曾改變，因此，傳統犯罪學理論之基本假設及理論概念亦可在虛擬網路中適用。部分學者亦指出，現實世界中犯罪與被害之關係可同樣在網路環境中加以擬和(Bossler & Holt, 2009)，因此，自我控制及日常活動建構之指標仍適用於網路被害之預測(Choi, 2008; Holt & Bossler, 2016; Pratt et al., 2010; Pratt et al., 2014)。此外，Hsieh 和 Wang(2018)指出，日常活動理論之適用性可能因網路時空混亂受到限制，而 Yar(2005)網路犯罪生態學中指出，很難以在網路時空中證明犯罪者與被害者如何在空間與時間上融合，因此，日常活動理論之適用仍待研究。

有鑑於此，本研究經相關、迴歸分析後發現，網路生活型態與網路詐欺被害間確實存在顯著關聯性，此研究結果亦證實過去解釋現實生活方式之日常活動理論，亦可適用於虛擬網路空間中，以網路設備為導向生活方式之被害解釋，此一研究發現亦證實過往學者研究(Argun & Dağlar, 2016; Breetzke & Cohn, 2013; Choi, 2008; Holtfreter et al., 2008; Louderback & Roy, 2018; Pratt et al., 2010)，而以自我控制理論所建構之衝動性、冒險性及投機性指標，確實能有效解釋網路詐欺被害現象並進一步推估未來再次被害之可能。綜上所述，本研究發現，證實傳統犯罪學理論之假設及理論不僅可用以解釋實體、物理的犯罪場域，亦可擴充其理論適用範圍，用於解釋虛擬網路場域中以網路為導向之犯罪及被害行為。

此外，部分學者對於日常活動及自我控制理論在網路被害行為解釋之理論競合提出許多討論(Chen et al., 2017; Franklin et al., 2015; Holt et al., 2018; Pratt et al., 2014; Schreck et al., 2002; Turanovic & Pratt, 2012)。經研究後發現，以網路日常活動及自我控制理論為架構之網路詐欺被害解釋理論框架，理論彼此間確實具有解釋之兼容性，此研究發現亦與 Holt 等人(2018)、Pratt 等人(2014)、Turanovic 和 Pratt(2012)及 Turanovic(2015)之研究發現一致。因此，強調個人層面之自我控制特質與強調情境機會因素之外在環境因素，兩者確實可以相互結合，共同適用於網路詐欺被害行為之解釋。

十、建構網路詐欺被害之重要評估指標

所謂被害原因，亦即被害者之弱點特質。江志慶(2005)研究指出，詐欺被害者通常具有多種被害特質，兼具越多被害特質者，其被害風險就越高，而 Bossler 和 Holt(2010)指出，犯罪者會依據明顯的脆弱性指標來選擇潛在的被害者。經被害者學及環境犯罪學理論之探討後可知被害並非隨機分布，而是集中於特定少數人，Tseloni 和 Pease(2004)亦指出，被害風險與個人特質及其生活方式有關。因此，發掘特定個人易被害特質成為犯罪學研究及犯罪預防重要的課題。

經對全體樣本、男性、女性網路使用者進行二元 logistic 迴歸分析後發現，無業、每周上網 3-7 小時、平日深夜時段(0-8 時)上網、假日深夜時段(0-8 時)上網、網路風險職業活動、網路負面誘因、衝動性，皆係各分組中網路詐欺被害之高風險因子。此外，在網路詐欺被害者中，經 Poisson 迴歸分析發現，男性、網路負面誘因、投機性變項係網路詐欺被害次數及重複被害次數之共同重要預測因素。

十一、確立自我控制理論之性別差異

Gottfredson 與 Hirschi(1990)自我控制理論認為，由於男性及女性在社會化過程中所受到之教育方式存有差異，故不同性別間將存在實質性之自我控制差異。部分學者更進一步指出，性別係自我控制程度的重要預測因素，而不同性別間之自我控制程度係解釋被害性別差異之重要因素(Schreck, 1999; Tittle et al., 2003)。

本研究係以衝動性、冒險性及投機性等指標，加以評估網路使用者之自我控制程度。經差異分析後發現，在冒險性部份，男性網路使用者顯著高於女性，而在投機性部分，女性網路使用者則顯著高於男性。此外，經迴歸分析後發現，影響男性、女性網路詐欺被害因素之低自我控制程度亦有所差異。在網路詐欺被害影響因素中，男性以衝動性及冒險性具有解釋能力，而在女性則以衝動性及投機性具有解釋能力。

經上述研究結果發現，男性及女性在自我控制程度上確實存在顯著差異，此一研究發現不僅證實 Gottfredson 與 Hirschi(1990)所提出自我控制在不同性別存在顯著差異之理論觀點，亦證實以往有關不同性別自我控制差異之研究(Burton et al., 1998; Gibbs et al., 1998; Higgins, 2004; Lagrange & Silverman, 1999; Schreck, 1999; Tittle et al., 2003)。

第二節 政策意涵

Cornish 和 Clarke(1986)指出，犯罪分析所得結果對於犯罪預防政策之擬定尤其重要。犯罪學研究涵蓋以下幾個重要目的:描述(Description)社會現象、解釋(Explain)社會現象發生之原因、評估(Evaluate)政策執行之成效，並提出有效的犯罪預防(Prevention)策略，最終達成降低及預防犯罪之最終目的。犯罪學理論之提出，不僅是為了解釋當代的生活問題與犯罪現象外，更重要的是將理論之因應措施轉換為有用且具影響力之政策，實行於社會中，以協助達成正義及減少因實行犯罪行為後所帶來之成本與代價。有鑑於此，本節將對於文獻探討及問卷分析結果後所得之犯罪學研究成果，具體轉化為未來可行之政策建議，以提供有關單位參酌，相關建議內容茲分述如下:

一、強化網路安全教育、提升網路風險危機認知意識

陳佳玉(2007)指出，透過教育及宣導，提升全民防詐意識，是防制詐欺被害最基礎也最重要的工作。經過往文獻探討後可知，各項網路行為所帶來之利益及誘因不僅吸引低自我控制能力者，亦增加網路使用者暴露於潛在犯罪者之風險，而網路使用者之網路安全措施及風險危機認知意識，對其是否成為網路詐欺被害者之可能性，更具有重要且顯著之影響，這也顯示，落實網路安全教育、提升民眾風險意識係刻不容緩之重要課題。

在網路安全教育部分，美國國土安全部(DHS)曾提出自動化資安威脅情資共享計畫(Automated Indicator Sharing, 簡稱 AIS)，亦於 2015 年提出 Stop、Think、Connect 計畫，該計畫係一項提升公眾資訊安全防護意識計畫，除了期望建構更安全的網路使用環境外，更著重於強化網路使用者對於網路中存在各項風險威脅之了解。該計畫強調個人在網路使用的過程中，必須先就個人帳戶之安全性進行檢視、檢視該帳戶是否設置安全密碼，並避免網路使用者之個資共享，以減少網路身分識別及個人資訊揭露，其次係評估個人的各項網路行為後果及即將訪問網站之可信賴程度，最後則要求網路使用者須要有限度地與他人聯繫、減少個人與網路風險因子接觸之機會。透過此類網路的安全教育計畫，不僅能有效改變網路使用者之風險行為、提升網路使用者資訊安全防護之意識，更有效減少潛在網路犯罪者鎖定合適標的物之機會，藉以減少網路詐欺被害行為之發生。

由於網路的便利性，多數網路使用者在網路使用之過程中疏於深入查證與確認，這也使潛在犯罪者獲得犯罪之機會。此外，減少網路詐欺風險需要政府、大眾傳播媒體及企業間之通力合作，以教育網路消費者如何與他人進行網路安全互動，故未來建議有關防制網路詐欺犯罪之教育內涵，除涵括如何讓社會大眾辨識合法網站與否外，亦應提升網路使用者對於網路技術之了解、強化個人風險辨識、危機處理及資訊判讀之應變能力，提升個人資訊安全防護意識、並進一步了解其從事之各項網路行為在何時、如何，影響網路詐欺被害風險之程度，以強化網路使用者對於網路場域之風險評估與控管能力。

二、強化網路安全監控、降低網路負面誘因

由前述研究發現可知，網路安全監控係網路詐欺重要影響因素。在物理監控方面，Holt 和 Graves(2007)指出，由於現今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。研究更指出，電子郵件不僅有助於隱藏犯罪者之身分，更是網路使用者與網路詐欺犯罪者間的中介聯繫管道。此外，部分網路詐欺犯罪者透過散播病毒或詐欺訊息，以竊取並獲得網路使用者之私人資訊。

因此，在物理監控方面，未來若能建構良好的電子垃圾郵件過濾技術，在電子郵件發送前，先檢查連結或網址是否存有惡意病毒或詐欺訊息，就能減少大量詐欺電子郵件與潛在網路詐欺被害者接觸之機會。此外，未來建議可以透過網頁瀏覽保護措施、使用防火牆、惡意軟件之檢測軟體及定期偵測、修補網路安全漏洞、強化網路設備防禦系統等物理監控措施，以有效避免網路安全漏洞，並最大程度降低潛在的網路風險與損失。

在個人監控方面，Williams(2016)認為，由於工作場所之網路資訊安全防護策略較非工作場所嚴格，故較能有效限制個人的網路使用行為。Hsieh 和 Wang(2018)亦指出，非工作場所之網路使用者，可能因缺乏網路安全監控措施，從而增加其在網路空間被害之機率，因此，強化非工作場所之個人監控，在網路犯罪預防中，儼然成為重要的議題。有鑑於此，在個人監控部分，建議網路使用者應定期更新個人帳戶密碼或使用動態密碼(One-Time Password，OTP)、強化個人帳戶安全隱私設定、降低網路個人資訊之揭露、減少瀏覽陌生網站、避免下載未知來源之檔案、避免點擊不明來源之電子郵件連結，以避免個人資訊遭竊取、盜用或洩漏之風險，藉以有效強化個人監控。

三、訂定明確法令規範、強化道德倫理及法令教育

經文獻探討後發現，網路詐欺手法不斷推陳出新，因此，犯罪者可能因為網路規範不足，而利用司法行政疏漏或規範空窗期遂行犯罪行為。此外，古典犯罪學理論認為，懲罰越迅速(swift)、確定(certain)、嚴厲(severe)，越能有效控制犯罪行為。在網路環境中，由於司法管轄權之複雜性及匿名性，使犯罪者難以被追蹤、舉證困難，而網路詐欺之定罪率及判決之嚴厲性程度普遍較低，亦導致法令規範無法達到犯罪嚇阻之成效。

Jaishankar(2008)認為，透過強化自我調節能力，可以有效降低網路犯罪及被害，而自我調節能力則取決於個人道德標準與原則，因此，要有效減少網路犯罪根源，可透過提升公民品德及強化個人成為守法公民之期望。Morita(2005)指出，除提升網路使用者之安全防護意識外，政府亦應訂定明確的網路法令規範，針對網路犯罪做出即時、迅速的反應，並實際透過深入各級學校教育的方式，不僅可提升網路使用者對於法令規範之意識，亦可透過明確法令規範，進一步對網路詐欺犯罪者產生有效的嚇阻作用。

因此,為有效減少網路詐欺被害之發生,建議有關單位應強化社會大眾之法治素養,教育大眾知法、守法之法治觀念，營造法治社會、以避免個人誤觸法網、提升個人道德倫理觀念、強化自我調節能力，從而減少個人從事網路風險活動及偏差動機之產生。

四、強化網路社群媒體監控、要求網路業者落實分級管理

經二元 logistic 迴歸分析發現，影響全體樣本、男性及女性網路使用者之網路詐欺被害共通因素係「網路負面誘因」，而經 Poisson 迴歸分析後亦發現，在預測網路詐欺被害次數與重複被害次數方面,「網路負面誘因」仍然係顯著的預測因子。由此可知，在網路詐欺被害之影響因子中，網路負面誘因係不可或缺的重要解釋及預測因子。

在現今網路場域中，網路社群媒體日益增加，雖然提供多樣且豐富的資訊，但同時可能帶來部分網路負面偏差訊息。有鑑於網路負面誘因係網路詐欺被害之重要預測指標，因此，未來建議有關單位應強化各網路社群媒體平台之監控，除了要求各網路社群平台先過濾資訊之正確與否，以及實際內容是否涉及負面誘因訊息外，亦應要求各網路社群媒體落實分級制度，對於網站瀏覽者之身分採取嚴格查核制度，以降低網路使用者接收負面誘因之機會，藉以有效減少網路詐欺被害之發生。

五、提前辨識網路詐欺高風險被害族群，以防患於未然

經環境犯罪學理論及被害者學理論之探討後可知，犯罪及被害行為並非隨機分布，而是集中於特定的行為人、特定時間或地點，因此，針對可能被害的行為者或可能發生犯罪之時間提前進行辨識，就能有效減少犯罪發生之可能性，而 Hsieh 和 Wang(2018)亦指出，將犯罪預防資源運用於潛在被害標的物上、透過教育及讓被害者參與網路安全防護及規避風險之策略，最有助於降低犯罪被害發生之風險。

有鑑於前述研究結果顯示，被害行為集中於少數特定人，亦即這些具特定個人弱點特質者經常成為網路詐欺犯罪者鎖定之目標，因此，未來建議網路詐欺犯罪防制機構應對於可能或經常遭受網路詐欺被害之族群提早進行辨識，並結合銀行及匯款部門，針對網路使用者之個人特質、交易模式及被害行為進行分析，以具體了解被害者之個人特徵，並了解何人何時可能成為網路詐欺被害者，同時對於網路詐欺被害重複被害者進行個人特質及風險因素之分析與識別，以將有限的犯罪預防資源挹注於所謂的「重複被害者」(Repeated victims)或「核心被害者」(Hard-core victims)上，藉以有效提升執法單位犯罪預防之成效。

六、降低網路依賴、減少風險網路生活型態

Reisig 等人(2009)研究指出，減少個人上網時間及網路購物頻率就能有效降低其成為網路詐欺被害者的機會。有鑑於近年來網路使用人口及網路使用設備逐漸增加之趨勢，人們接觸網路之管道及機會提升，這不僅改變人們的日常生活型態，亦進一步導致不同類型之網路犯罪與被害更加頻繁地發生(Hsieh & Wang, 2018; Singer & Friedman, 2013)，因此，降低個人網路依賴程度、減少網路偏差生活型態便成為防制網路被害首要之務。

經前述研究結論可得知，網路風險生活型態與網路詐欺被害風險呈現顯著正相關，當網路使用者從事高風險網路生活型態，將增加個人與潛在網路詐欺犯罪者接觸之機會，並提升其成為網路詐欺被害者之可能性。此外，研究亦發現，每次上網時間較高、每周上網次數較高者，相較於低上網時間或使用頻率者，有較高的網路詐欺被害機率。因此，若要有效減少網路詐欺被害風險，除了須降低個人網路依賴程度、減少網路使用時間及頻率外，亦須減少網路風險生活型態，鼓勵網路使用者從事正向網路休閒與職業活動。

七、將網路犯罪與網路資訊安全防護納入核心專業學習課程範疇

由於虛擬網路場域是一個比現實世界更缺乏監控之環境，故McQuade(2006)指出，要有效強化網路資訊安全性、提升監控，並減少網路犯罪之重要方法係透過「公眾意識」(Public awareness)、「正規教育」(formal education)及「專業培訓」(professional training)。Morita(2005)亦認為，雖然網路使用人數逐年上升、網路技術日新月異且蓬勃發展，但具結構性、系統性之網路犯罪預防課程卻仍未深入各級學校之核心學習職能課程，納入網路使用者之核心專業修習範疇。

以美國為例，近年來在部分高中、大學之課程中，除已將網路犯罪及網路資訊安全之基礎防護課程納入其必修課程外，亦將部分進階網路通訊及資訊安全課程，納入專業之核心職能課程，不僅可使網路使用者具有最基本的網路安全防護技能，讓網路使用者可以辨識在何種情況係處於高風險之情境下，亦可以強化個人對於各類網路犯罪之基本認知，以減少網路犯罪行為之發生。

未來建議將網路資訊安全、網路犯罪預防課程納入各級學校之入門及專業必修課程，這不僅可為網路使用者提供基本的網路資訊安全知識、強化網路安全防護意識，亦可透過對於網路犯罪手法、類型及其管道之理解，相應地採取減少網路犯罪被害風險之行為，以強化個人資安防護意識並有效遏止網路被害之發生。

八、即時公布最新網路詐欺犯罪手法與犯罪機制、持續強化網路詐欺宣導

Choi(2008)網路日常活動理論之核心概念在於，從事高風險網路生活型態及缺乏網路安全監控者，其遭受各類型之網路犯罪被害之可能性將會增加。此外，部分實證研究顯示，潛在的網路詐欺者透過網路上所獲得之資訊來選擇合適的標的物(Pratt et al., 2010; Wilsem, 2013)，而網路使用者所從事之高風險網路行為則增加其成為網路詐欺被害者之可能性(Leukfeldt & Yar, 2016; Mesch & Dodel, 2018; Whitty, 2019)。

有鑑於此，提升網路使用者之風險認知意識，進而減少其網路風險生活型態，便成了減少網路詐欺被害風險之重要犯罪預防策略。因此，未來建議應定期公布高風險網路賣家，以提升網路使用者之風險認知意識，藉以減少網路使用者與潛在網路詐欺犯罪者接觸之機會、降低暴露於網路詐欺風險之機會。

此外，由於網路詐欺犯罪者經常利用人性弱點及人們的消費特性，製造虛擬場域中真假難辨之資訊，故政府各項措施應與時俱進，即時公布網路詐欺犯罪機制或交易手法，協助個人辨識新型態網路詐欺手法及高風險網路交易平台、減少網路中個人資訊揭露，並持續強化反詐騙宣導，不僅可使網路使用者了解，在何種情境下具有較高被害風險與機會，亦能使網路使用者了解如何在此種風險被害情境下，採取能有效避免被害之措施，藉以降低其成為網路詐欺被害者之可能性。

九、避免在高風險被害時段從事網路行為

在前述差異分析後發現，不同性別網路使用者在平日及假日上網時段有所差異，而網路詐欺被害者與非被害者在平日及假日上網時段亦有所差異，其中，男性在平日及假日深夜時段(0-8 時)上網之比例顯著高於女性，而被害者在平日及假日深夜時段(0-8 時)上網之比例亦顯著高於未被害者。經由多變量分析後亦可以得知，在全體樣本、男性及女性樣本中，網路詐欺被害影響因素之網路使用特性，其中在平日深夜時段(0-8 時)及假日深夜時段(0-8 時)上網者，在各組樣本中皆顯著提升其網路詐欺被害之可能性，故可以得知，不同上網時段顯著地影響網路詐欺被害之風險。

生活方式暴露理論認為，當個人生活型態與犯罪者接觸之機會越高，其暴露於風險情境之機會亦隨之增加，這也使個人被害可能性增加，而 Fisher 等人(2002)、Grabosky 和 Smith(2001)及 Lwin 等人(2008)亦指出，多數網路犯罪被害皆係缺乏有能力之監控者，而缺乏有能力之監控者將使潛在的犯罪者獲得直接接觸標的物之機會，因此，若在個人網路使用過程中，適時地出現有能力之社會或物理監控者，則將有效遏阻個人成為網路犯罪被害者之可能性。

有鑑於前述學者之研究概念及前述研究發現，因此，在平日或假日深夜時段上網者相較於在白天時段(8-16 時)或夜間時段(16-24 時)上網者，缺乏有效之社會或物理監控者，這也使個人在網路使用過程中缺乏網路安全監控，進而容易成為網路詐欺被害者。因此，建議網路使用者除應避免在深夜時段(0-8 時)上網外，在平時網路使用之過程中，亦應避免獨自從事各項網路行為、並提升個人網路風險意識，藉以有效強化個人之社會或物理監控程度，以降低網路詐欺被害之風險。

十、建構完整網路詐欺犯罪預防機制

綜合上述網路詐欺犯罪預防具體政策建議後，本研究根據不同政策類型加以歸納、整理，並參酌日常活動理論及犯罪鐵三角理論之概念架構後，依據標的物(被害者)、潛在犯罪者及情境(場域)等三個重要面向，具體劃分為三大網路詐欺犯罪預防機制，並進一步提出完整網路詐欺犯罪預防機制運轉模式。

首先，在標的物(被害者)之犯罪預防策略包括:降低個人網路依賴程度、減少從事網路風險行為並增加網路風險意識。其次，在網路場域之犯罪預防策略中，係透過明確網路法令規範、落實網路分級管理、減少網路負面誘因，以減少網路場域之犯罪行為。最後係就潛在犯罪者所提出之犯罪預防策略，其中包括:強化網路監控、提升道德倫理規範並抑制個人偏差動機。有關網路詐欺犯罪預防機制之運轉模式分析如圖 5-2-1 所示:

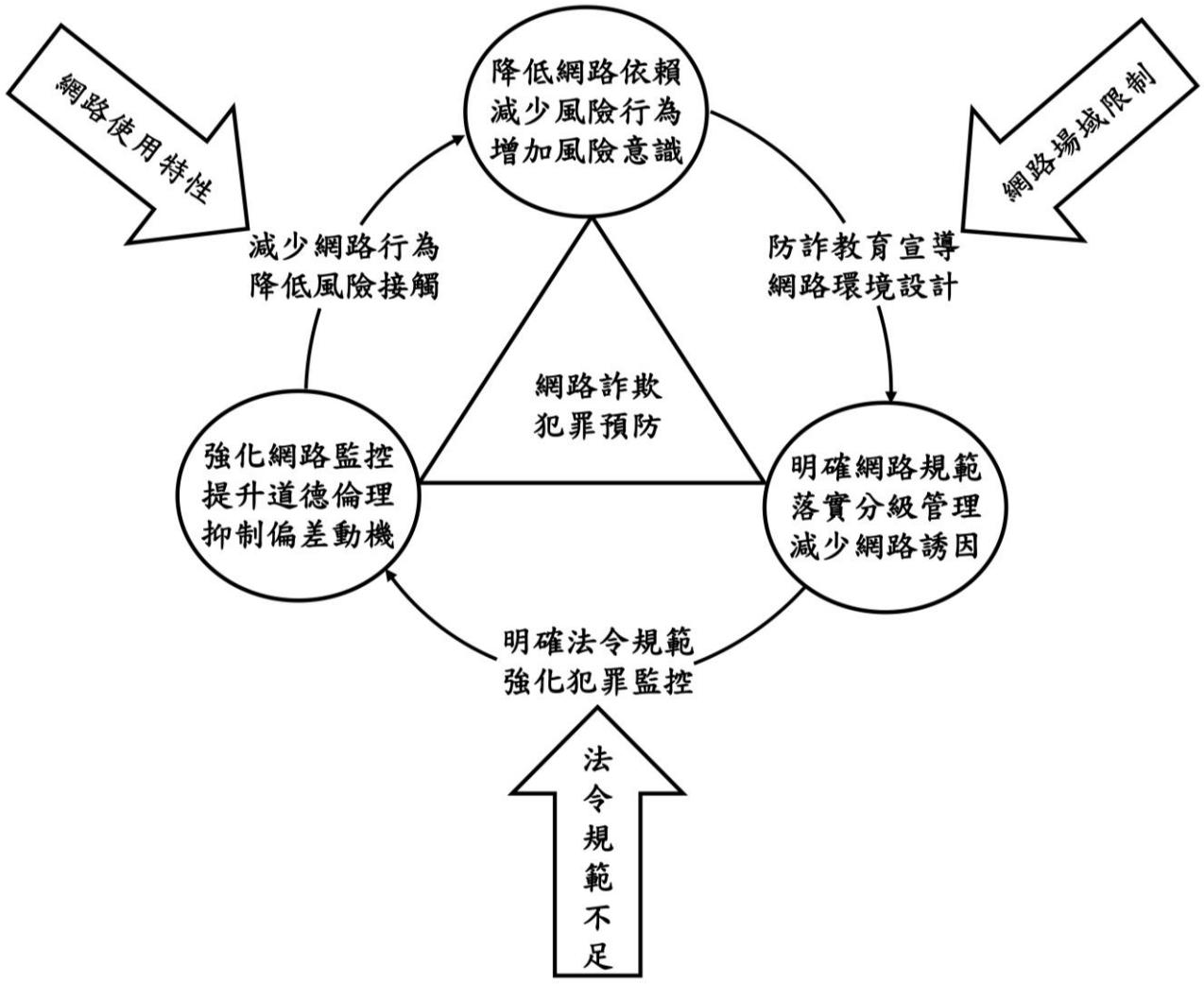

圖 5-2-1 網路詐欺犯罪預防機制運轉模式

第三節 未來研究建議

一、建議以量化研究之方式增加情境模擬之理性選擇理論模式

Piquero 和 Bouffard(2007)指出，詐欺行為涉及個人評估其行為可能性之成本及利益理性思考之認知決策，因此，理性選擇也須要納入決策之歷程中。雖然過往研究以理性選擇理論為架構，對於網路詐欺被害或重複被害現象進行研究，但多數研究以質化訪談方式，對於被害者網路詐欺被害歷程進行探討，而未以情境模擬之量化方式深入研究。

溫怡婷(2008)指出，個人特性會影響詐欺被害之情境、機會因素與監控程度，形成訊息互動的特性，而在訊息互動之過程中，則展現加害者與被害者之間的動態互動關係。由此可知，網路詐欺被害即為一連串負面因果機制所導致之結果，當中不僅涉及被害者與犯罪者間的動態互動關係，亦與個人理性思考後所做出之抉擇有關，故未來研究建議可以理性選擇理論為架構，以情境模擬之方式，建構數個模擬場域，以量化研究之方式了解網路使用者在面對不同的虛擬網路模擬場域時，其理性選擇之決意歷程。

二、建議增加網路風險認知評估模型

陳永鎮(2006)認為，詐欺歷程涉及個人生活型態及風險評估過程，Chen 等人(2017)研究指出，網路詐欺被害者之網路風險認知具有高度嚴重性及脆弱性。有鑑於網路詐欺被害涉及個人在從事網路行為過程中，對於網路風險認知之評估程度，故未來研究建議可納入個人暴露於各種網路風險情境時之個人風險認知評估模型(例如，保護動機理論 Protection Motivation Theory，簡稱 PMT)，藉由評估個人風險感知程度、自我效能以及反應策略，以了解其在從事各項網路行為之風險認知程度與網路詐欺被害之間的關係。

三、建議增加心理認知與人格傾向因素

有鑑於前述網路詐欺被害涉及一連串理性思考及決意歷程，在這複雜的決意歷程中，網路使用者評估風險之程度及其從事各項行為當中所蘊含之心理機制，更係影響其從事各項網路行為之重要因素，因此建議未來研究可於研究架構中增加心理機制相關理論(例如，平行過程延伸模式 Extended parallel process model，簡稱 EPPM)，以更加深入、完整地了解網路使詐欺被害者之複雜心理機制及行為認知評估歷程。

此外，Choi(2008)指出，多數學者認為冒險行為係屬於個人之人格傾向，具冒險性人格特質者決定其從事冒險行為之認知程度，因此，未來研究除了可納入上述心理機制理論外，亦可增加個人人格特質因素，以完整解釋個人網路風險行為。

四、建議納入社會學習理論模型

Choi 和 Lee(2017)認為，除了評估個人及情境因素外，社會學習理論之概念原則亦有助於促進網路犯罪之動態發展。在網路犯罪過程中，父母監控之社會監控程度不再是網路空間中的決定性因素，係因網路犯罪者可透過與網路使用者之互動過程，決定是否將其視為犯罪鎖定之目標，因此，在網路互動的過程中，個人與他人互動歷程及其行為模式便成為是否遭受網路被害之重要因素。

有鑑於網路使用者之個人網路行為模式係網路被害之重要決定因子，故網路場域之同儕、熟識者及重要他人對於形塑其行為發展具有重要意義。在社會學習理論中，個人透過與他人之接觸學習而形塑其行為模式，故未來研究建議可將社會學習理論納入架構，並整合日常活動理論、自我控制理論，以更完整地評估不同類型之網路犯罪被害。

五、建議將各網路社群網站之網路安全管理措施納入研究範疇

有鑑於現今社群媒體網站之蓬勃發展，不同社群媒體網站具有不同的網路安全管理措施，而不同程度的網路安全管理措施相對而言也影響著網路被害之風險程度，因此，未來研究建議將不同社群網站之安全防護監控措施納入研究之評估中，除比較不同社群媒體管理措施之安全性程度外，亦可全面地了解網路安全監控與網路詐欺被害之關聯性（例如：採取較多網路安全防護措施之社群媒體，其網路詐欺被害機率是否相對較低）。

六、建議可採用縱貫性研究

Hindelang 等人(1978)認為，研究模型中各因素的許多重要因果連結必須透過縱貫性數據進行檢驗，因此，縱貫性資料不僅可以確立不同因素之間的因果機制，亦可以探究隨時間變化而產生改變之日常活動及被害行為。此外，由於網路詐欺被害係因個人內在特質與外在環境因素交互作用產生之結果，係一連串動態的變化歷程，故未來研究建議可擴充調查時間及研究範圍，不僅有助於更全面性地了解網路詐欺被害者之被害歷程，亦能深入探究不同因素發生之時間序列及其因果機制。

第四節 研究限制

Bossler 和 Holt(2010)指出，過去主導被害者學領域之研究多為注重情境之理論，而較少評估個人層級理論。本研究旨在探究不同性別網路詐欺被害之影響因素及網路詐欺被害次數、重複被害次數之影響因子，雖已盡可能地系統性評估整體網路詐欺被害因子，並將強調情境、機會因素之網路日常活動理論及強調個人層面之自我控制理論納入研究架構中，但仍不免存在部分研究上之限制，以下僅就本研究之限制臚列說明如下:

一、橫斷性資料無法檢驗網路詐欺被害因素間之因果機制

本研究考量研究之時程限制與實際執行可行性，故無法以縱貫性研究進行長時間之被害調查，而係以橫斷性問卷調查對於網路詐欺被害者過去一年內之網路詐欺被害經驗進行統計分析，但由於橫斷性資料僅能就受訪者特定時間、地點內所為之行為進行檢驗，而無法進一步檢驗網路詐欺被害因素之間的因果機制及行為發展歷程變化，故本研究除無法確立自我控制與日常活動之間的因果關係外，亦無法深入探究日常活動及自我控制因素在被害行為之影響及其時間序列關係，使部分重要概念難以深入一一釐清。

二、以自陳報告調查無法完全精準掌握被害發生現象

由於本研究調查涉及個人網路詐欺被害經驗，可能涉及個人敏感性隱私問題或引起受訪者之痛苦經驗，故本研究雖以較具隱私及匿名性之網路問卷進行網路詐欺被害調查，但 Lee 和 Soberon-Ferrer(1997)指出，受試者仍可能因問題敏感性及避免其創傷經歷再次顯現，而隱藏真實被害行為之經歷，而 Choi 和 Lee(2017)更指出，即便問題不具敏感性，但由於本研究在網路詐欺被害經驗之調查係屬於回溯性之自陳調查報告，故仍有可能因受訪者之記憶誤差或不實陳述，而造成其被害經驗之錯誤報告。因此，有鑑於自陳調查報告之特性，仍須考量報告中存在些許不準確或數據偏差之可能性。

此外，部分被害者除了不想表明其被害經驗、未詳實報告其被害時間及被害程度外，亦有多數網路使用者雖已蒙受網路詐欺之害，但卻尚不清楚個人已成為網路詐欺被害者，這些因素都將使實際被害者被歸類為未被害者，產生犯罪調查中之犯罪黑數(Dark figure of Crime)，使整體被害人數或被害次數被低估，因而造成調查上可能存在些許誤差。

三、網路安全監控測量仍可能存在些許誤差

本研究在網路安全監控之測量部分，依據Cohen與Felson(1979)日常活動理論概念，將有能力之監控者(Capable Guardianship)更進一步劃分為社會監控(Social Guardianship)及物理監控(Physical Guardianship)兩個概念，並依據過往文獻對此二構面進行題項編制，但在網路安全監控之測量方面，由於現今網路社群媒體日益增加，故本研究並未將所有網路社群媒體安全監控措施納入整體網路安全管理評估之測量範疇中，因此，未來研究可納入不同社群媒體之網路安全監控措施，以更完整地評估社群網站之網路安全監控。此外，有鑑於電腦防護軟體之安裝時間長短，係物理監控措施中相當重要的評估指標，故未來研究可藉由調查網路使用者實際安裝電腦防護軟體之時間，藉以更加深入地探究物理監控與網路詐欺被害間之關聯性。

四、計數型資料之測量仍可能存有些許誤差

本研究在網路詐欺被害次數之測量方面，雖已參酌過去有關計數型資料之研究設計，盡可能地提升測量之精確程度，但由於係採自陳式回溯調查，故部分受試者仍可能因其記憶誤差、扭曲、失真，而造成實際填報次數過多或過少，亦或是被害數量過於龐大而使其填輸數字產生誤差，這也導致研究者在無法得知其實際被害情形之狀況下，僅能就受試者實際填答之被害次數進行分析並據以推論，從而可能造成測量有效性產生誤差。

五、網路問卷調查應避免過度推論

林秀怡(2011)指出，量化研究主要限制之一，係樣本代表性及統計結果推論適切性。本研究在抽樣技術部分，雖係採用非隨機抽樣中之立意抽樣方法來擇定受試對象，但為使調查樣本盡可能地具代表性，故本研究控制「性別」及「年齡」，決定各分層中母體與樣本之實際抽樣結構，並依據實際抽樣所得之結果，與母體結構進行卡方適合度檢定。經檢定結果顯示，樣本與母體結構在各分層之比例中均未達統計上之顯著水準(P>.05)，亦即母體與樣本在結構上並未有差異，故統計分析之結果可據以推論至母體。

雖然本研究抽取之樣本具有代表性，但由於網路問卷調查僅係對於網路使用者進行其網路使用行為之調查，故雖可據以推論至母體，但母體亦僅侷限於全體網路使用人口，而非一般社會大眾，故在統計結果之推論上，研究應避免過度推論至一般民眾。

參考文獻

中文部分

王文生(2005)。**新興詐欺犯罪被害者之研究─以台北縣假盜刷真詐財案件為例**（未出版之碩士論文）。中央警察大學，桃園市。

王秋惠(2007)。**網路詐欺被害特性與被害歷程之研究**（未出版之碩士論文）。中央警察大學，桃園市。

王茜(2014)。**網路成癮、網路偏差及網路被害者之關係:人的聚合還是網路活動場域的聚合？**（未出版之碩士論文）。國立臺北大學，新北市。

刑事警察局(2018)。**中華民國刑案統計**。台北:內政部警政署刑事警察局。

江志慶(2005)。**ATM 轉帳詐欺犯罪的實證研究**（未出版之碩士論文）。中央警察大學，桃園市。

江南逸(2003)。**國中生使用網路之偏差行為和網路沈迷程度對生活適應之研究**（未出版之碩士論文）。國立中正大學，嘉義縣。

江旭麗(2004)。**社會控制、自我控制與少女偏差行為之研究**（未出版之碩士論文）。國立臺北大學，新北市。

李政忠(2004)。從抽樣與統計方法探討網路問卷調查的可行性：比較電話訪談與網路問卷樣本的實質差異性。**廣播與電視**，**21**，55-94。

李政忠(2004)。網路調查所面臨的問題與解決建議。**資訊社會研究**，**6**，1-24。

吳柏鏢(2005)。**電話詐欺犯罪特性之研究－以台北縣為例**（未出版之碩士論文）。輔仁大學，新北市。

吳嫦娥(2004)。台北市少年網路成癮傾向及網路被害現況調查。**青少年網際網路使用相關問題與防治對策學術研討會論文集**，47-48。

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。

范國勇、謝文彥(2005)。**網路犯罪成因與防制對策之研究**。台北：內政部警政署刑事警察局。

范國勇、張平吾、蔡田木(2004)。**ATM 轉帳詐欺犯罪之實證研究**。內政部警政署刑事警察局委託研究案。

林山田、林東茂、林燦璋、賴擁連(2019)。**犯罪學(修訂六版)**。台北：三民書局。

林宜隆(2000)。網路犯罪及其偵查活動之實證分析研究。**中央警察大學警學叢刊**，**31**(3)，189-210。

林宜隆(2010)。**網際網路與犯罪問題之研究**。桃園:中央警察大學出版社。

林宜隆、黃讚松(2002)。網路使用問題分析與犯罪預防之探討。*Journal of Information, Technology and Society*，*2*(2)，95-114。

林秀怡(2011)。**性別、緊張及青少年偏差與犯罪行為之實徵研究---一般化緊張理論之驗證**（未出版之博士論文）。中央警察大學，桃園市。

林清榮(2005)。**新興詐欺犯罪被害歷程之研究-以信用貸款詐欺為例**（未出版之碩士論文）。國立中正大學，嘉義縣。

周愫嫻 (2014) 。青少年網路虛擬身份分與網路被害、不當行為。**犯罪與刑事司法研究**，**22**，45-73。

徐郁婷(2017)。**比較廣義回歸模型和負二項回歸模型處理過度離散資料的問題**(未出版之碩士論文)。國立陽明大學，台北市。

張紹勳、林秀娟(2018)。**邏輯斯迴歸分析及離散選擇模型：應用 SPSS**。台北：五南圖書出版公司。

張隆興(2005)。**詐欺重複被害研究**(未出版之碩士論文)。國立臺北大學，新北市。

張耀中(2003)。**倒會被害人特徵與倒會被害機會之研究**（未出版之碩士論文）。國立臺北大學，新北市。

張耀中(2009)。「維基式犯罪預防」—從日常生活理論談網路犯罪預防模式。**犯罪學期刊**，**12**，87-115。

許春金(2000)。**台灣地區犯罪被害經驗調查研究**。台北：法務部、內政部警政署。

許春金(2006)。**人本犯罪學**。台北：三民書局。

許春金(2013)。**犯罪學(修訂七版)**。台北：三民書局。

許春金、楊士隆等著(2016)。**刑事司法與犯罪學研究方法**。台北：五南圖書出版公司。

許維維(2009)。**國中生網路虛擬財物竊盜之加害人與被害人特性分析**（未出版之碩士論文）。國立臺北大學，新北市。

許淑華(2002)。**性別、自我控制與機會對少年犯罪與偏差行為之影響犯罪共通性理論之驗證**（未出版之碩士論文）。中央警察大學，桃園市。

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)，1-32。

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**，115-145。

陳永鎮(2007)。**台灣地區新興詐欺犯罪趨勢與歷程之研究**（未出版之碩士論文）。中央警察大學，桃園市。

陳永鎮(2009)。**詐欺犯罪被害歷程之研究－以高雄地區假冒公務員名義通訊詐財為例**（未出版之碩士論文）。國立中正大學，嘉義縣。

陳佳玉(2007)。**通訊金融詐欺犯罪被害特性及歷程之分析**（未出版之碩士論文）。中央警察大學，桃園市。

陳怡儒(2010)。**少年網路霸凌被害因素研究-以日常活動理論分析**（未出版之碩士論文）。國立中正大學，嘉義縣。

陳怡璇(2007)。**性別、少年網路偏差與犯罪行為影響因素之研究**（未出版之碩士論文）。中央警察大學，桃園市。

陳碧祥(2011)。以網路為研究媒介之研究倫理問題新挑戰：85-97 學年度教育類論文之分析研究。**教育科學研究期刊**，**56**(2)，27-67。

陳靜慧(2015)。**網路犯罪之新趨勢與規範狀態之初探～從物聯網之發展談起**。臺灣嘉義地方法院檢察署 104 年度自行研究報告。

曾百川(2006)。**網路詐欺犯罪歷程之質化研究**（未出版之碩士論文）。中央警察大學，桃園市。

黃蘭媖(2002)。英國防治重複被害策略之研究。**中央警察大學犯罪防治學報**，**3**，317-341。

黃富源(2002)，被害者學理論的再建構。**中央警察大學犯罪防治學報**，**3**，1-24。

黃富源、范國勇、張平吾(2002)。**犯罪學概論**。桃園：中央警察大學。

黃富源、張平吾(2008)。**被害者學新論**。台北：三民書局。

黃祥益(2006)。**台灣地區少年網路犯罪與被害特性之研究**（未出版之碩士論文）。中央警察大學，桃園市。

黃俊祥(2006)。**少年網路偏差與犯罪行為成因之研究**（未出版之博士論文）。中央警察大學，桃園市。

黃珮如(2010)。**影響電話詐騙犯罪被害因素之研究**（未出版之博士論文）。中央警察大學，桃園市。

黃讚松(2000)。**從情境犯罪預防理論探討網路犯罪預防對策之研究**（未出版之博士論文）。中央警察大學，桃園市。

溫怡婷(2008)。**詐欺犯罪之重複被害特性及其歷程**（未出版之碩士論文）。中央警察大學，桃園市。

廖釗頡(2010)。**網路釣魚被害類型及其成因**（未出版之碩士論文）。國立臺北大學，新北市。

葉雲宏(2007)。**網路詐欺犯罪被害影響因素之研究**（未出版之碩士論文）。中央警察大學，桃園市。

蔡田木、陳永鎮(2007)。通訊詐欺犯罪模式與決意歷程之研究。**中央警察大學犯罪防治學報**，**8**，147-188。

蔡田木、陳永鎮(2007)。新興詐欺犯罪趨勢與防治對策之探討。**中央警察大學犯罪防治學報**，**7**，309-331。

蔡田木、周文勇、陳玉書(2009)。**詐騙犯罪被害人屬性之研究**。內政部警政署刑事警察局委託研究報告。

蔡佳瑜(2010)。**少年網路詐欺被害歷程之研究**（未出版之碩士論文）。中央警察大學，桃園市。

蔡其芳(2006)。**線上遊戲竊盜加害與被害特徵之研究**（未出版之碩士論文）。國立臺北大學，新北市。

劉品秀(2007)。**網路交友欺騙類型及被害特質之研究**（未出版之碩士論文）。國立中正大學，嘉義縣。

鄧煌發等著(2012)。**犯罪預防理論與實務**。台北：洪葉文化事業有限公司。

鄧煌發(2007)。犯罪分析與犯罪學理論—環境犯罪學理論之應用與評析。**警學叢刊**，**38**(1)，1-20。

鄭文鐸(2018)。**男性與女性電信詐欺犯罪者自我控制與同理心之研究**（未出版之碩士論文）。國立中正大學，嘉義縣。

鄭佳虹(2006)。**網路詐欺犯罪之實證研究—以網路拍賣詐欺為例**（未出版之碩士論文）。中央警察大學，桃園市。

賴克宗(2005)。**大學生網路犯罪被害研究-以國立中正大學學生為例**（未出版之碩士論文）。國立中正大學，嘉義縣。

簡鳳容(2018)。**網路偏差與被害特性及其影響因素之研究**（未出版之博士論文）。中央警察大學，桃園市。

英文部分

Anderson, K. B. (2004). *Consumer fraud in the United States: An FTC survey*. Washington, DC: Federal Trade Commission.

Averdijk, M. (2011). Reciprocal effects of victimization and routine activities. *Journal of Quantitative Criminology*, *27*(2), 125–149.

Averdijk, M., & Loeber, R. (2012). The role of self-control in the link between prior and future victimization. *International Review of Victimology*, *18*(3), 189–206.

Baron, S. W., Forde, D. R., & Kay, F. M. (2007). Self-control, risky lifestyles, and situation: The role of opportunity and context in the general theory. *Journal of Criminal Justice*, *35*(2), 119–136.

Bay, D., Cook, G., Grubisic, J., & Nikitkov, A. (2014). Identifying fraud in online auctions: A case study. *Accounting Perspectives*, *13*(4), 283-299.

Bossler, A., & Holt, T. (2009). On-line activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology*, *3*(1), 400-420.

Bossler, A., & Holt, T. (2010). The effect of self-control on victimization in the cyberworld. *Journal of Criminal Justice*, *38*(3), 227-236.

Buchanan, T., & Whitty, M. T. (2014). The online dating romance scam: Causes and consequences of victimhood. *Psychology, Crime & Law*, *20*(3), 261-283.

Burton, V. S., Cullen, F. T., David Evans, T., Alarid, L. F., & Gregory Dunaway, R. (1998). Gender, self-control, and crime. *Journal of Research in Crime and Delinquency*, *35*(2), 123–147.

Cameron, A., & Trivedi, P. (2013). *Regression analysis of count data*. Cambridge: Cambridge University Press.

Capeller, W. (2001). Not such a neat net: Some comments on virtual criminality. *Social & Legal Studies*, *10*(2), 229–242.

Chainey, S., Curtis-Ham, S., Evans, R., & Burns, G. (2018). Examining the extent to which repeat and near repeat patterns can prevent crime. *Policing: An International Journal*, *41*(5), 608-622.

Chen, H., Beaudoin, C. E., & Hong, T. (2017). Securing online privacy: An empirical test on internet scam victimization, online privacy concerns, and privacy protection behaviors. *Computers in Human Behavior*, *70*, 291–302.

Choi, K. (2008). Computer crime victimization and integrated theory: An empirical assessment. *International Journal of Cyber Criminology*, *2*(1), 308-333.

Choi, K., & Lee, J. (2017). Theoretical analysis of cyber-interpersonal violence victimization and offending using cyber-routine activities theory. *Computers In Human Behavior*, *73*, 394-402.

Clarke, R. V. (1999). *Hot products: Understanding, anticipating, and reducing demand for stolen goods*. *Police Research Series*. London: Home Office.

Cohen, L., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, *44*(4), 588-608.

Cullen, F., Agnew, R., & Wilcox, P. (2018). *Criminological theory* (6th ed.). NY : Oxford University Press.

Donner, C., Marcum, C., Jennings, W., Higgins, G., & Banfield, J. (2014). Low self-control and cybercrime: Exploring the utility of the general theory of crime beyond digital piracy. *Computers In Human Behavior*, *34*, 165-172.

Dziuban, C., & Shirkey, E. (1974). When is a correlation matrix appropriate for factor analysis? Some decision rules. *Psychological Bulletin*, *81*(6), 358-361.

Ellingworth, D., Farrell, G., & Pease, K. (1995). A victim is a victim? Chronic victimization in four sweeps of the British crime survey. *British Journal of Criminology*, *35*(3), 360-365.

Farrell, G., & Pease, K. (1993). *Once bitten, twice bitten*. *Police Research Group Crime Prevention Unit Series Paper 46*. London: Home Office Police Department Research Group.

Farrell, G., Phillips, C., & Pease, K. (1995). Like taking candy: Why does repeated victimization occur? *The British Journal of Criminology*, *35*(4), 384-399.

Fischer, P., Lea, S. E. G., & Evans, K. M. (2013). Why do individuals respond to fraudulent scam communications and lose money? *Journal of Applied Social Psychology*, *43*(10), 2060–2072.

Franklin, C. A., Franklin, T. W., Nobles, M. R., & Kercher, G. A. (2012). Assessing the effect of routine activity theory and self-control on property, personal, and sexual assault victimization. *Criminal Justice and Behavior*, *39*(10), 1296–1315.

Flanagin, A., Hocevar, K., & Samahito, S. (2014). Connecting with the user-generated Web: How group identification impacts online information sharing and evaluation. *Information, Communication & Society*, *17*(6), 683-694.

Forde, D. R., & Kennedy, L. W. (1997). Risky lifestyles, routine activities, and the general theory of crime. *Justice Quarterly, 14*(2), 265-294.

Gottfredson, M. R., & Hirschi, T. (1990). *A general theory of crime*. Stanford, CA: Stanford University Press.

Goucher, W. (2010). Being a cybercrime victim. *Computer Fraud & Security*, *10*(2), 16–18.

Grabosky, P. (2001). Virtual Criminality: Old wine in new bottles? *Social & Legal Studies*, *10*(2), 243–249.

Hilbe, J. M. (2017). *Negative binomial regression* (2nd ed.). Cambridge, UK: Cambridge University Press.

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 Publishing Company.

Holt, T. J., & Bossler, A. M. (2009). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior*, *30*(1), 1–25.

Holt, T. J., & Bossler, A. M. (2013). An assessment of the current state of cybercrime scholarship. *Deviant Behavior*, *35*(1), 20-40.

Holt, T. J., & Bossler, A. M. (2016). *Cybercrime in progress: Theory and prevention of technology-enabled offenses*. London, England: Routledge.

Holt, T. J., van Wilsem, J., van de Weijer, S., & Leukfeldt, R. (2020). Testing an integrated self-control and routine activities framework to examine malware infection victimization. *Social Science Computer Review*, *38*(2), 187–206.

Holtfreter, K., Reisig, M., & Pratt, T. (2008). Low self-control, routine activities, and fraud victimization. *Criminology*, *46*(1), 189-220.

Holtfreter, K., Reisig, M., Leeper Piquero, N., & Piquero, A. (2010). Low self-control and fraud: Offending, victimization, and their overlap. *Criminal Justice And Behavior*, *37*(2), 188-203.

Hosmer, D., & Lemeshow, S. (2013). *Applied Logistic Regression*(3th ed.). NY: Wiley.

Hsieh, M. L., & Wang, S. Y. K.(2018). Routine activities in a virtual space: A Taiwanese case of an ATM hacking spree. *International Journal of Cyber Criminology*, *12*(1), 333-352.

Ignatans, D., & Pease, K. (2015). On whom does the burden of crime fall now? Changes over time in counts and concentration. *International Review of Victimology*, *22*(1), 55–63.

Jensen, G., & Brownfield, D. (1986). Gender, lifestyles, and victimization: Beyond routine activity. *Violence And Victims*, *1*(2), 85-99.

Kanayama, T. (2017). Impact of cybercrime in Japan—Findings of cybercrime victimization survey. *Sociology Study*, *7*(6), 331-340.

Kigerl, A. (2012). Routine activity theory and the determinants of high cybercrime countries. *Social Science Computer Review*, *30*(4), 470-486.

Kutner, M. H., Nachtsheim, C. J., Neter, J., & Li, W. (2019). *Applied linear statistical models* (5th ed.). NY: Mcgraw-Hill.

LaGrange, T. C., & Silverman, R. A. (1999). Low self-control and opportunity: Testing the general theory of crime as an explanation for gender differences in delinquency. *Criminology*, *37*(1), 41-72.

Langton, L., Piquero, N., & Hollinger, R. (2006). An empirical test of the relationship between employee theft and low self-control. *Deviant Behavior*, *27*(5), 537-565.

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, *37*(3), 263–280.

Long, J. (2011). *Regression models for categorical and limited dependent variables*. Thousand Oaks (Calif.): Sage Publications.

Louderback, E. R., & Antonaccio, O. (2017). Exploring cognitive decision-making processes, computer-focused cyber deviance involvement and victimization. *Journal of Research in Crime and Delinquency*, *54*(5), 639–679.

Leukfeldt, E. (2014). Phishing for suitable targets in the Netherlands: Routine activity theory and phishing victimization. *Cyberpsychology, Behavior, And Social Networking*, *17*(8), 551-555.

Mertler, C., & Vannatta, R. (2016). *Advanced and Multivariate Statistical Methods: Practical Application and Interpretation* (6th ed.). Routledge: Taylor & Francis.

Mesch, G. S., & Dodel, M. (2018). Low self-control, information disclosure, and the risk of online fraud. *American Behavioral Scientist*, *62*(10), 1356–1371.

Moore, E., & Mills, M. (1990). The neglected victims and unexamined costs of white-collar crime. *Crime & Delinquency*, *36*(3), 408–418.

Miller, J. (2013). Individual offending, routine activities, and activity settings: Revisiting the routine activity theory of general deviance. *Journal of Research in Crime and Delinquency*, *50*(3), 390–416.

Negahdari, A. (2014). A study on gender differences influencing on online buying. *Management Science Letters*, 2203–2212.

Newman, G., & Clarke, R. (2003). *Superhighway Robbery: Preventing E-Commerce Crime.* UK: Willan Publishing.

Ngo,F.T., & Paternoster, R.(2011). Cybercrime victimization : An examination of individual and situational level factors, *International Journal of Cyber Criminology*, *5*(1), 773-793.

Nhan, J., Kinkade, P., & Burns, R. (2009). Finding a pot of gold at the end of an internet rainbow: Further examination of fraudulent email solicitation. *International Journal of Cyber Criminology*, *3*(1), 452–475.

Pavan Kumar, V. V., & Duffull, S. B. (2010). Evaluation of graphical diagnostics for assessing goodness of fit of logistic regression models. *Journal of Pharmacokinetics and Pharmacodynamics*, *38*(2), 205–222.

Pease, K., Ignatans, D., & Batty, L. (2018). Whatever happened to repeat victimisation?. *Crime Prevention and Community Safety*, *20*(4), 256-267.

Peker, A. (2017). An examination of the relationship between self-control and cyber victimization in adolescents. *Journal of Educational Research*, *17*(67), 1-15.

Pratt, T., Holtfreter, K., & Reisig, M. (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*, 87-116.

Reisig, M. D., Pratt, T. C., & Holtfreter, K. (2009). Perceived risk of internet theft victimization: Examining the effects of social vulnerability and financial impulsivity. *Criminal Justice and Behavior*, *36*(4), 369–384.

Reisig, M., & Golladay, K. (2019). Violent victimization and low self-control: The mediating effect of risky lifestyles. *Violence And Victims*, *34*(1), 157-174.

Ren, L., He, N. Phil, Zhao, R., & Zhang, H. (2017). Self-control, risky lifestyles, and victimization: A study with a sample of Chinese school youth. *Criminal Justice and Behavior*, *44*(5), 695–716.

Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being pursued online: Applying cyberlifestyle–Routine activities theory to cyberstalking victimization. *Criminal Justice and Behavior*, *38*(11), 1149–1169.

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. (2015). A routine activity perspective on online victimisation. *Journal of Financial Crime*, *22*(4), 396-411.

Savona, E., & Mignone, M. (2002). The fox and the hunters: How IC technologies change the crime race. *European Journal On Criminal Policy And Research*, *10*(1), 3-26.

Schreck, C. (1999). Criminal victimization and low self-control: An extension and test of a general theory of crime. *Justice Quarterly*, *16*(3), 633-654.

Schreck, C. J., Stewart, E. A., & Fisher, B. S. (2006). Self control, victimization, and the influence on risky lifestyles: A longitudinal analysis using panel data. *Journal of Quantitative Criminology*, *22*, 319−340.

Schreck, C. J., wright, R. A., & Miller, J. M. (2002). A study of individual and situational antecedents of violent victimization. *Justice Quarterly*, *19*, 159-180.

Smith, T. R. (2004). Low self-control, staged opportunity, and subsequent fraudulent behavior. *Criminal Justice and Behavior*, *31*(5), 542–563.

Sun, S., & Fan, X. (2018). Is there a gender difference in cyber-victimization? *Journal of Media Psychology*, *30*(3), 125-138.

Tittle, C. R., Ward, D. A., & Grasmick, H. G. (2003). Gender, age, and crime/deviance: A challenge to self-control theory. *Journal of Research in Crime and Delinquency*, *40*(4), 426–453.

Titus, R., Heinzelmann, F., & Boyle, J. (1995). Victimization of persons by fraud. *Crime & Delinquency*, *41*(1), 54-72.

Turanovic, J. J., & Pratt, T. C. (2014). "Can't stop, won't stop": Self-control, risky lifestyles, and repeat victimization. *Journal of Quantitative Criminology*, *30*, 29-56.

Turanovic, J. J., Reisig, M. D., & Pratt, T. C. (2015). Risky lifestyles, low self-control, and violent victimization across gendered pathways to crime. *Journal of Quantitative Criminology*, *31*, 183-206.

Turanovic, J. J., Pratt, T. C., & Piquero, A. R. (2018). Structural constraints, risky lifestyles, and repeat victimization. *Journal of Quantitative Criminology*, 34(1), 251–274

Vahdati, S., & Yasini, N. (2015). Factors affecting internet frauds in private sector: A case study in cyberspace surveillance and scam monitoring agency of Iran. *Computers In Human Behavior*, *51*, 180-187.

Van Wilsem, J. (2013). 'Bought it, but never got it' Assessing risk factors for online consumer fraud victimization. *European Sociological Review*, *29*(2), 168-178.

Van Wyk, J., & Mason, K. A. (2001). Investigating vulnerability and reporting behavior for consumer fraud victimization. *Journal of Contemporary Criminal Justice*, *17*(4), 328-345.

Wall, D. (2007). *Cybercrime:The transformation of crime in the information age.* Cambridge: Polity Press.

Ward, J. T., Fox, K. A., Tillyer, M. S., & Lane, J. (2014). Gender, low self-control, and violent victimization. *Deviant Behavior*, *36*(2), 113–129.

Welsh, B., & Farrington, D. (2012). *Preventing crime*. New York, NY: Springer New York.

Wilsem, J. van. (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.

Winkelmann, R. (1995). Duration dependence and dispersion in count-data models. *Journal of Business & Economic Statistics*, *13*(4), 467.

Whitty, M. (2019). Predicting susceptibility to cyber-fraud victimhood. *Journal of Financial Crime*, *26*(1), 277-292.

Wyk, J. V., & 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.

Yar, M. (2005). The Novelty of 'Cybercrime': An assessment in light of routine activity theory. *European Journal of Criminology*, *2*(4), 407–427.

Yu, S. (2014). Does low self-control explain voluntary disclosure of personal information on the internet? *Computers in Human Behavior*, *37*, 210–215.

Zaykowski, H., & Gunter, W. (2013). Gender differences in victimization risk: Exploring the role of deviant lifestyles. *Violence And Victims*, *28*(2), 341-356.

Zhang, L., Welte, J. W., & Wieczorek, W. F. (2001). Deviant lifestyle and crime victimization. *Journal of Criminal Justice*, *29*(2), 133–143.

網路部分

中央社(2018)。台灣網路犯罪受害者 去年逼近 4 百萬人。取自 https://www.digi.ey.gov.tw/News_Content.aspx?n=0A9FCBFE358FBE72&sms=C5D097AE49AFEE4C&s=04D61FE21633790C，瀏覽日期: 20181113。

中時電子報(2018)。2017 年台灣寬頻網路使用調查 TWNIC 公布：全國上網率達 80％。取自 https://www.chinatimes.com/newspapers/20170724000111-260208，瀏覽日期: 20181012。

內政統計通報(2019)。108 年第 22 週內政統計通報(女性被害概況)。取自 https://www.moi.gov.tw/files/site_node_file/8195/108%e5%b9%b4%e7%ac%ac22%e9%80%b1%e5%85%a7%e6%94%bf%e7%b5%b1%e8%a8%88%e9%80%9a%e5%a0%b1_%e5%a5%b3%e6%80%a7%e8%a2%ab%e5%ae%b3%e6%a6%82%e6%b3%81.pdf。瀏覽日期: 20190909。

內政部警政署全球資訊網(2020)。警政統計通報 109 年第 9 周(108 年網路犯罪概況)。取自 https://www.npa.gov.tw/NPAGip/wSite/ct?xItem=95821&ctNode=12594&mp=1，瀏覽日期: 20200412。

台網中心電子報（TWNIC E-PAPER）(2018)。網路釣魚詐欺與域名管理。取自 http://www.myhome.net.tw/2011_06/p02.htm，瀏覽日期: 20181111。

吳怡靜(2005)。台灣人，好騙歹教。取自 http://www.navy77.url.tw/analects/%E5%8F%B0%E7%81%A3%E4%BA%BA%EF%BC%8C%E5%A5%BD%E9%A8%99%E6%AD%B9%E6%95%99.htm，瀏覽日期: 20181112。

灼識投資諮詢有限公司（CIC）(2019)。CIC 灼識諮詢報告：台灣進入 C2C 行動電商時代。取自 http://www.cninsights.com/news/detail.aspx?tid=1601，瀏覽日期: 20191102。

科技新報(2019)。CIC 報告：台灣進入 C2C 行動電商時代。取自 http://technews.tw/2018/06/08/c2c-taiwan/，瀏覽日期: 20190404。

風傳媒(2018)。台灣最美的風景是「騙人」？詐欺案 5 年增 2 成，網購、電信佔 45%。取自 https://www.storm.mg/article/394572，瀏覽日期: 20181111。

風傳媒(2019)。年輕人騙年輕人！詐欺、被騙年齡層 都是 18~39 歲青壯人口。取自 https://www.storm.mg/article/394573?srcid=null，瀏覽日期: 20190210。

財團法人台灣網路資訊中心（TWNIC）(2018)。2017 年臺灣寬頻網路使用調查報告。取自 https://report.twnic.tw/2018/TWNIC_TaiwanInternetReport_2018_CH.pdf，瀏覽日期: 20181011。

國家通訊傳播委員會(2019)。2018 年寬頻使用調查結果摘要報告。取自 https://www.ncc.gov.tw/chinese/files/18030/3923_38847_180301_1.pdf，瀏覽日期: 20200220。

創市際市場研究顧問（Insight-Xplorer）(2020)。2019 年臺灣上網率追蹤調查。取自 https://www.ixresearch.com/reports/cati，瀏覽日期: 20200411。

資策會產業情報研究所（MIC）(2019)。日常購物頻率，網購已達 45%。取自 https://mic.iii.org.tw/IndustryObservations_PressRelease02.aspx?sqno=488

聯合晚報(2018)。男生真好騙？ 提醒你 LINE 上不要做這 3 件事。取自 https://theme.udn.com/theme/story/6774/3280302，瀏覽日期: 20181224。

聯合新聞網(2018)。台灣網路人口 1738 萬創新高！上網率已達 82.3%。取自 https://www.inside.com.tw/article/11569-taiwan-network-user，瀏覽日期: 20190409。

YAHOO!奇摩新聞(2018)。每 24.7 分鐘就有 1 起詐欺案 這 3 種人最常被騙。取自 https://tw.news.yahoo.com/%E6%AF%8F24-7%E5%88%86%E9%90%98%E5%B0%B1%E6%9C%891%E8%B5%B7%E8%A9%90%E6%AC%BA%E6%A1%88-%E9%80%993%E7%A8%AE%E4%BA%BA%E6%9C%80%E5%B8%B8%E8%A2%AB%E9%A8%99-025329877.html，瀏覽日期: 20191112。

YAHOO!奇摩新聞(2019)。詐騙猖獗，去年國人被騙逾 37 億元。取自 https://tw.news.yahoo.com/%E8%A9%90%E9%A8%99%E7%8C%96%E7%8D%

97-%E5%8E%BB%E5%B9%B4%E5%9C%8B%E4%BA%BA%E8%A2%AB%E9%A8%99%E9%80%BE37%E5%84%84%E5%85%83-101900215.html，瀏覽日期: 20191111。

Federal Trade Commission(2019)。The top frauds of 2018 。取自 https://www.consumer.ftc.gov/blog/2019/02/top-frauds-2018，瀏覽日期: 20190408。

International Business Machines Corporation(2006)。取自 https://www.ibm.com/investor/att/pdf/IBM_Annual_Report_2006.pdf，瀏覽日期: 20181031。

Internet Crime Complaint Center(2020)。2019 Internet Fraud –Crime report. Washington, The US Internet Crime Complaint Center。取自 https://pdf.ic3.gov/2019_IC3Report.pdf，瀏覽日期: 20200413。

Norton(2018)。Cybercrime Report: The Human Impact。取自 https://www.symantec.com/content/en/us/home_homeoffice/media/pdf/cybercrime_report/Norton_USA-Human%20Impact-A4_Aug4-2.pdf，瀏覽日期: 20181115。

Pew Research Center Internet & Technology(2018)。About a quarter of U.S. adults say they are ‘almost constantly’ online。取自 http://www.pewresearch.org/fact-tank/2018/03/14/about-a-quarter-of-americans-report-going-online-almost-constantly/，瀏覽日期: 20181026。

Pew Research Center Internet & Technology(2020)。Internet/Broadband Fact Sheet。取自 https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120，瀏覽日期: 20200412。

Pew Research Center Internet & Technology(2019)。10% of Americans don’t use the internet. Who are they?。取自 https://www.pewresearch.org/fact-tank/2019/04/22/some-americans-dont-use-the-internet-who-are-they/，瀏覽日期: 20190913。

附錄 網路生活型態問卷

親愛的網路使用者您好：

首先，感謝您於百忙之中，撥冗填寫本問卷。本研究之目的在於了解網路使用者日常生活中從事網路行為的型態。為了瞭解您的日常網路使用情形，特別進行這項調查，希望能獲得您寶貴的意見，以作為未來提供政府建構更完善網路政策之參考。

這是一份問卷調查，每個人有不同的狀況，所以沒有「對」與「錯」的答案，您只需要回答符合個人實際狀況及自己想法的答案，在方格□內打「√」，或是在橫線上____作答即可。

本項調查採用「**不記名**」、「**不編號**」的匿名方式，亦即您不需留下姓名或稱謂，問卷調查的結果僅作為學術研究整體分析使用，不會牽涉到個人的權益，**研究者將遵守個人資料保護法相關規定，盡力維護您的隱私及善盡保密責任，對於您所填答的內容絕對保密，希望您能放心地作答。**此外，為確保您的受訪權益，在填答過程中若您認為有任何不舒服或不想填答的狀況時，您不需有任何理由，可隨時選擇終止填答。

您的經驗和意見對於我們了解網路使用者的問題，有非常大的幫助；問卷的每個部分均有填答方式說明，請您詳細閱讀填答說明後，盡可能地回答每個問題。最後，非常感謝您的協助與合作！

敬祝　闔家平安、身體健康

中央警察大學犯罪防治研究所
指導教授：賴擁連 博士
研 究 生：方呈祥 敬上
聯絡電話：

一、以下各題是有關您對自己的看法或生活經驗，請您就個人實際狀況，選擇最符合現況的選項，在適當的□內打 √ 。

1、一般而言，您平均每次上網時間約有：

□(1)不足 1 小時　　□(2)1 小時至 3 小時以內

□(3)3 小時至 5 小時以內　　□(4)5 小時至 7 小時以內

□(5)7 小時至 9 小時以內　　□(6)9 小時以上

2、您平均每週上網的次數：

□(1)少於 1 次　□(2)1~3 次　□(3)4~6 次　□(4)7~9 次　□(5)10 次以上

3、星期一至星期五您最常上網的時段大約在：

□(1)08：01 至 12：00　□(2)12：01 至 16：00　□(3)16：01 至 20：00

□(4)20：01 至 00：00　□(5)00：01 至 04：00　□(6)04：01 至 08：00

4、星期六至星期日您最常上網的時段大約在：

□(1)08：01 至 12：00　□(2)12：01 至 16：00　□(3)16：01 至 20：00

□(4)20：01 至 00：00　□(5)00：01 至 04：00　□(6)04：01 至 08：00

5、您接觸網路的時間大約多久：

□(1)1 年未滿　□(2)1 年以上至 2 年未滿　□(3)2 年以上至 3 年未滿

□(4)3 年以上至 5 年未滿　□(5)5 年以上至 10 年未滿　□(6)10 年以上

6、您最常使用網路的地點是在:（可複選）

□(1)在家中(租屋處)上網。　□(2)在學校(含圖書館/書局)上網。

□(3)在朋友(或同學/同事)家中上網。　□(4)在網咖上網。

□(5)在公共場所上網。(如：捷運站、火車站、機場…)　□(6) 在工作場所上網。

7、您最常因為下列何種原因而使用網路:（可複選）

□(1)抒發情緒。　□(2)搜尋資料（如功課/工作需要）。

□(3)買賣東西。　□(4)交友聊天。

□(5)休閒娛樂（如線上遊戲）。　□(6)找尋新奇的事物。

□(7)收發信件。

□(8)尋找網路戀情或滿足性幻想(如網愛、瀏覽情色網站等)。

9、下列問題是有關您最近一年內(2018 年 1 月 1 日至 2018 年 12 月 31 日期間)使用網路的情形，請您就個人實際狀況，選擇最符合現況的選項，在適當的□內打 √ 。

問 卷 內 容	經常	偶爾	很少	從未
(1)在過去1年內，您經常使用即時通訊軟體(LINE、微信或WECHAT)與他人溝通互動。				
(2)在過去1年內，您經常使用網路社群媒體(FB或IG)。				
(3)在過去1年內，您經常從事網路購物行為。				
(4)在過去1年內，您經常在網路上瀏覽或觀看新聞。				
(5)在過去1年內，當您無聊時經常花時間上網。				
(6)在過去1年內，您經常檢查您的電子郵件。				
(7)在過去1年內，您經常寄送電子郵件。				
(8)在過去1年內，您經常利用網路來進行檔案傳輸。				
(9)在過去1年內，您經常利用網路來搜尋資料。				
(10)在過去1年內，您經常在網路上下載資料。				
(11)在過去1年內，您經常瀏覽色情網站。				
(12)在過去1年內，您經常從網站上下載免費遊戲。				
(13)在過去1年內，您經常從網站上下載免費音樂。				
(14)在過去1年內，您經常從網站上下載免費電影。				
(15)在過去1年內，您經常從網站上下載不明來源的檔案。				
(16)在過去1年內，您經常點擊不明來源的電子郵件。				
(17)在過去1年內，您經常點擊不明來源電子郵件的附件檔案。				
(18)在過去1年內，您經常點擊不明來源電子郵件的相關網頁連結。				
(19)在過去1年內，您經常點擊經由即時通訊軟體所接收到的未知來源檔案或附件。				
(20)在過去1年內，您經常寄送信件至不明來源的電子郵件。				

二、以下是有關您在使用網路時的經驗、情境與想法，請您就個人實際狀況，選擇與您情況最相符的選項，在適當的□內打 √ 。

問 卷 內 容	經常	偶爾	很少	從未
1、您上網時，父親(或母親)會注意您的網路使用情形。				
2、您上網時，兄弟姐妹會在您的身邊。				
3、您上網時，同學(或同事)會在您身邊。				
4、您上網時，同學以外的朋友會在您身邊。				
5、您上網時，學校師長(或工作時上司、長輩)會在您身邊。				
6、您的電腦有安裝防毒軟體。				
7、您的電腦有定期更新防毒軟體。				
8、您對於不同的網路帳號會使用不同的密碼。				
9、您會定期更改個人網路帳號的密碼。				
10、您會注意到在網路的空間中該留下何種個人資訊。				
11、您曾經在網路上看到線上賭博或下注賭盤的訊息。				
12、您曾經在網路上看到網路援交或一夜情的訊息。				
13、您曾經在網路上看到買賣違禁物品的訊息。				
14、您曾經在網路上看到買賣盜版軟體的訊息。				
15、上網時，您曾經想利用網路以干擾別人使用網路。				
16、您曾經想在不知情或不允許查看他人訊息或文件的情況下使用他人的帳戶或文件。				
17、您曾經想在未經所有者知情或許可的情況下，在其電腦中增加、刪除、更改或列印任何資訊。				
18、您曾經想利用網路瀏覽色情網站或從事網路援交。				
19、您曾經想利用網路詐騙別人財物。				
20、您曾經想利用網路從事網路賭博。				
21、您曾經想利用網路從事非法交易（如買賣贓物）。				

三、下面這些題目是想了解有關您日常生活中使用網路的情形，請選擇與您情況相符的答案選項，在適當的□內打 √ 。

問 卷 內 容	非常同意	同意	不同意	非常不同意
1 、您經常在不考慮所有選擇的情況下採取行動。…				
2、有時您無法阻止自己做某事，即使您知道這是錯的。				
3、您會因為眼前的立即快樂而較少考慮以後才會發生的事				
4、生活中做些簡單的事帶給您無窮的樂趣。……				
5、您會做些有點冒險的事情來考驗一下自己。……				
6、刺激跟冒險對您來說比安全更重要。……				
7、有時候您會覺得做些惹麻煩的事反而刺激。……				
8、您偶爾會進行風險性的金融投資。……				
9、只要有獲得報酬的機會，您就會進行投資行為。				
10、您會逃避您認為是比較困難的事情。……				
11、您不喜歡艱鉅且挑戰能力極限的任務。……..				
12、您會關心眼前即將發生的事，比較少考慮以後才會發生的事。……..				

四、下面這些題目是想了解您最近一年內(2018年1月1日至2018年12月31日期間)是否曾經有網路詐欺犯罪被害的經驗，請選擇與您情況相符的答案選項，在適當的□內打 √ 。

1、請問您**最近一年(2018 年 1 月 1 日至 2018 年 12 月 31 日期間)**是否曾經有網路詐欺犯罪被害的經驗：

□(1)有(共_____次)　　□(2)沒有(請跳答第五部分)

2、請問您**最近一次**所遭遇的網路詐欺犯罪被害型態為何?

□(1)網路購物詐欺(自己是買方)　　□(2)網路拍賣詐欺(自己是賣方)

□(3)商業金融詐欺　　□(4)網路遊戲詐欺

□(5)網路交友詐欺(如：援交)　　□(6)色情網站詐欺

□(7)網路賭博詐欺　　□(8)其他(請說明：_____)

3、請問您**最近一次**網路詐欺犯罪被害損失之總金額為多少：

□(1)500元以下　　□(2)501~1000元

□(3)1001~5000元　　□(4)5001~1萬元

□(5)1萬以上，未滿 5萬元　　□(6)5萬以上，未滿 10萬元

□(7)10萬元以上，未滿 15萬元　　□(8)15萬元以上，未滿 20萬元

□(9)20萬元以上

4.請問您**最近一次**網路詐欺犯罪被害的交易方式為何：

□(1)現金交付　□(2)ATM轉帳　□(3)金融機構匯款(如：銀行、郵局)

□(4)網路銀行付款　　□(5)其他(請說明：　　)

5、請問您**最近一次**所遭遇的網路詐欺犯罪被害，您跟加害者的關係為何：

□(1)親人　□(2)同學　□(3)朋友或同事　□(4)陌生人

□(5)其他(請說明：　　)

6、請問您**最近一次**所遭遇的網路詐欺犯罪被害，是否與加害者互動?

□(1) 是(請繼續回答第 7 題)　　□(2) 否(請跳答第 8 題)

7、請問您**最近一次**所遭遇的網路詐欺犯罪被害，係透過何種管道與加害者互動?

□(1)拍賣網站　□(2)網路電話　□(3)線上遊戲

□(4)即時通訊軟體(SKYPE、QQ、MSN 、LINE、微信或即時通)

□(5)網路社群網站(FACEBOOK、INSTAGRAM)　□(6)其他(請說明：　　)

8、請問您**最近一次**所遭遇的網路詐欺犯罪被害，係如何得知自己被害：
□(1)自己察覺　□(2)警方通知　□(3)朋友或同事發現　□(4)親人發現
□(5)其他(請說明：　　)

9、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?
□(1)1 日以內　□(2) 1～3 天　□(3) 4～6 天　□(4)7～14 天
□(5)14～30 天　□(9) 30 天以上

10、請問您**最近一次**所遭遇的網路詐欺犯罪被害，當您發現自己被害時，您是否有向官方機構(如:警察單位、165 專線)報案?
□(1) 有(請繼續回答第 11 題)　□(2) 無(請跳答第 12 題)

11、請問您**最近一次**所遭遇的網路詐欺犯罪被害，向警察報案的方式為何？
□(1)電話報案　□(2)網路報案　□(3)傳真報案　□(4)郵寄方式報案
□(5)親自到警察單位報案　□(6)其他方式（請說明：　　）

12、請問您**最近一次**所遭遇的網路詐欺犯罪被害，未向官方機構報案的原因為何?（可複選）
□(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(請說明：　　)

13、請問您**最近一次**所遭遇的網路詐欺犯罪被害，當您發現自己被害時，您所採取的其他應對措施為何：(可複選)
□(1)告知親人、朋友　□(2)向網路賣家查詢　□(3)網路申訴
□(4)其他(請說明：　　)

14、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：(可複選)
□(1)自身疏忽　□(2)貪小便宜　□(3)過於相信別人
□(4)自己太笨　□(5)產品很吸引人　□(6)缺乏自我保護常識
□(7)不清楚　□(8)運氣不好　□(9)其他(請說明：　)

五、以下是有關您的個人資料，請您就現在的實際狀況，選擇最符合現況的選項，在適當的□內打√。

1、您的性別是：
□(1) 男。 □(2) 女。

2、您的年齡是：
□(1) 18 歲以下 □(2) 19-29 歲 □(3) 30-39 歲 □(4) 40-49 歲
□(5) 50-59 歲 □(6) 60 歲以上。

3、您目前的職業為何？
□ (1)未就業(含退休) □ (2)學生 □ (3)軍警公教人員
□ (4)從事家庭管理 □ (5)服務、事務工作人員
□ (6)技術員及助理專業人員 □ (7)民意代表、行政主管及經理人員
□ (8)其他(請說明：)。

4、您目前每月總收入約新台幣：
□ (1)未滿 1 萬元 □ (2)1 萬以上，3 萬未滿
□ (3)3 萬以上，6 萬未滿 □ (4)6 萬以上，9 萬未滿
□ (5)9 萬以上，12 萬未滿 □ (6)12 萬以上，15 萬未滿
□ (7)15 萬元以上

5、您的教育程度：
□(1) 國小(肄) 畢業 □(2) 國中(肄) 畢業
□(3) 高中、高職(肄) 畢業 □(4) 專科、大學(肄) 畢業
□(5) 研究所(肄) 畢業以上 □(6) 其他(請說明：)。

6、您目前的婚姻狀況：
□(1) 單身 □(2) 未婚(非單身) □(3) 已婚(含同居)
□(4) 離婚(含分居) □(5) 喪偶 □(6) 再婚
□(7) 其他(請說明：)。

非常感謝您用心填寫這份問卷

請您從頭到尾再看一遍有沒有漏答的地方！ 祝福您平安快樂！