專論

我國網路詐欺被害風險實證分析：心理特質與網路風險暴露之雙重脆弱性[1]

葉碧翠[*]、陳玉書[**]、蔡田木[***]、賴擁連[****]

要　目

DOI：10.6460/CPCP.202608_(44).0003

[1] 本文所採用之量化資料，係取自賴擁連等人於 2023 年執行之法務部司法官學院委託研究計畫「我國網路詐欺被害調查與防制研究」（計畫編號：112-A-002）。特此致謝研究團隊成員之貢獻與委託單位之經費支持。本文內容與觀點僅屬作者個人立場，與委託機關無涉。

[*] 葉碧翠，中央警察大學犯罪防治學系副教授。
[**] 陳玉書，中央警察大學犯罪防治學系副教授（退休）。
[***] 蔡田木，中央警察大學代理副校長暨犯罪防治學系教授。
[****] 賴擁連（通訊作者），國立中正大學犯罪防治系教授。
Email：crmlyl@ccu.edu.tw

摘要

本研究針對我國網路詐欺被害風險進行實證分析，旨在探討其類型、特性與影響因素。研究採用全國性網路問卷調查，回收有效樣本 1,146 份，區分為 564 位具被害經驗者與 582 位無被害經驗者進行比較。主要分析變項涵蓋人口特性（性別、年齡、收入、教育程度、職業、居住地）、心理特質（偏差價值觀、網路依賴、低自我控制）與網路風險暴露（風險接觸、防護監控、高誘因涉險傾向），以檢驗其對詐欺被害風險之影響。結果顯示，男性、40 歲以下、中低收入與教育程度偏低者之被害風險較高，城鄉差異則不具顯著性。在心理特質與網路風險暴露方面，除防護監控外，其餘變項於被害組均顯著高於無被害組，顯示心理傾向與涉險行為在詐欺風險中扮演關鍵角色。邏輯斯迴歸結果亦指出，衝動性、心理依賴、網路誘因吸引與遊樂動機為主要預測因子。綜合分析結果，本文建議應強化高風險心理特質與涉險行為之早期識別機制，並推動具預警功能之防詐教育策略，以提升防制政策之精準度與介入成效。

關鍵字：網路詐欺、被害風險、實證分析、心理特質、網路風險暴露

Empirical Analysis of Online Fraud Victimization Risk in Taiwan: A Dual Vulnerability Model of Psychological Traits and Online Risk Exposure

Pi-Tsui Ye*, Yu-Shu Chen**, Tien-Mu Tsai***, Yung-Lien Lai****

Abstract

This study conducts an empirical analysis of online fraud victimization risk in Taiwan, aiming to explore its types, characteristics, and influencing factors. A nationwide online survey was conducted, yielding 1,146 valid responses, which were divided into 564 participants with victimization experience and 582 participants without such experience for comparative analysis. The main analytical variables encompassed demographic characteristics (gender, age, income, education, occupation, residence), psychological traits (deviant values, internet dependency, low self-control), and online risk exposure (risk contact, defensive monitoring, high-incentive risk-taking propensity) to examine their impact on fraud victimization risk. The results revealed that males, individuals under 40 years of age, those with low-to-moderate income, and those with lower educational attainment exhibited higher victimization risks, while urban-rural differences showed no significant association. Regarding psychological traits and online risk exposure, all variables except defensive monitoring were significantly higher in the victimized group compared to the non-victimized group, indicating that psychological predispositions and risk-taking behaviors play crucial roles in fraud vulnerability. Logistic regression analysis further identified impulsivity, psychological dependency, online incentive attraction, and recreational motivation as primary predictive factors. Based on the comprehensive analysis results, this study recommends strengthening early identification mechanisms for high-risk psychological traits and risk-taking behaviors and promoting fraud prevention education strategies with early warning functions to enhance the precision and intervention effectiveness of prevention policies.

Keywords: Online fraud, victimization risk, empirical analysis, psychological traits, online risk exposure

* Associate Professor, Department of Crime Prevention and Correction, Central Police University.

** Associate Professor (Retired), Department of Crime Prevention and Correction, Central Police University.

*** Acting Vice President and Professor, Department of Crime Prevention and Correction, Central Police University.

**** Corresponding author. Professor, Department of Criminology, National Chung Cheng University. E-mail: crmlyl@ccu.edu.tw

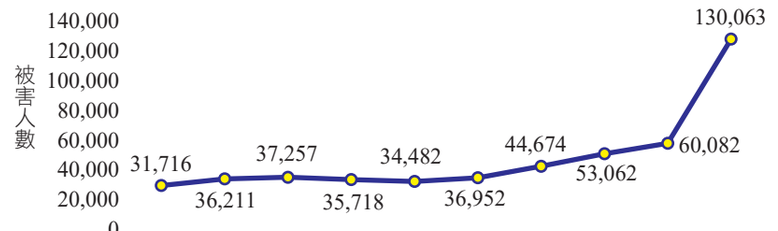
壹、緒論

一、研究背景與重要性

根據內政部警政署統計，自 2015 年以來，我國詐欺案件被害人數呈現持續上升趨勢，從 2015 年之 31,716 人增至 2024 年之 130,063 人，增加 98,347 人，約為原數之 4.1 倍（見圖 1）。自 2023 年 9 月起，警政署改以「每一被害人計一發生數」方式統計，取代以往「一案一發生數」的模式，使數據更能反映實際治安情況。此一統計調整顯示，網路詐欺事件不僅持續攀升，且已普遍滲透至日常生活。隨著 3C 科技與網路應用普及，傳統犯罪樣態逐漸虛擬化，行為地點從實體空間轉移至網路環境中（Zhang & Ye, 2022；陳宗義、沈筱娟，2015；曾百川，2006）。在此脈絡下，如何有效遏止詐欺行為、降低被害風險，並建構具預防功能之防制體系，已成為當前刑事政策之核心課題。

圖 1

警政署 2015 年至 2024 年詐欺被害人數統計分析



	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
被害人數	31,716	36,211	37,257	35,718	34,482	36,952	44,674	53,062	60,082	130,063

資料來源：內政部警政署統計查詢網（https://ba.npa.gov.tw/statis/webMain.aspx?k=defjsp）。

目前社會對網路詐欺的理解多仰賴警政機關的統計資料，此類資料雖能反映整體趨勢，但仍存在犯罪黑數與紀錄偏誤的問題（梁馨科等人，2009；蔡德輝、楊士隆，2023），難以全面掌握實際被害狀況。因此，針對民眾實際被害經驗進行調查，有助於補足官方統計的盲點，進一步掌握網路詐欺的被害歷程與風險因素。

過往研究多聚焦於犯罪者、法律與偵查技術等面向（孔令維，2018；張志盛，2022；梁馨科等人，2009），對於被害者特性及其在虛擬空間中的行為模式探討相對不足，且樣本多限於青少年與學生族群（Qu et al., 2024；石泱、王乃琳，2021）。為補足此缺口，本研究透過大樣本問卷調查，蒐集性別、年齡、職業、教育程度與被害經驗等資料，分析其與網路風險暴露、心理特質的關聯，以識別導致被害的關鍵因子。

相關研究亦指出，人口特性與情境機會密切相關，且對被害損失有顯著影響（陳玉書等人，2020），而偏差行為與被害經驗亦常交織出現（Burden, 2025; Choi & Lee, 2017）。因此，建立有效的防詐策略，需從實證資料出發，分析本地網路詐欺的實際樣態與高風險因子，進而提出具體預防建議，作為司法實務與政策制定的依據。

二、研究目的與問題

本研究旨在建構一套針對網路詐欺被害風險之整合性分析架構，並以實證調查方式檢驗其影響因素。透過結合人口特性、心理特質與網路風險暴露等三大構面，探討不同構面如何共同影響個體的網路詐欺被害風險。具體目的如下：

（一）**瞭解網路詐欺被害樣態：**分析受訪者在過去一年中是否曾遭遇詐欺事件，及其被害類型與重複被害次數之分布情形。

（二）**辨識潛在風險因子：**針對人口結構（性別、年齡、職業等）、心理特質（偏差價值觀、**網路依賴**、低自我控制）與網路風險暴露（風險接觸、防護監控、高誘因涉險傾向）等，評估其與網路詐欺被害之關聯。

（三）**驗證理論架構之解釋力：**採用二元邏輯斯迴歸（binary logistic regression）進行統計分析，檢視各構面變項對有無網路詐欺被害機率之預測效果，評估整體分析模型之適切性。

（四）**提出防制建議：**依據實證結果，提出針對高風險群體與重複被害者之防詐教育與政策建議，作為未來社會預防策略與風險溝通機制設計之參考依據。

貳、文獻探討

一、網路詐欺被害者人口特性

根據警政署（2025）統計，男性被害人數略高於女性，主要被害類型集中於投資型詐欺，而女性則以解除分期付款詐欺為主。多數國內外實證研究亦指出，男性之網路詐欺被害率較高（方呈祥，2020；Buse et al., 2024; Izuakor, 2021），惟在特定詐欺型態中女性被害比例亦有上升（Whitty, 2020）。亦有部分研究未發現性別差異具統計意義，主張性別非獨立預測因子（Leukfeldt & Yar, 2016; Louderback & Antonaccio, 2017）。

Havers 等人（2024）針對英國網路詐欺的研究發現，雖然年輕族群的被害率較高，但年長者在網路詐欺中往往面臨更嚴重的後果，包括重複被害與財務損失，呈現出「發生率高峰在年輕、嚴重度高峰在高齡」的雙峰風險構型。其中，高齡者在投資詐欺上的被害風險尤為突出（Whitty, 2020）。此結果與 Titus 和 Gover（2001）等研究一致，顯示年輕人因網路參與度高、風險接觸多樣而成為高風險群體；相對地，年長者則因對數位金融詐術的辨識能力不足，同樣處於高度風險之中。

職業與收入對網路詐欺風險亦有影響。部分研究發現，學生、服務業及無穩定工作者被害率較高（方呈祥，2020；陳玉書等人，2020）；另有研究指出，月收入低於新臺幣 4 萬元者為高風險群（蔡田木等人，2009；廖釗頡，2010），但亦有研究指出收入高低與被害機率無顯著關聯（Leukfeldt & Yar, 2016; Van Wyk & Mason, 2001）。

教育程度與被害風險的關聯亦具爭議。部分研究認為低學歷者風險較高（葉雲宏，2007；Whitty, 2020），但 Titus 與 Gover（2001）則發現高學歷者因使用網路頻率與功能多元，亦可能增加暴露風險。綜合而言，人口特性與詐欺風險間非線性關係明顯，並受限於類型差異、調查樣本與變項操作方式，研究結果呈多元化與區域性差異。

二、心理特質與網路詐欺被害

本研究聚焦於心理特質與網路詐欺被害風險的關聯性，三個核心變項包括偏差價值觀、網路依賴與低自我控制。首先，相關研究指出偏差行為與被害風險往往呈現重疊現象。「對等團體」（equivalent group）理論認為，加害者與被害者經常來自相似生活型態的群體，兩者在行為與動機上難以明確區隔（Lauritsen et al., 1991; Jennings et al., 2012）。進一步而言，青少年與成人的網路偏差行為皆被證實與被害經驗呈顯著正相關（簡鳳容，2018）。此外，Modic 和 Lea（2012）強調個人特質的重要性，指出具備特定人格特質者本身即為高風險目標，凸顯偏差價值觀對於被害脆弱性的預測作用。

其次，網路依賴亦被視為一項關鍵風險因子。多項研究發現，網路依賴與網路詐欺被害呈正向關聯，尤其是青少年網路霸凌與色情誘騙等案例中，被害者的上網時間與成癮傾向明顯偏高（周愫嫻，2014）。此外，網路依賴亦與逃避現實壓力、心理困擾及風險辨識能力低落密切相關（Mihajlov & Vejmelka, 2017），使個體長時間暴露於高風險互動情境中，增加被詐誘因。

再者，低自我控制亦被證實為詐欺被害的重要心理預測因子。Gottfredson 和 Hirschi（1990）指出，低自我控制者傾向衝動、尋求刺激且缺乏長期目標。Pratt 等人（2014）透過後設分析指出，低自我控制與非接觸型被害（如詐欺）之間具穩定相關性；Holtfreter 等人（2008）亦強調，詐欺犯罪常依賴被害人配合，因此自我控制能力低落者較難抵抗誘騙情境。Schreck（1999）進一步指出，自我控制能力不足會降低風險警覺與行為抑制，使其更易成為目標。然而，亦有學者指出，在控制網路使用頻率與消費行為後，自我控制與特定詐欺型態（如信用卡詐欺）之關聯性不顯著（Holt et al., 2012），顯示此變項在不同詐欺樣態間可能具異質性解釋效果。

綜合而言，心理特質構面中的偏差價值觀、網路依賴與低自我控制，皆與網路詐欺被害風險密切相關。為深入探究此關聯，本研究納入相關變項進行模型建構與驗證，補足國內此類實證探討之不足。

三、網路風險暴露對詐欺被害風險之影響

根據 Felson 和 Clarke（1998）所提出的日常活動理論，被害風險與情境機會密切相關，網路使用者若長時間暴露於網路活動，接觸潛在加害者的機率也相對提高。多數研究指出，上網時間長（Pratt et al., 2014）、頻繁網購（Reyns, 2013）、常透過社群工具互動（Leukfeldt & Yar, 2016），皆與網路詐欺被害風險呈正相關。這顯示網路風險暴露與詐欺風險具有可預測性。

另有研究強調，若使用者具備良好的數位防護與監控意識（如避免點擊陌生連結、定期更新系統等），可有效降低風險（Choi, 2008；廖釗頡，2010；簡鳳容，2018）。然而，部分實證研究認為單純提升監控能力未必能有效抑制詐欺被害的發生（Ngo & Paternoster, 2011；李雅惠等人，2024），顯示「監控作用」的影響仍存在爭議。

此外，生活方式暴露理論亦指出，接觸越多詐欺誘因（如高報酬投資、虛假交友、抽獎訊息）將增加個人暴露機會與偏差價值觀，進而提高被害風險（Bossler & Holt, 2009；簡鳳容，2018）。研究亦顯示，被詐欺訊息吸引的個體往往具備高風險特質，容易成為詐欺者的鎖定對象（Holtfreter et al., 2008；李雅惠等人，2024）。

綜合上述，網路詐欺被害並非偶然事件，而是個人網路使用模式、資訊防護能力與情境接觸誘因交織下的結果。未來防詐策略應聚焦於高暴露者之數位風險教育與誘因辨識強化，提升整體抗詐意識。

四、從心理特質到網路風險暴露：雙重脆弱性如何形塑網路詐欺被害

近年來，學術界日益關注網路詐欺的被害機制，其中尤以「生活方式－日常活動理論」（Lifestyle-Routine Activities Theory, L-RAT）最常被運用來解釋個體暴露於風險中的結構性條件。該理論係由日常活動理論（Routine Activities Theory, RAT）與生活方式理論（Lifestyle Exposure Theory, LET）整合而成，主張犯罪的發生仰賴三項條件的同時存在：潛在的犯罪者、適合的目標，以及缺乏足夠的監控或防衛措施（Cohen & Felson, 1979）。當個人之生活型態與活動模式使其頻繁接觸具有犯意之對象，且自身特質或環境配置使其成為低防衛、高價值的潛在標的時，便會顯著提升其面臨被害的可能性（Herrero et al., 2021）。

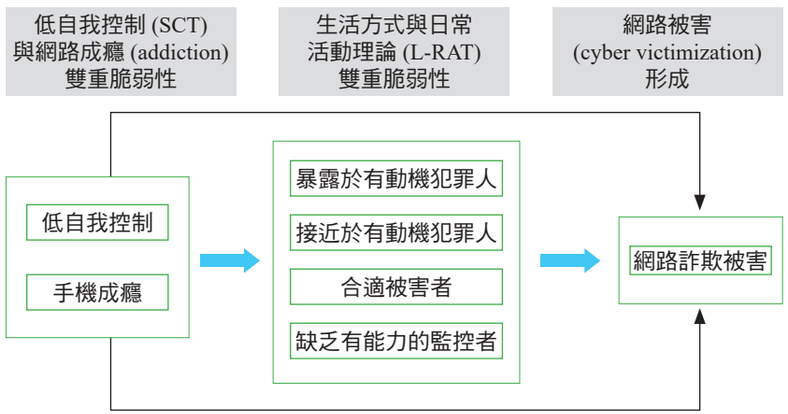
相關研究成果顯示，不論在實體或虛擬空間，L-RAT 架構皆能有效說明詐欺等機會型犯罪的生成條件與風險分布（方呈祥，2020；陳玉書等人，2020；Herrero et al., 2021; Leukfeldt & Yar, 2016）。尤其在網路場域中，使用者的行為選擇、接觸路徑與監護機制的有無，更凸顯風險與機會的交織性與動態性，進一步形塑其被害脆弱性。

Pratt 等人（2014）指出，縱使控制網路使用行為，自我控制能力仍對是否成為被害者具有顯著影響。自我控制力低者往往選擇風險較高的生活方式，增加暴露於網路詐欺等風險的機率。許多研究證實，自我控制理論可有效解釋詐欺等非接觸式被害（葉雲宏，2007；陳玉書等人，2020；

Holtfreter et al., 2008）。生活方式與日常活動理論（L-RAT）也已納入自我控制觀點，說明部分使用者因衝動性、短視等特質，導致高風險的網路行為（Gottfredson & Hirschi, 1990; Hirschi & Gottfredson, 1993; Schreck, 1999）。例如 Herrero 等人（2021）提出「網路被害的雙重脆弱性模型」（Dual Vulnerability Model），整合 L-RAT 與自我控制理論，認為網路依賴者因心理特質與使用習慣雙重因素，更易暴露於網路詐欺情境。如圖 2 中的模型反映網路詐欺被害者的雙重脆弱性形成過程。

圖 2

Herrero 等人（2021）網路犯罪被害的雙重脆弱性模型圖



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

此外，Akdemir 和 Lawless（2020）實證分析 L-RAT 對網路詐欺的適用性，發現除了個人特質，電腦使用習慣與外部資訊洩露等結構性因素，亦會提升被害風險，顯示網路詐欺風險的生成，同時受個人與社會環境交互作用所影響。因此，生活方式與日常活動理論（L-RAT）適合解釋網路上的被害事件發生及預防措施。

五、網路詐欺被害風險模型之建構

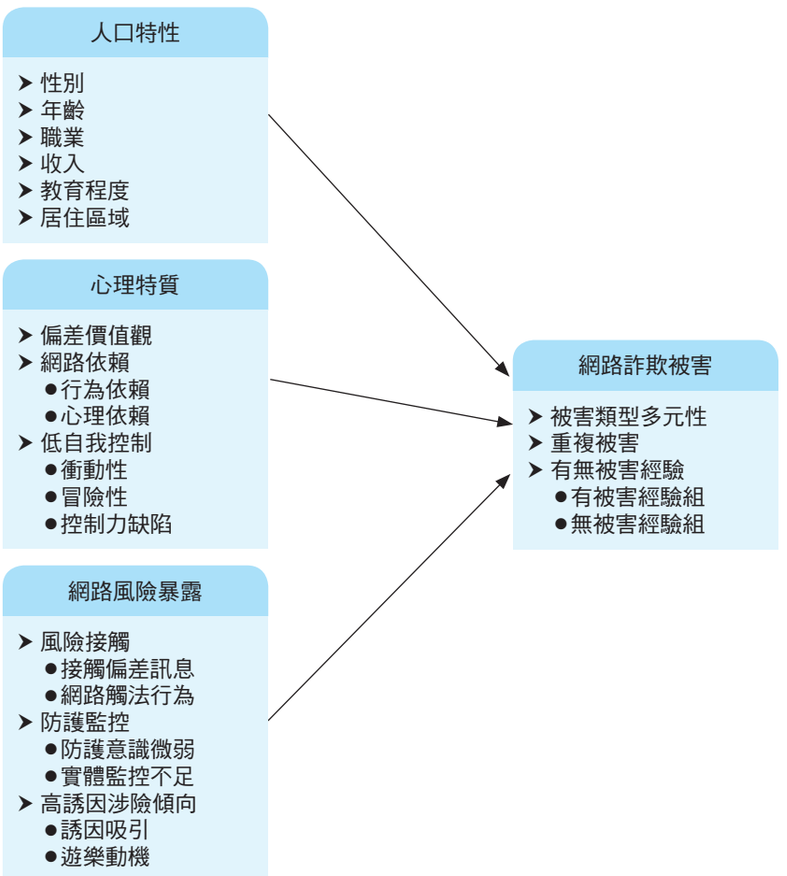
本研究旨在建構一套整合性之網路詐欺被害風險分析架構，檢驗人口特性、心理特質與網路風險暴露等因素對被害發生的影響。理論上，本研究以生活方式－日常活動理論（L-RAT）為基礎，說明個體因日常習慣與網路使用行為不同，導致其暴露於高風險情境而成為合適標的；並輔以自我控制理論（SCT），從衝動性、冒險性與控制力缺陷等心理特質，解釋個體在網路環境中做出高風險選擇的可能性。

本研究從三個面向探討網路詐欺的被害成因：第一，人口特性（性別、年齡、職業、收入、教育程度、居住地）影響個體接觸詐欺風險的機會與脆弱程度；第二，心理特質（偏差價值觀、網路依賴、低自我控制）與風險傾向高度相關，可能使其難以辨識詐欺陷阱或提高涉險機率；第三，網路風險暴露（風險接觸、防護監控、高誘因涉險傾向）則反映個體是否容易成為網路詐欺攻擊的目標。由圖 3 可見，當個體同時具備高風險的人口特性與心理特質，且其網路風險暴露程度較高時，遭遇網路詐欺被害的機率亦會隨之增加。

本模型可作為辨識潛在高風險族群的依據，並有助於規劃防詐策略與預防介入措施。

圖 3

本研究架構圖



參、研究設計與實施

一、研究方法與執行過程

本研究旨在比較有無網路詐欺被害經驗者的特性與影響因素，依據相關理論與文獻、官方資料與研究者實務經驗，設計「網路詐欺被害調查問卷」，並透過 SurveyCake 平臺進行線上問卷調查。問卷內容涵蓋人口特性、心理特質、網路風險暴露以及有無詐欺被害經驗等四大面向，填答時間約為 10 分鐘。調查對象為年滿 18 歲、居住於臺灣地區的網路使用者。本調查設計無記名制，填答前須詳閱知情同意書。完成問卷者可自願填寫聯絡方式，前 1,200 名有效填答者可獲 100 元超商電子禮券，經審核後由研究團隊透過 E-mail 或簡訊發送。

問卷設計前，研究團隊曾召開學者焦點座談，並進行 96 份前測，依據審查建議進行修訂後，方底定正式版本。調查期間自 2023 年 5 月 15 日至 7 月 14 日，問卷公告於法務部司法官學院官網，並透過刑事警察局協助，於 165 防詐網、Line 官方帳號及各派出所提供報案民眾填答資訊，以強化樣本多元性與代表性。

二、研究樣本

本研究參考財團法人臺灣網路資訊中心（2023）所發布之《2023 年臺灣網路報告》，依其網路使用人口結構進行目的抽樣（purposive sampling），並以性別與年齡分布作為主要控制條件，以確保樣本在基本人口特性上與實際網路

使用者群體相近。另為確保有足夠案例檢驗「被害」與「非被害」群體之差異，樣本設計刻意將兩組比例控制在接近各半。本研究之主要目的在於分析「相對風險因子」與「群體差異」，並非反映真實母體的被害盛行率。此外，在問卷調查過程中，為避免重複填答，設置了 IP 檢核與身分驗證機制；為提升資料品質，亦排除以下無效樣本：年齡未滿 18 歲、填答時間不足 240 秒、IP 重複且內容雷同、明顯機器填答或答案不合邏輯等。最終有效樣本為 1,146 份，占總回收樣本（n = 2,307）之 49.67%。

由表 1 可知，本研究有效樣本共 1,146 人。性別比例均衡（男性 51.1%，女性 48.9%）。年齡以 31 至 40 歲為最多（34.1%），其次為 18 至 30 歲（27.7%）及 41 至 50 歲（23.2%）。教育程度集中於大學或專科（68.4%），研究所以上占 17.0%，高中及以下合計僅 14.6%。職業以軍公教人員（25.8%）、服務業（13.4%）、學生（11.4%）及製造營建業（10.4%）為主要分布。月收入以 2 萬至 6 萬元區間居多（55.6%），另有 17.8% 低於 2 萬元或無收入，10.1% 超過 8 萬元。整體而言，樣本以中青年及高學歷族群為主，顯示樣本結構存在一定偏向，在推論與解釋研究結果時，需特別注意代表性限制，以避免過度推論。

表 1

本研究樣本人口特性分布表（n = 1,146）

變項	人數	%	變項	人數	%
性別			**教育分組**		
男性	586	51.1	國中畢（肄）業以下	11	1.0
女性	560	48.9	高中畢（肄）業	156	13.6
年齡			大學或專科畢（肄）業	784	68.4
18-30 歲	318	27.7	研究所以上	195	17.0
31-40 歲	391	34.1	**職業**		
41-50 歲	266	23.2	學生	131	11.4
51 歲以上	171	14.9	軍公教人員	296	25.8
每月收入			服務業 / 文藝 / 傳播 / 行銷	154	13.4
無收入	82	7.2	建築 / 營造 / 製造 / 供應商	119	10.4
未滿 2 萬元	122	10.6	交通 / 運輸 / 旅遊 / 物流	41	3.6
2 萬至未滿 4 萬元	312	27.2	醫療 / 法律 / 金融 / 保險 / 房地產	116	10.1
4 萬至未滿 6 萬元	325	28.4	資訊相關 / 網路 / 實體銷售	106	9.3
6 萬至未滿 8 萬元	189	16.5	家管 / 退休	84	7.3
8 萬元以上	116	10.1	其他（無業 / 農林漁牧等）	99	8.7

三、概念測量與信效度分析

（一）網路問卷概念測量

本研究依據相關理論與實證成果，建構網路詐欺被害風險分析架構，從人口特性、心理特質與網路風險暴露等層

面，探討其與被害經驗之關聯。研究假設，各構面變項皆為潛在風險因子，對網路詐欺被害的發生具有顯著影響。

如表 2 所示，問卷設計涵蓋四大構面：（1）人口特性，包括性別、年齡、職業、教育程度、收入與居住地區；（2）心理特質，包括偏差價值觀、網路依賴與低自我控制；（3）網路風險暴露，涵蓋接觸風險訊息、防護監控行為與高誘因涉險傾向；（4）網路詐欺被害經驗，作為依變項，評估受訪者過去一年是否曾遭遇詐欺事件、其類型及重複被害次數。其中，詐欺被害經驗為本研究之核心變項，類型包括：上網購物、網路投資、網路交友或愛情詐騙、參加網路活動、解除分期付款詐騙（ATM）、網路遊戲、不明人士盜（冒）用好友身分、求職詐騙、「猜猜我是誰」（假冒親友）之來電或訊息，以及其他網路詐騙類型。重複被害次數則以過去一年內實際遭遇的次數測量，分為 0 次、1 次、2 次、3 次及 4 次以上。各構面測量題項均依據文獻與現有量表調整編製，並經前測與專家審閱確認內容效度。實證分析採二元邏輯斯迴歸模型，檢驗各風險因子對網路詐欺被害之影響力。

表 2

本研究概念與變項測量表

研究概念	變項內容
自變項	
人口特性	性別、年齡、職業、收入、教育程度、居住區域
心理特質	偏差價值觀、網路依賴、低自我控制
網路風險暴露	風險接觸、防護監控、高誘因涉險傾向
依變項	
網路詐欺被害	詐欺被害類型多元性、重複被害、有無被害經驗

（二）信度、效度分析

本研究問卷設計涵蓋三大研究概念：心理特質、網路風險暴露，以及有無網路詐欺被害經驗。各構面皆依據既有理論與量表編製，並透過主軸因素分析（principal axis factoring）與最大變異法（varimax）旋轉進行建構效度驗證，Cronbach’s α 檢視內部一致性，整體信效度良好（詳如表 3 所示）。

在「心理特質」部分，包含偏差價值觀、網路依賴與低自我控制三構面。「偏差價值觀」項目參考 Titus 和 Gover（2001）、陳玉書等人（2020）等研究設計七題，例如「在網路世界沒有人是誠實的，所以對他們說謊也是剛好而已」，其因素負荷量分別介於 0.670–0.795，解釋變異量為 52.42%，Cronbach’s α 為 0.843。「網路依賴」則依據李雅惠等人（2024）之研究，區分為行為依賴與心理依賴，題項如「每天醒來第一件事就是上網」、「因為上網的關係，

您從事其他休閒活動的時間減少了」，此兩因子之解釋變異量分別為 52.93% 與 8.95%，α 值為 0.895 與 0.867。「低自我控制」構面包含冒險性、衝動性與控制力缺陷三因子，參考 Gottfredson 與 Hirschi（1990）與 Grasmick 等人（1993）量表設計，項目如「一衝動起來就採取行動」、「很生氣時他人離我遠一點」，各因子解釋變異量 38.71%、13.30%、10.79%，α 值介於 0.766 至 0.821 之間。

「網路風險暴露」構面則包括網路風險、防護監控與高誘因涉險傾向三部分。其中「風險接觸」又細分為「接觸偏差訊息」（如「接觸網路詐欺別人財物的訊息」、「接觸援交或賭博訊息」）與「網路觸法行為」（如「曾妨害他人電腦使用」、「曾在網路買賣違禁物品」），因素負荷量分別為介於 0.641–0.829 與 0.626–0.892 之間，解釋變異量為 37.80% 與 14.39%，α 值為 0.816 與 0.731。「防護監控」部分則含「防護意識微弱」（如「未定期更改個人帳號密碼」、「未使用雙重認證」）與「實體監控不足」（如「上網時，家人未注意網路使用情形」、「朋友未提供意見」），負荷量分別為 0.606–0.761 與 0.864–0.877，解釋變異量 32.01% 與 14.63%，α 值為 0.843 與 0.785。「高誘因涉險傾向」包含「誘因吸引」（如「點擊未知電子郵件」、「下載不明來源檔案」）與「遊樂動機」（如「遊玩網路遊戲」、「與陌生人聊天」），分別解釋變異量 48.00% 與 18.61%，α 值為 0.781 與 0.662。所有題項皆採李克特四點量表，由「從未」（1 分）至「經常」（4 分），分數愈高表示風險涉入程度愈高。上述量表架構與測項內容參考自 Bossler 和 Holt（2009）、Leukfeldt 和 Yar（2016）、陳玉書等人（2020）等研究。

表 3

研究概念測量與信效度分析表

測量變項	測量項目	因素負荷量	特徵值	解釋變異量 %	Cronbach's α
心理特質	**偏差價值觀**	0.670-0.795	3.670	52.42	0.843
	網路依賴				
	行為依賴	0.692-0.803	6.881	52.93	0.895
	心理依賴	0.550-0.814	1.164	8.95	0.867
	低自我控制				
	冒險性	0.594-0.837	4.466	38.71	0.821
	衝動性	0.608-0.810	1.595	13.30	0.777
	控制力缺陷	0.571-0.820	1.294	10.79	0.766
網路風險暴露	**風險接觸**				
	接觸偏差訊息	0.641-0.829	3.024	37.80	0.816
	網路觸法行為	0.626-0.892	1.151	14.39	0.731
	防護監控				
	防護意識微弱	0.606-0.761	4.162	32.01	0.843
	實體監控不足	0.864-0.877	1.902	14.63	0.785
	高誘因涉險傾向				
	誘因吸引	0.722-0.871	2.880	48.00	0.781
	遊樂動機	0.543-0.835	1.116	18.61	0.662

四、研究倫理

本研究量化資料源自法務部司法官學院 2023 年「我國網路詐欺被害調查與防制研究」委託案。該研究於 2022 年 10 月核准後，經國立成功大學人類研究倫理審查委員會審查，於同年 12 月 16 日通過（編號：111-526）。調查對象為 18 歲以上網路使用者，採匿名填答方式保護個人隱私。參與者在問卷首頁會獲得研究目的、內容等相關說明，可自由決定是否參與，並有權隨時退出。整個研究過程均遵循研究倫理規範執行。

肆、研究發現

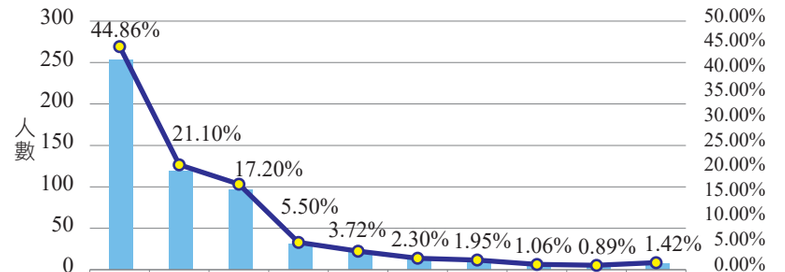
一、網路詐欺被害類型之多元性與重複被害

（一）被害類型之多元性

本研究共納入 1,146 份樣本，採立意抽樣，並控制網路詐欺被害組與非被害組比例各半，其中 564 名（49.21%）受訪者具被害經驗。圖 4 結果顯示，受訪者所遭遇之詐欺類型具有高度集中與長尾分布特徵：253 人（44.86%）僅曾遭遇一種類型，119 人（21.10%）歷經兩種類型，97 人（17.20%）曾遭三種類型，另有 95 人（16.84%）遭遇四種以上，顯示部分受訪者具有多重類型被害經驗。此結果說明，部分個體存在重複或多次被害情形，反映網路詐欺並非單一型態風險，而是一種具備複合性與多樣性的被害模式。

圖 4

網路詐欺被害類型之多元性分布（*n* = 564）



	1	2	3	4	5	6	7	8	9	10
人數	253	119	97	31	21	13	11	6	5	8
%	44.86	21.10	17.20	5.50	3.72	2.30	1.95	1.06	0.89	1.42

（二）被害類型之重複性

如表 4 顯示，不同網路詐欺類型與被害次數間存在明顯差異。多數受訪者僅曾遭遇一次詐欺，惟部分類型的重複被害比例偏高，顯示詐欺風險具長期性與多樣性。本研究以自陳問卷調查為基礎，樣本多為未報案且損失金額較低者，與警政統計資料略有落差，可能隱含一定程度的犯罪黑數。

其中，以網購詐欺最常見，共有 455 名受訪者曾遭此類型，其中 80.44% 為單次經驗，仍有近兩成具重複被害情形。相較下，「猜猜我是誰（假冒親友）」詐欺的重複被害更為顯著，單次被害者僅占 48.02%，另有 18.06% 遭遇四次以上。隨著生成式 AI 普及，民眾對仿聲、合成影像的辨識困難度提高，亦助長此類詐欺的迷惑性與再被害風險。另如「交友愛情詐欺」與「其他類型」（如訂房、演唱會票券、虛擬貨

幣等）亦呈現一定比例之重複被害，遭遇四次以上者分別占 9.15% 與 16.87%。整體而言，重複被害非個案現象，顯示特定族群面對多重詐欺攻擊具持續脆弱性，未來應強化辨識與預警，聚焦其心理特質與行為模式，提升防詐策略的針對性與實效。

表 4

被害類型與被害次數之交叉分布表

被害類型	1 次	%	2 次	%	3 次	%	4 次以上	%	總計
上網購物	**366**	**80.44**	60	13.19	19	4.18	10	2.20	455
猜猜我是誰（假冒親友）	109	48.02	58	25.55	19	8.37	**41**	**18.06**	227
網路投資	122	74.39	25	15.24	7	4.27	10	6.10	164
網路遊戲	125	78.62	17	10.69	9	5.66	8	5.03	159
冒用身分	117	75.00	30	19.23	7	4.40	2	1.28	156
交友愛情	95	66.90	22	15.49	12	8.45	**13**	**9.15**	142
網路活動	98	75.38	20	15.38	5	3.85	7	5.38	130
解除分期	73	70.19	16	15.38	9	8.65	6	5.77	104
其他被害	50	60.24	12	14.46	7	8.43	**14**	**16.87**	83
求職被害	44	63.77	17	24.64	4	5.80	4	5.80	69

註：原始樣本 1,146 名，扣除遺漏值 82 名，有效樣本為 1,064 名，其中 564 名（53.0%）具有被害經驗，此處 53.0% 係以表 4 有效樣本 1,064 名為分母計算，與全文整體樣本 1,146 名之 49.21% 不同。其他被害類型，包括罐頭簡訊、網路訂房、搜尋資料、宅急便、演唱會買票、比特幣等詐欺類型。

二、網路詐欺被害相關因素之分析

（一）高風險族群特徵分析

本研究針對 582 名未曾遭遇網路詐欺者（50.79%）與 564 名曾有被害經驗者（49.21%）進行分析，探討其人口特性與詐欺被害間的關聯。結果顯示，性別、年齡、收入、教育程度與職業類型與被害經驗呈顯著相關，而居住地區與城鄉屬性則無統計差異。

由表 5 得知，男性被害比例高於女性（$\chi^2 = 5.930^{*}$）；年齡層中，40 歲以下、尤其 18 至 30 歲族群的被害比例顯著偏高（$\chi^2 = 23.930^{***}$）。在收入層面，分析結果顯示每月收入未滿 4 萬元者被害比例較高（$\chi^2 = 33.422^{***}$）。相對而言，收入逾 4 萬元者的被害風險明顯較低。在教育程度上，學歷愈低愈易被害，尤以國中以下為最，具研究所以上學歷者則相對安全（$\chi^2 = 20.655^{***}$）。職業類型中，學生、服務業、交通運輸與資訊銷售相關從業者被害比例較高；軍公教、公職、製造業、專業服務、家管與退休者則較低（$\chi^2 = 26.576^{**}$）。至於地理區位與城鄉屬性則無顯著關聯（地區：$\chi^2 = 1.739$；城鄉：$\chi^2 = 1.529$），顯示網路詐欺風險並不因居住位置而有明顯差異。

表 5

人口特性與有無被害經驗之關聯分析表（$n = 1,146$）

變項	有 (n=564)	無 (n=582)	χ^2; sig
性別			
男	309(52.7)	277(47.3)	5.930*
女	255(45.5)	305(54.5)	
每月收入分組			
無收入	36(43.9)	46(56.1)	
未滿 2 萬元	73(59.8)	49(40.2)	
2 萬 - 未滿 4 萬元	185(59.3)	127(40.7)	33.422***
4 萬 - 未滿 6 萬元	150(46.2)	175(53.8)	
6 萬 - 未滿 8 萬元	79(41.8)	110(58.2)	
8 萬以上	41(35.3)	75(64.7)	
職業分組			
學生	78(59.5)	53(40.5)	
軍公教人員	123(41.6)	173(58.4)	
服務業 / 文藝 / 傳播 / 行銷	94(61)	60(39)	
建築 / 營造 / 製造 / 供應商	50(42)	69(58)	26.576**
交通 / 運輸 / 旅遊 / 物流	24(58.5)	17(41.5)	
醫療 / 法律 / 金融 / 保險 / 房地產	54(46.6)	62(53.4)	
資訊相關 / 網路 / 實體銷售	56(52.8)	50(47.2)	
家管 / 退休	40(47.6)	44(52.4)	
其他（無業 / 農林漁牧等）	45(45.5)	54(54.5)	

表 5（續）

變項	有 (n=564)	無 (n=582)	χ^2; sig
年齡分組			
18-30 歲	187(58.8)	131(41.2)	
31-40 歲	198(50.6)	193(49.4)	23.930***
41-50 歲	109(41)	157(59)	
51 歲以上	70(40.9)	101(59.1)	
教育程度分組			
國小 / 國中（肄）業	9(81.8)	2(18.2)	
高中（職）畢（肄）業	81(51.9)	75(48.1)	20.655***
大學 / 專科畢（肄）業	404(51.5)	380(48.5)	
研究所以上	70(35.9)	125(64.1)	
居住地區			
北部（北北基桃竹）	223(47.4)	247(52.6)	
中部（中彰苗投雲）	151(48.9)	158(51.1)	1.739
南部（嘉南高屏）	166(52.2)	152(47.8)	
東部（宜花東）/ 離島	24(49.0)	25(51.0)	
居住城鄉 [a]			
鄉村	124(45.9)	146(54.1)	1.529
都會	440(50.2)	436(49.8)	

註：關於城鄉類別之劃分，係由受訪者依自身認知填答；* $p < .05$；** $p < .01$；*** $p < .001$。

（二）心理特質與網路風險暴露之風險評估

本研究針對是否曾遭遇網路詐欺之群體，分析其在心理特質、網路風險暴露及情境機會變項上的差異。經由獨立樣本 t 檢定，由表 6 可知，兩組在多數變項上具有統計顯著差

異（$p < .001$ 或 $p < .01$），反映心理與情境特徵在詐欺風險中扮演關鍵角色。

在**心理特質**方面，被害組於偏差價值觀（$M = 12.85$）、網路依賴（$M = 34.12$）、行為依賴與心理依賴、低自我控制（$M = 26.94$）、衝動性（$M = 10.03$）、冒險性（$M = 7.88$）及控制力缺陷（$M = 9.03$）等指標上均顯著高於無被害組，顯示其更傾向衝動行為、風險尋求與高度網路依賴，反映出較低的行為自律與風險防禦能力。

在**網路風險暴露**方面，被害組於風險接觸（$M = 18.67$）、接觸偏差訊息（$M = 14.16$）、網路觸法行為（$M = 4.51$）、實體監控不足（$M = 4.34$）、誘因吸引（$M = 5.98$）及遊樂動機（$M = 7.25$）等分數也顯著較高，突顯其暴露於高風險網路情境，且具備較多被害誘發因素。惟在防護監控與防護意識微弱方面，兩組差異不具統計意義。整體而言，詐欺被害群體呈現較強烈的心理弱勢傾向與風險暴露型網路使用模式，顯示該類變項可作為預測與防治網路詐欺的重要參考，未來可進一步納入風險辨識與行為干預設計中。

表 6

有無被害經驗在心理特質與網路風險暴露之差異分析（$n = 1,146$）[a]

心理特質測量變項	有無被害	*M*	*SD*	*t; sig*	網路生活型態與機會變項	有無被害	*M*	*SD*	*t; sig*
偏差價值觀	有	12.85	4.51	5.776***	**風險接觸**	有	18.67	4.43	6.036***
	無	11.43	3.78			無	17.06	4.62	
網路依賴	有	34.12	8.55	7.091***	接觸偏差訊息	有	14.16	3.50	4.780***
	無	30.62	8.18			無	13.11	3.93	
行為依賴	有	19.38	4.93	5.240***	網路觸法行為	有	4.51	1.90	5.723***
	無	17.85	4.99			無	3.94	1.39	
心理依賴	有	14.74	4.24	8.233***	**防護監控**	有	30.23	5.85	0.653
	無	12.77	3.83			無	29.99	6.17	
低自我控制	有	26.94	6.01	6.272***	防護意識微弱	有	25.88	5.36	0.495
	無	24.79	5.58			無	26.05	5.79	
衝動性	有	10.03	2.39	6.916***	實體監控不足	有	4.34	1.58	4.331***
	無	9.05	2.41			無	3.95	1.51	
冒險性	有	7.88	2.70	5.327***	**高誘因涉險傾向**	有	13.23	3.57	12.757***
	無	7.09	2.31			無	10.66	3.22	
控制力缺陷	有	9.03	2.46	2.597**	誘因吸引	有	5.98	1.91	11.026***
	無	8.65	2.46			無	4.81	1.67	
					遊樂動機	有	7.25	2.27	10.549***
						無	5.85	2.21	

註：有被害經驗組（n=564）；無被害經驗組（n=582）；* $p < .05$；** $p < .01$；*** $p < .001$。

三、影響有無網路詐欺被害之關鍵因子

（一）各影響網路詐欺被害因子之相關分析

由表 7 研究發現，**人口特性變項**中，年齡與詐欺被害經驗呈負相關（$\rho = -.141^{***}$），表示年齡愈小，愈可能成為受害者。教育程度（$\rho = -.104^{***}$）與收入（$\rho = -.105^{***}$）愈低者，也愈容易被騙，顯示社經條件會影響網路詐欺的風險。在**心理特質**方面，有偏差價值觀（$\rho = .159^{***}$）、網路依賴（$\rho = .195^{***}$）、行為依賴（$\rho = .148^{***}$）、心理依賴（$\rho = .226^{***}$）的人較容易受害；同時，自我控制低（$\rho = .171^{***}$）、衝動（$\rho = .195^{***}$）、愛冒險（$\rho = .142^{***}$）也會增加被害風險。雖然控制力缺陷的相關性比較低（$\rho = .069^{*}$），但仍是顯著的。

此外，在**網路風險暴露**方面，經常接觸網路風險（$\rho = .171^{***}$）、偏差訊息（$\rho = .133^{***}$）和網路觸法行為（$\rho = .153^{***}$）的人，比較容易受害。雖然防護意識微弱沒有顯著差異，但「實體監控不足」如缺乏周遭人提醒或監督（$\rho = .126^{***}$），也會提高風險。另外，如果個人本身有強烈的網路風險暴露，例如期待獲利或娛樂，高誘因涉險傾向（$\rho = .357^{***}$）、誘因吸引（$\rho = .317^{***}$）和遊樂動機（$\rho = .298^{***}$）的相關性都非常明顯，代表這類人更容易被詐欺吸引。

表 7

各影響因子與有無網路詐欺被害相關分析表（*n* = 1,146）

測量概念	變項	*M*	*SD*	*Spearman's rho* (ρ)
人口特性	年齡	38.26	11.98	-.141***
	教育程度	-	-	-.104***
	每月收入	-	-	-.105***
心理特質	**偏差價值觀**	12.13	4.21	.159***
	網路依賴	32.34	8.54	.195***
	行為依賴	18.60	5.02	.148***
	心理依賴	13.74	4.16	.226***
	低自我控制	25.84	5.90	.171***
	衝動性	9.53	2.45	.195***
	冒險性	7.48	2.54	.142***
	控制力缺陷	8.84	2.46	.069*
網路風險暴露	**風險接觸**	17.85	4.59	.171***
	接觸偏差訊息	13.63	3.76	.133***
	網路觸法行為	4.22	1.68	.153***
	防護監控	30.11	6.01	-.005
	防護意識微弱	25.97	5.58	-.035
	實體監控不足	4.14	1.56	.126***
	高誘因涉險傾向	11.93	3.63	.357***
	誘因吸引	5.39	1.88	.317***
	遊樂動機	6.54	2.35	.298***

註 1：變項「有無被害經驗」之編碼為有 =1，無 =0；正值代表變項值愈高、被害機率愈高，負值代表變項值愈高、被害機率愈低；年齡為連續變項；教育與收入為順序變項：國小 / 國中 =1，高中職 =2，大學 / 專科 =3，研究所以上 =4；每月收入三組：無收入及未滿 2 萬元 =1，每月 2 萬以上至未滿 6 萬元 =2，每月 6 萬以上 =3；$^{*}p < .05$；$^{**}p < .01$；$^{***}p < .001$。

註 2：人口特性變項中，性別與居住城鄉區別另以卡方檢定分析（見表 5）。

（二）網路詐欺被害影響因素之二元邏輯斯迴歸分析

本研究綜合分析人口特性（性別、年齡、收入、教育程度）、心理特質（偏差價值觀、網路依賴、低自我控制）與網路風險暴露（風險接觸、防護監控、高誘因涉險傾向）等變項對網路詐欺被害之影響。依據理論架構與前述統計分析結果，本研究將相關變項納入二元邏輯斯迴歸（binary logistic regression）模型，並建構三組解釋模式，以逐步檢視不同構面對詐欺被害風險之預測效果。Hosmer–Lemeshow 適配度檢定結果顯示，各模型均未達顯著水準，表示模型與觀察資料之間未呈現明顯不適配，整體配適情形尚稱良好（詳見表 8）。以下將依序說明三種迴歸模型對詐欺被害風險的預測效果：

1. 性別、年齡及每月收入對有無網路詐欺被害有預測力，惟解釋力略顯不足

在模型一中，將人口特性變項納入邏輯斯迴歸分析，以檢驗其對有無網路詐欺被害經驗的預測效力。表 8 結果顯示，性別為顯著預測因子，男性相較於女性更易成為受害者（$B = .397$，$Exp(B) = 1.487$，$Wald = 10.035^{**}$），顯示男性被害機率約為女性的 1.49 倍。年齡亦呈現穩定之負向預測（$B = -.017$，$Exp(B) = 0.983$，$Wald = 10.199^{**}$），表示年齡愈小，詐欺受害機率愈高。月收入水準在模型一中具有顯著預測效果。相較於每月 6 萬元以上者，無收入及未滿 2 萬元者（$B = .434$，$Exp(B) = 1.544$，$p < .05$）及每月 2 萬至未滿 6 萬元者（$B = .586$，$Exp(B) = 1.796$，$p < .001$）之被害風險較高，此結果顯示，相較於高收入群體，中低收入者較易成為網路詐欺被害者。教育程度則在控制性別、年齡與收入後未達顯著水準（$p > .05$）。

整體而言，年輕、男性與經濟弱勢個體為高風險族群，其社會資源處境可能影響其辨識詐欺風險與採取保護行動之能力。然而，雖然性別、年齡與收入等變項對詐欺被害具有統計上的預測力，但其對整體模型的解釋力仍相對有限，顯示人口特性只能部分說明詐欺被害的差異，尚需結合心理特質與網路風險暴露等因素，才能更完整理解被害風險。

2. 心理依賴與衝動性為穩定預測因子

本研究進一步將心理特質納入預測模型，結果顯示部分變項與網路詐欺被害經驗具顯著關聯（見表 8）。其中，以「心理依賴」之預測效果最為穩定，在模型二（$B = .112$，$Exp(B) = 1.119$，$Wald = 22.29^{***}$）與模型三（$B = .089$，$Exp(B) = 1.093$，$Wald = 12.900^{***}$）中皆達高度顯著水準，反映個體在網路使用上若具高度情感依附與依賴傾向，將可能削弱其辨識風險與自我防衛能力。「衝動性」亦為穩定的預測變項，在模型二（$B = .119$，$Exp(B) = 1.126$，$Wald = 13.225^{***}$）與模型三（$B = .082$，$Exp(B) = 1.086$，$Wald = 5.815^{*}$）中均具統計意義，支持衝動控制困難者更易陷入詐欺情境之推論。

此外，「偏差價值觀」於模型二達顯著水準（$B = .046$，$Wald = 7.229^{**}$），顯示若個體本身具有違規、規避規範的傾向，可能增加其暴露於高風險互動場域的機率；惟該

變項於模型三則不顯著，推測其效果可能受網路風險暴露變項之影響。相對地，控制力缺陷雖在模型二與模型三達顯著，惟方向與理論預期不一致；冒險性則未達顯著，兩者均不足以支持其穩定預測效果。

整體而言，本研究結果指出，心理依賴與衝動性為最具預測效力之心理特質變項，揭示心理弱勢可能降低網路詐欺風險辨識與自我調節能力，應列為後續風險識別與預防教育之核心指標。

3. 高誘因涉險傾向為預測網路詐欺被害的重要因素

在模型三中納入網路使用動機與風險行為變項後，發現「誘因吸引」與「遊樂動機」為整體模型中最具影響力之預測因子。「誘因吸引」顯著正向影響詐欺受害機率（$B = .224$，$Exp(B) = 1.253$，$Wald = 25.159^{***}$），而「遊樂動機」亦達顯著水準（$B = .174$，$Exp(B) = 1.191$，$Wald = 19.125^{***}$），顯示若個體基於娛樂、金錢、情感或好奇等目的而主動進入高風險場域，其成為詐欺目標的機率明顯升高。其他如接觸偏差訊息、網路觸法行為、實體監控不足雖方向與預期一致，惟未達統計顯著。此結果反映詐欺被害的產生並非僅為單向風險暴露，更涉及使用者主動參與的「情境互動性」，顯示未來防詐策略應著重於風險動機的辨識與引導。

表 8

網路詐欺被害影響因素之邏輯斯迴歸分析（*n* = 1,146）

測量概念	自變項	模型一		模型二		模型三	
		B(Wald)	*Exp (B)*	*B(Wald)*	*Exp (B)*	*B(Wald)*	*Exp (B)*
人口特性	性別 [a](1)	**.397(10.035**)**	1.487	.148(1.185)	1.159	-.163(1.148)	0.850
	年齡	**-.017(10.199**)**	0.983	**-.015(6.611**)**	0.986	-.004(0.402)	0.996
	收入三組 [b](1)	**.434(4.325*)**	1.544	**.497(5.202*)**	1.644	.414(3.340)	1.513
	收入三組 (2)	**.586(15.263***)**	1.796	**.517(10.815**)**	1.676	**.412(6.367*)**	1.510
	教育程度 [c](1)	.195(1.127)	1.216	.25(1.683)	1.284	.232(1.351)	1.261
心理特質	**偏差價值觀**			**.046(7.229**)**	1.047	.014(0.606)	1.014
	網路依賴						
	行為依賴			-.026(1.847)	0.975	-.029(2.098)	0.972
	心理依賴			**.112(22.290***)**	1.119	**.089(12.900***)**	1.093
	低自我控制						
	衝動性			**.119(13.225***)**	1.126	**.082(5.815*)**	1.086
	冒險性			.015(0.220)	1.015	-.031(0.859)	0.968
	控制力缺陷			-.065(4.340*)	0.937	-.069(**4.455***)	0.933
網路風險暴露	**風險接觸**						
	接觸偏差訊息					-.008(0.168)	0.992
	網路觸法行為					.042(0.666)	1.043
	防護監控						
	實體監控不足					-.022(0.217)	0.978
	高誘因涉險傾向						
	誘因吸引					**.224(25.159***)**	1.253
	遊樂動機					**.174(19.125***)**	1.191

表 8（續）

測量概念	自變項	模型一		模型二		模型三	
		B(Wald)	*Exp (B)*	*B(Wald)*	*Exp (B)*	*B(Wald)*	*Exp (B)*
常數		0.615(5.243*)		-1.497(12.109***)		-3.242(38.646***)	
-2*LL* 對數概似值		1548.786		1470.136		1393.545	
H-L 檢定（模型適配度）		χ2=12.313; p=0.138		χ2=8.609; p=0.376		χ2=5.868; p=0.662	
Cox & Snell R2 (Nagelkerke R2)		0.034(0.045)		0.104(0.138)		0.156(0.209)	
正確預測率		58.6		64.4		67.6	

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

(2) 本研究之「區域特性」與「防護意識微弱」未達顯著，職業變項則因類別較多且部分組別樣本數較少，故未納入模型；其餘變項採強迫輸入法（forced entry method），依理論架構依序投入，以檢驗其對被害風險之影響。

(3) *p < .05；**p < .01；***p < .001。

伍、討論與建議

一、詐欺不是意外：重複受害與中低收入族群之被害風險盲點

本研究針對臺灣網路詐欺的被害情形進行系統性調查，結果顯示，詐欺早已不再是偶發事件，而是一種反覆出現、多樣交織的結構性風險。以「猜猜我是誰」這類假冒親友的詐欺為例，有超過五成的受害者曾被騙兩次以上，突顯這類情感操弄型詐欺，不只訴諸關係信任，更容易反覆侵入受害者生活，與一般財務詐欺有本質上的不同。

進一步分析結果顯示，性別（男性）、年齡（40 歲以下）、教育程度與職業類型等因素皆與被害機率呈顯著關聯，此發現與 Izuakor（2021）及 Reyns（2015）的研究結果一致，顯示詐欺風險並非隨機，而是呈現一定的結構性分布。在收入層面，本研究發現每月收入 2 萬至 4 萬元者的被害風險高於收入逾 4 萬元者。進一步檢視收入與被害的相關性，兩者呈顯著負相關（$\rho = -.105^{***}$），亦即收入愈低，愈容易成為網路詐欺的受害者。此結果不僅呼應特徵與相關分析的發現，也突顯社會經濟條件在理解網路詐欺被害風險上的重要意涵。

因此，本研究建議政府與民間團體，應針對「情感操弄型詐欺」設計追蹤式預警系統與模擬訓練課程，尤其是那些情緒較為脆弱、易受人際關係影響的族群。其次，應強化中低收入者的風險意識，跳脫過去只針對高齡與低社經地位者宣導的舊有模式，改以網路活躍但防備不足的族群為對象，搭配社群推廣、互動課程與實境模擬，建立更貼近真實情境的防詐教育策略。

二、心理特質與網路風險暴露共同推升詐欺被害風險

本研究進一步分析心理特質、網路風險暴露與有無網路詐欺被害經驗之關聯性，結果顯示，「偏差價值觀」、「網路依賴」與「低自我控制」等心理特質皆與被害風險具顯著

正向關聯。特別是具有高網路使用頻率與衝動性傾向者，更易落入詐欺陷阱。這些心理特質並非孤立作用，而是與個體的網路行為模式、情境選擇相互影響，進而強化其成為合適標的物的可能性。此結果與 Herrero 等人（2021）提出的「網路被害雙重脆弱性模型」相呼應，說明心理脆弱性與風險暴露共同交織出高風險網路情境。

此外，在「風險接觸」、「實體監控不足」、「高誘因涉險傾向」三個面向中，亦可觀察到具體的風險輪廓。例如，習慣點擊不明連結、曾參與線上賭博或盜版軟體交易者，其網路詐欺被害機率明顯升高。反之，數位防護習慣雖在本研究中未呈現顯著差異，但仍具理論上的保護意義，未來可進一步檢驗其在不同詐欺類型中的作用。

此一發現顯示，網路詐欺的成因並非單一人格或行為導致，而是心理特質、風險習慣與情境選擇所交互形成的「行為脆弱區」。本研究建議，未來防詐教育除應針對認知提升與情境模擬訓練外，亦可結合心理風險評估與生活型態調整介入，發展預防型數位素養課程與早期辨識機制。

三、心理特質與高誘因涉險傾向交織下之詐欺被害風險模型

本研究以生活方式－日常活動理論（L-RAT）為基礎，結合自我控制理論（SCT），建構整合式風險分析模型，並以邏輯斯迴歸檢驗各構面對網路詐欺被害的預測力。結果顯示，模型三之整體解釋力較前兩模型提升（Nagelkerke R^2 = .209），且 Hosmer–Lemeshow 檢定未達顯著，顯示模型配適情形尚可，其中「高誘因涉險傾向」構面下的「網路誘因吸引」與「遊樂動機」具顯著預測效果，顯示主動追求金錢、情感或娛樂刺激者的被害風險顯著提高。

Choi 與 Lee（2017）指出，部分個體並非被動遭遇風險，而是出於尋求刺激、資源或人際互動等目的，自願進入高風險互動場域。此類行為與心理傾向交織而成的涉險模式，可能導致個體在接觸詐欺訊息時缺乏防備，進而增加受害可能。研究亦發現，如點擊不明連結、下載盜版內容、參與線上博弈等高風險使用行為，常與心理衝動性及風險動機共現，形成高度易被害的行為樣態。

上述結果亦擴充了 L-RAT 模型中「目標適合性（target suitability）」的概念。傳統觀點多強調個體的靜態特質與暴露狀態，然而本研究指出，目標適合性亦包含行為習慣與心理特質之能動選擇。換言之，個體是否成為詐欺目標，並非僅因暴露環境或監護缺位，更涉及其主動涉險的動機與傾向。

因此，防詐策略應超越傳統手法揭露與被動防範，轉向辨識高風險心理傾向與涉險行為組合，並建議發展具預測性的行為識讀訓練與風險自評機制，以預防再暴露與重複被害的擴張風險。

四、防詐策略設計與實務建議：分眾辨識與行為導向的預防機制

本研究結果顯示，網路詐欺風險並非均質分布，而是隨個體之人口特性、心理特質與網路行為模式而有所差異，尤其中低收入、低自我控制、高網路涉入與高誘因涉險傾向者，更易成為重複被害的高風險族群。根據此結果，現行以高齡者為防詐重點對象的宣導策略，應進行調整與擴充。

首先，在識別對象方面，應強化「中低收入」、「高網路接觸」、「心理防線薄弱」的風險組合辨識，導入數據監測與早期預警機制，優先納入易重複被害者與高曝險活動參與者。其次，在防詐內容設計上，須跳脫「靜態警語」模式，轉向「行為導向、情境模擬」的互動式教學，強化使用者對風險訊號的即時辨識與應對反應。

針對「猜猜我是誰」、「交友愛情」等倚賴情感操弄與人際信任的詐欺手法，更應發展「關係風險識讀」課程與「數位同理教育」，協助使用者識破假借親情、愛情等名義進行操控之伎倆。對於已具被害經驗者，則建議導入「重複被害支持系統」，結合心理諮詢、法律協助與社會支持網絡，避免其再度落入類似陷阱。

此外，防詐政策設計亦須橫跨教育、警政與平臺治理三層面。例如，教育端應於中等與高等教育課程中融入「數位風險素養」；警政端應強化跨系統合作與非報案資料運用，擴大黑數掌握力；平臺端則應強化詐欺通報、機制阻斷與用戶行為異常偵測，形成多層次、即時性與行為化的整體防護架構。

五、研究限制與未來研究建議

本研究透過問卷調查，分析個人特質與網路詐欺風險的關係，並比較被害與非被害群體以找出關鍵風險因子，然而，本研究仍存在若干限制。首先，本研究因經費與時間考量採目的抽樣，雖已盡力控制性別、年齡及被害／非被害比例，但樣本並非真實母體。被害比例刻意設為約半數（49.21%），高於實證調查之 16.32%（方呈祥，2020），故結果僅適用於探討風險因子與群體差異，不能推估實際被害率。

其次，在研究設計上的限制，問卷調查雖能掌握趨勢與關聯，但難以完整反映實際犯罪狀況，且部分心理特質測量依賴自陳量表，可能受到社會期望影響而產生偏誤。此外，本研究採橫斷面設計，無法觀察被害風險隨時間的變化，更不易確認因果關係。再者，在研究範圍方面，本研究主要聚焦於個人與家庭層面的網路詐欺，尚未涵蓋企業或商業詐欺問題；同時，研究結果主要適用於臺灣社會脈絡，其跨文化推論能力有限。

針對未來研究方向，建議擴大調查規模至萬人以上，結合線上與線下多元方式增強統計效力。研究範圍應拓展至企業與商業詐欺領域，並採用長期追蹤設計觀察風險變化軌跡。測量方面可結合行為實驗等客觀方法，減少自我報告偏

差。同時建立跨國比較研究，搭配深度訪談深入瞭解被害經驗。總而言之，本研究為網路詐欺風險評估提供初步基礎，未來需朝向方法多元化、範圍擴展化及國際合作方向發展，以建構更完整的防詐知識體系。

參考文獻

一、中文書目

☆ 內政部警政署（2025）。*警政統計查詢網*。檢索於 2025 年 7 月 31 日，取自 https://ba.npa.gov.tw/statis/webMain.aspx?k=defjsp

☆ 孔令維（2018）。*論網路犯罪偵查相關數位證據——以網路即時通訊軟體為中心*〔碩士論文，國立高雄第一科技大學〕。臺灣博碩士論文知識加值系統。https://hdl.handle.net/11296/46u736

☆ 方呈祥（2020）。*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*〔碩士論文，國立中央警察大學〕。臺灣博碩士論文知識加值系統。https://hdl.handle.net/11296/q2z4ep

☆ 王秋惠（2007）。*網路詐欺被害特性與被害歷程之研究*〔碩士論文，國立中央警察大學〕。臺灣博碩士論文知識加值系統。https://hdl.handle.net/11296/w2n4gd

☆ 石泱、王乃琳（2021）。青少年偏差行為和網路不當行為影響因素之研究。*青少年犯罪防治研究期刊，13*（2），1-41。

☆ 李雅惠、陳玉書、劉士誠、葉碧翠（2024）。網路互動犯罪被害促發因素之實證研究。*刑事政策與犯罪防治研究專刊*（7），1-46。

☆ 周愫嫻（2014）。青少年網路虛擬身分與網路被害、不當行為。*犯罪與刑事司法研究*（2），45-73。

☆ 財團法人臺灣網路資訊中心（2023）。*2023 年臺灣網路報告*。臺灣網路報告官網。https://report.twnic.tw/2023/

☆ 張志盛（2022）。*科技偵查法制理論與實務研究——以集團式詐欺為例*〔碩士論文，中國文化大學〕。臺灣博碩士論文知識加值系統。https://hdl.handle.net/11296/uw4ce3

☆ 梁馨科、吳美蓉、張廣志（2009）。電腦與網路犯罪及其防治的科技管理觀。*2009 年中小企業經營管理研討會論文集*。佛光大學。

☆ 陳玉書、簡鳳容、呂豐足、劉士誠（2020）。網路犯罪被害：人口特性與情境機會的影響。載於法務部司法官學院（主編），*刑事政策與犯罪研究論文集*（頁 113-148）。法務部司法官學院。https://doi.org/10.6482/ECPCR.202010.0004

☆ 陳宗義、沈筱娟（2015）。從網路犯罪觀點探討虛擬社群之網路人際行為與互動安全因素。*電子商務研究，13*（2），241-270。

☆ 曾百川（2006）。網路詐欺犯罪歷程之質化研究〔碩士論文，國立中央警察大學〕。臺灣博碩士論文知識加值系統。https://hdl.handle.net/11296/e5h8rw

☆ 葉雲宏（2007）。*網路詐欺犯罪被害影響因素之研究*〔碩士論文，國立中央警察大學〕。臺灣博碩士論文知識加值系統。https://hdl.handle.net/11296/tq65v6

☆ 廖釗頡（2010）。*網路釣魚被害類型及其成因*〔碩士論文，國立臺北大學〕。臺灣博碩士論文知識加值系統。https://hdl.handle.net/11296/85hv77

☆ 蔡田木、周文勇、陳玉書（2009）。*詐騙犯罪被害人屬性之研究*〔委託研究報告〕。內政部警政署刑事警察局。https://books.google.com.tw/books?id=gGoJtwAACAAJ

☆ 蔡德輝、楊士隆（2023）。*犯罪學*。五南。

☆ 賴擁連、蔡田木、陳玉書、許春金、葉碧翠、劉士誠、黃百豪（2023）。*我國網路詐欺被害調查與防制研究*（計畫編號：112-A-002）〔委託研究報告〕。法務部。https://www.grb.gov.tw/search/planDetail?id=14811970

☆ 簡鳳容（2018）。*網路偏差行為與被害特性及其影響因素之研究*〔博士論文，國立中央警察大學〕。臺灣博碩士論文知識加值系統。https://hdl.handle.net/11296/r9b973

二、英文書目

☆ Akdemir, N., & Lawless, C. J. (2020). Exploring the human factor in cyber-enabled and cyber-dependent crime victimisation: A lifestyle routine activities approach. *Internet Research*, *30*(6), 1665-1687.

☆ Bossler, A. M., & Holt, T. J. (2009). On-line activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology*, *3*(1).

☆ Burden, M. (2025). The cybercrime victim-offender overlap: Evaluating predictors for victims, offenders, victim-offenders, and those who are neither. *Victims & Offenders*, *20*(4), 710-728.

☆ Buse, J. H., Fong, C., & Tripathi, S. (2024). The interplay of social behaviour and demographics in cyber scam susceptibility: A Singapore study. *Open Journal of Business and Management*, *12*(5), 2949-2964.

☆ Choi, K.-S. (2008). Computer crime victimization and integrated theory: An empirical assessment. *International Journal of Cyber Criminology*, *2*(1).

☆ Choi, K.-S., & Lee, J. R. (2017). Theoretical analysis of cyber-interpersonal violence victimization and offending using cyber-routine activities theory. *Computers in Human Behavior*, *73*, 394-402.

☆ Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review, 44(4), 588-608.

☆ Felson, M., & Clarke, R. V. (1998). Opportunity makes the thief. *Police Research Series, 98,* 1-36.

☆ Gottfredson, M. R., & Hirschi, T. (1990). *A general theory of crime*. Stanford University Press.

☆ Grasmick, H. G., Tittle, C. R., Bursik, R. J., Jr., & Arneklev, B. J. (1993). Testing the core empirical implications of Gottfredson and Hirschi's general theory of crime. *Journal of Research in Crime and Delinquency*, *30*(1), 5-29.

☆ Havers, B., Tripathi, K., Burton, A., McManus, S., & Cooper, C. (2024). Cybercrime victimisation among older adults: A probability sample survey in England and Wales. *PLOS ONE, 19*(12), e0314380. https://doi.org/10.1371/journal.pone.0314380

☆ Herrero, J., Torres, A., Vivas, P., Hidalgo, A., Rodríguez, F. J., & Urueña, A. (2021). Smartphone addiction and cybercrime victimization in the context of lifestyles routine activities and self-control theories: The user's dual vulnerability model of cybercrime victimization. *International Journal of Environmental Research and Public Health*, *18*(7), 3763.

☆ Hirschi, T., & Gottfredson, M. (1993). Commentary: Testing the general theory of crime. *Journal of Research in Crime and Delinquency*, *30*(1), 47-54.

☆ Holt, T. J., Bossler, A. M., & May, D. C. (2012). Low self-control, deviant peer associations, and juvenile cyberdeviance. *American Journal of Criminal Justice*, *37*(3), 378-395.

☆ Holtfreter, K., Reisig, M. D., & Pratt, T. C. (2008). Low self-control, routine activities, and fraud victimization. Criminology, 46(1), 189-220. https://doi.org/10.1111/j.1745-9125.2008.00109.x

☆ Izuakor, C. F. (2021). Cyberfraud: A review of the internet and anonymity in the Nigerian context. *ISSA Journal*, *19*(3).

☆ Jennings, W. G., Piquero, A. R., & Reingle, J. M. (2012). On the overlap between victimization and offending: A review of the literature. *Aggression and Violent Behavior*, *17*(1), 16-26.

☆ Lauritsen, J. L., Sampson, R. J., & Laub, J. H. (1991). The link between offending and victimization among adolescents. *Criminology*, *29*(2), 265-292.

☆ Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, *37*(3), 263-280.

☆ Louderback, E. R., & Antonaccio, O. (2017). Exploring cognitive decision-making processes, computer-focused cyber deviance involvement and victimization: The role of thoughtfully reflective decision-making. *Journal of Research in Crime and Delinquency*, *54*(5), 639-679.

☆ Mihajlov, M., & Vejmelka, L. (2017). Internet addiction: A review of the first twenty years. *Psychiatria Danubina*, *29*(3), 260-272.

☆ Modic, D., & Lea, S. E. (2012). *How neurotic are scam victims, really? The Big Five and internet scams.* [Working paper]. SSRN. https://doi.org/10.2139/ssrn.2448130

☆ Ngo, F. T., & Paternoster, R. (2011). Cybercrime victimization: An examination of individual and situational level factors. *International Journal of Cyber Criminology*, *5*(1), 773.

☆ Pratt, T. C., Turanovic, J. J., Fox, K. A., & Wright, K. A. (2014). Self-control and victimization: A meta-analysis. *Criminology*, *52*(1), 87-116.

☆ Qu, J., Lin, K., Wu, Y., & Sun, I. Y. (2024). Fear and perceived risk of cyber fraud victimization among Chinese university students. *Crime, Law and Social Change*, *82*(3), 543-562.

☆ Reyns, B. W. (2013). Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. *Journal of Research in Crime and Delinquency*, *50*(2), 216-238.

☆ Reyns, B. W. (2015). A routine activity perspective on online victimisation: Results from the Canadian General Social Survey. *Journal of Financial Crime*, *22*(4), 396-411.

☆ Schreck, C. J. (1999). Criminal victimization and low self-control: An extension and test of a general theory of crime. *Justice Quarterly*, *16*(3), 633-654.

☆ Titus, R. M., & Gover, A. R. (2001). Personal fraud: The victims and the scams. *Crime Prevention Studies*, *12*, 133-152.

☆ Van Wyk, J., & Mason, K. A. (2001). Investigating vulnerability and reporting behavior for consumer fraud victimization: Opportunity as a social aspect of age. *Journal of Contemporary Criminal Justice*, *17*(4), 328-345.

☆ Whitty, M. T. (2020). Is there a scam for everyone? Psychologically profiling cyberscam victims. *European Journal on Criminal Policy and Research*, *26*(3), 399-409.

☆ Zhang, Z., & Ye, Z. (2022). The role of social-psychological factors of victimity on victimization of online fraud in China. *Frontiers in Psychology*, *13*, 1030670. https://doi.org/10.3389/fpsyg.2022.1030670