學術論著

網路被害特性與情境預防 [1]

DOI：10.6905/JC.202601_15(1).0003

Characteristics of Internet Victimization and Contextual Prevention

劉士誠 中央警察大學犯罪防治研究所博士生
內政部警政署刑事警察局警務正

陳玉書 美國杜克大學社會學博士
中央警察大學犯罪防治學系（所）副教授

葉碧翠 中央警察大學犯罪防治學系（所）犯罪學博士
中央警察大學犯罪防治學系（所）副教授

DOI：10.6905/JC.202601_15(1).0003

摘 要

劉士誠 [2]、陳玉書 [3]、葉碧翠 [4]

本研究的主要目的是探討不同類型的網路犯罪被害情況，並分析人口特徵、日常活動和情境機會與網路被害之間的關聯性。研究還檢驗基於生活型態和日常活動理論（LRAT）的概念框架。研究樣本包括 3,056 名參與網路和實體問卷調查的受訪者。結果顯示：1. 前五大網路被害類型爲：遭駭客攻擊、檔案被盜、購物詐騙、資料被刪除 / 更改和網路性騷擾，這些類型占所有被害事件的 84.65%。2. 男性受訪者的被害率顯著高於女性，每月收入是被動被害的重要影響因素，而教育程度則影響互動被害。3. 網路使用環境、網路成癮、偏差價值觀、情境機會和被害誘因與網路被害呈現顯著正相關。4. 被害誘因、偏差價值觀和網路成癮對網路被動或互動被害均有顯著影響，但監控遏阻的影響力較弱。根據研究結果，提出網路犯罪被害情境的預防措施和未來研究的建議。

關鍵字｜網路犯罪被害、情境預防、人口特性、生活型態、情境機會

[1] 本研究使用資料來源為科技部於 2020 至 2021 年間補助之研究計畫「自我控制、情境機會與網路被害之實證研究」（計畫編號：108-2410-H-015-009），由陳玉書與葉碧翠教授主持。該研究已通過國立成功大學人類研究倫理審查委員會審查（審查編號：108-171）。特此感謝審查委員的寶貴建議、委託單位的支持，以及研究團隊的協助與努力。

[2] 劉士誠，中央警察大學犯罪防治研究所博士生，內政部警政署刑事警察局警務正。

[3] 陳玉書，美國杜克大學社會學博士，中央警察大學犯罪防治學系（所）副教授。

[4] 葉碧翠，中央警察大學犯罪學博士，中央警察大學犯罪防治學系（所）副教授。本文通訊作者：tracy@mail.cpu.edu.tw

DOI：10.6905/JC.202601_15(1).0003

Characteristics of Internet Victimization and Contextual Prevention

Shih-Cheng Liu, Yu-Shu Chen, Pi-Tsui Yeh

Abstract

The primary purpose of this study is to investigate the types of cybercrime victimization, to analyze the associations between demographic characteristics, routine activities, and situational opportunities and cyber victimization, and to examine the conceptual framework based on the Lifestyle and Routine Activities Theory (LRAT). The study sample consisted of 3,056 online and in-person survey respondents. The results showed that (1) the top five types of cyber victimization were hacking, file theft, shopping fraud, data deletion and alteration, and online sexual harassment, which accounted for 84.65% of the total number of victimization types. (2) The victimization rate of male respondents is significantly higher than that of female respondents. Income are the significant factors affecting passive victimization, while education level influences interactive victimization. (3) Internet use environment, Internet addiction, deviant values, situational opportunities, and victimization incentives are significantly positively correlated with Internet victimization. (4) Victimization triggers, deviant values, and Internet addiction have significant effects on passive or interactive victimization, but the effect of deterrence and monitoring is less significant. Based on the results of this study, we propose the prevention of cybercrime victimization and related recommendations for future research.

Keywords: cybercrime victimization, situational prevention, demographic characteristics, lifestyle, situational opportunity

壹、前言

隨著網路科技與通訊軟體的迅速發展，虛擬環境已深度融入人們的日常生活，廣泛應用於消費、教育、工作、商業、文化、休閒與醫療等領域。與此同時，網路相關的犯罪與被害事件也呈現顯著上升趨勢。根據警政統計，2020年有超過1萬 4千人遭受網路犯罪被害，其中以詐欺、妨害名譽以及妨害電腦使用等類型最爲常見。

國內外的研究顯示，網路犯罪被害類型多樣，包括金錢、軟體、資訊和信用 / 名譽等（吳嫦娥，2004；黃文圳，2024；賴克宗，2005；Ho & Luong, 2022；Leukfeldt, Kleemans, & Stol, 2017；Reep-van den Bergh & Junger, 2018）。這些被害標的物的價值難以金錢衡量，被害者有時無法估計實際損失。因此，網路犯罪被害在類型和損失上顯著不同於傳統犯罪（陳玉書、簡鳳容、呂豐足、劉士誠，2020）。

臺灣曾多次透過面訪或電訪進行大樣本的犯罪被害調查（許春金、陳玉書、莫季雍，2000；許春金、陳玉書，2005；2010），主要關注實體情境的竊盜、強盜和詐欺等犯罪被害經驗，較少涉及網路與通訊軟體情境中的被害事件。然而，近年美國及歐盟的犯罪被害調查對於網路被害情形有長足的進度。美國司法統計局（Bureau of Justice Statistics）於 2023年發布的《An Environmental Scan of Cybercrime Measurement》報告中，已針對網路犯罪測量進行系統性檢討，並建議將網路詐騙、身分盜用、網路騷擾等問題納入全國犯罪被害調查（National Crime Victimization Survey, NCVS）中，並採行問卷預試與認知訪談等方式發展具效度的測量項目。

此外，歐盟統計局（Eurostat）也透過歐盟收入和生活條件統計 (European Union Statistics on Income and Living Conditions, EU-SILC) 調查之附加模組（Ad hoc Modules），於 2015 年與 2020 年納入「網路使用與風險暴露」問項，蒐集駭客攻擊、詐騙郵件、個資外洩等自陳經驗，並以一致結構性問卷實施於各會員國，以提升跨國比較的準確性與政策應用價值。因此，針對網路與通訊軟體情境中的犯罪被害進行專門的調查和研究，變得愈發重要和迫切。這不僅有助於了解網路犯罪的特點和影響，還能爲制定有效的預防和應對策略提供科學依據。

許多網路犯罪被害研究使用非隨機的特殊樣本，例如大學生（Al-Hasani, Zain, Azrag, & Edris, 2022；Lin, Wu, Sun, & Qu, 2023；Mwiraria, Ngetich, & Mwaeke, 2024；Reyns, Henson, & Fisher, 2011），這限制研究結果的推論性，難以將研究結果推論到一般人群。本研究使用更具代表性的隨機樣本，透過網路問卷調查，分析3,056位網路使用者的犯罪被害經驗，了解被動犯罪被害（如網路資料 / 寶物被盜、侵害智慧財產權、網路侵入 / 破壞、隱私權被侵害等）與互動犯罪被害（如妨害電腦使用、詐欺、賭博、色情、妨害名譽、恐嚇）的分布狀況，探討人口特性、網路生活型態、情境機會與網路犯罪被害的關聯性。不僅可以更準確地了解網路犯罪被害情況的普遍性，識別不同人群的特定風險因素，亦可透過多元迴歸分析，以檢驗犯罪被害者學理論對網路犯罪被害的解釋力，思考如何運用情境犯罪預防以降低網路犯罪被害。

貳、相關文獻

一、個人特性與網路被害型態

官方網路被害統計與相關實證研究表明，性別、年齡、教育程度等個人特性與網路被害型態密切相關。人口特性亦影響網路犯罪風險，以性別面向來看，男性網路被害經驗多於女性（葉雲宏，2008；陳玉書等，2020；Auwal & Lazarus, 2024），但性別影響尚存爭議（Mwiraria et al., 2024；Ngo & Paternoster, 2011）。以年齡差異來看，年齡與網路詐欺、遭電腦病毒感染等負相關（Leukfeldt et al., 2017；Marttila, Koivula, & Räsänen, 2021；Mwiraria et al., 2024）。以教育程度對網路被害之關聯性而言，實證研究結果不一，有稱高教育程度者可能面臨更多網路詐欺風險（黃祥益，2006），或言教育程度較低者遭網路犯罪被害的可能性較高（Mwiraria et al., 2024），但亦有研究認爲無顯著影響（Marttila et al., 2021；Ndubueze, Igbo, & Okoye, 2013）。Wang、Duan 與 Jin（2025）針對中國18省4,293位50歲以上網路使用者進行研究，發現高社經地位者更常成爲詐騙目標，但實際損失風險較低；反之，低社經地位者雖較少被針對，卻更容易遭遇財務損失。 此結果支持 SES 與「被詐騙針對」之正相關性，但與「實際受害」無顯著關聯。

這些變項反映不同個體在網路環境中面臨的被害風險差異。例如，研究發現年

輕人由於較高的網路使用頻率，可能成爲某些類型網路犯罪（如詐騙或網路騷擾）的高風險群體，而教育程度可能影響使用者在面對網路威脅時的應對能力。總結來看，網路被害風險與監護措施、人口特性及生活方式密切相關，本研究整合相關影響因子，並進一步探討各變項間對網路被害經驗之預測力。

二、網路生活型態與網路被害

日常活動理論（Routine Activity Theory, RAT）認爲，犯罪發生須具備三要素的時空匯聚：動機犯、合適目標與缺乏監護人（Cohen & Felson, 1979），強調犯罪機會來自個體行爲與時空環境交互，而非社會結構差異。相對地，生活型態暴露理論（Lifestyle Exposure Theory, LET）則認爲，個人的社會角色與生活型態選擇深受其社會結構位置（如年齡、性別、社經地位）所形塑，這些選擇進一步決定其接觸潛在加害者的機會與暴露風險（Hindelang, Gottfredson & Garofalo, 1978）。

近年來，犯罪學研究試圖使用生活型態－日常活動理論（Lifestyle-Routine Activities Theory, 簡稱 LRAT）來解釋犯罪受害的原因（Fisher, Cullen, & Turner, 2002; Holt & Bossler, 2008; Osgood, Wilson, O'Malley, Bachman, & Johnston, 1996）。其中 Holt 與 Bossler（2008）檢視 LRAT 理論對於解釋網路犯罪被害的適用性，研究發現，該理論部分適用於解釋網路騷擾，特別是「接觸動機犯」「目標適合性」和「暴露於高風險情境」有較強的解釋力，而「有力監護」在網路環境下效果有限。然而，有效的監護人（capable guardians）不僅需具備監督、偵測潛在犯罪者與主動介入的能力與意願（Lee & Wang, 2024；Reynald, 2009, 2010, 2011a）；其形式也可以是非正式的社會關係角色，如家人、鄰居、老師、同儕等在預防過程中所扮演的角色（Hollis, Felson, & Welsh, 2013；Parti, 2023）。 然而，在網路空間中，由於虛擬環境缺乏明確的時空邊界與物理接觸，RAT 與 LRAT 的核心變項在實證測量上面臨挑戰（Marttila et al., 2021；Vakhitova & Reynald, 2015）。例如，「接近性」與「監護人」的概念在網路情境下需重新定義 —— 如是否有反詐警示系統、社群平台上的社會回饋機制、家庭成員是否協助監督等，皆爲值得探討的延伸指標。Vakhitova、Reynald 與 Townsley（2016）探討過往的網路犯罪被害研究對 RAT、LET 的實證支持不一致，認爲係該等研究所使用的理論概念（如與加害者之接近程度、目標吸引力 / 合適的目標等）的測量方法可能並不合適。研究者

須對網路犯罪事件所涉及的機制深入分析，找到在網路空間的關鍵理論概念定義和操作化方法，俾產生更穩定的實證結果。

過去的犯罪被害理論與相關研究（Herrero, Torres, Vivas, Hidalgo, Rodríguez, & Urueña, 2021；Holt, Bossler, & Seigfried-Spellar, 2016；Leukfeldt et al., 2017；Vakhitova et al., 2016）指出，網路生活型態在網路犯罪被害中扮演重要角色。具體而言，頻繁使用社交媒體、參與網路遊戲或電子商務的行爲可能增加被害機會（Marttila et al., 2021）。此外，某些網路活動模式（如公開分享個人資訊或點擊不明連結）可能提高網路被害的風險。

三、情境機會與網路犯罪被害

（一）標的吸引力

「網路犯罪的發生，除了需要有動機的犯罪人在網路上尋找合適的被害標的物外，犯罪事件的完成還必須具備另一個重要要素，即加害者必須有實施犯罪的機會」（Cloward, 1959；Cullen, 1983）。環境犯罪學者認爲，透過減少犯罪機會、提高網路安全監控能力、降低被害誘因，比起企圖改變犯罪人的犯罪動機更爲容易。因此，情境機會成爲預防網路被害發生的策略（Clarke, 1980, 1997；Guerra & Ingram, 2022；Smith & Clarke, 2012）。依據 RAT（Cohen & Felson, 1979）與相關研究（陳玉書、王秋惠，2011；Herrero et al., 2021；Mikkola, Kaakinen, Savela, Oksa, Savolainen, & Oksanen, 2024；Ngo & Paternoster, 2011；Reyns, 2010），標的吸引力和監控缺乏是解釋網路犯罪被害的重要因素。標的吸引力指的是個人或其資產對犯罪者的吸引力，例如擁有高價值的數位資產或敏感個人資料。

Felson（1998）認爲，從網路潛在加害者的觀點來看，「被害標的物」選擇的關鍵要素爲價值（Value）、可移動性（Inertia）、可見性（Visibility）、可接近性（Access）等四大特徵（簡稱 VIVA）。其中，網路標的物的價值（V）即是指網路中的熱門商品，對潛在的網路犯罪者來說是高價值或易吸引注意的；其次，標的物的可移動性（I）指在網路購物或交易過程中，大多利用虛擬貨幣或線上刷卡交易，網路金錢交易及買賣物品的可移動性相當快速，被害標的物的下載、移動比實體更難掌握（黃俊祥，2007；Özaşçılar, Çalıcı, & Vakhitova, 2024；Yar, 2005）。再者，

對潛在加害者而言，虛擬網路標的物的可見性（V）指加害者可以接近被害者的途徑，隨著 5G 網路時代的來臨，幾乎人人手機皆可上網，亦大大增加網路資訊及被害者的可見性（黃俊祥，2007；Notté, Leukfeldt, & Malsch, 2021）。最後，網路標的物的可接近性（A）指標的物的可接近性及是否易於逃脫，對網路犯罪者來說，網路幾乎無時間及空間限制，加害人隨時隨地可以在不同地點及時間犯案，較容易躲避執法人員的追緝（王秋惠，2007；Nzeakor & Nwoke, 2023）。綜上，網路被害標的物 VIVA 特徵愈多，愈容易成爲潛在犯罪者的目標。

（二）監控缺乏

監控缺乏則反映在網路環境中，被害者因缺乏防護措施或安全意識，增加犯罪者的可乘之機。因此，網路監控遏阻能力亦爲一重要指標。相比實體世界，網路生活型態與犯罪被害網路犯罪監護可分爲數位（如防毒程式）與個人（如複雜密碼），並新增社會監控（如家庭成員的在場）。然而，實際上在網路上的社會監控較難干涉，因此，有能力的監控者較少（Parti, 2023；Yar, 2005）。

然而，網路監控之有效性存在爭議：一些研究認爲監護措施降低犯罪風險（Buil-Gil & Barrett, 2022；Williams, 2016）；Ngo 和 Paternoster（2011）認爲可利用防毒軟體和防火牆等實體監控，以及提高個人電腦知識與網路素養教育等個人監控方法，以有效在網路空間中進行監控。Hollis 等人（2013）進一步研究發現，青少年使用電腦時，是否有其他人或父母 / 監護人監控上網情況，與青少年被害風險呈現負相關，顯示網路監控遏阻能力愈高，可降低青少年網路被害機會。但也有研究指出，安全措施反而增加風險（Ngo & Paternoster, 2011；Parti, 2023；Reyns, Henson, & Fisher, 2016）。Akdemir 和 Lawless（2020）發現，安裝防毒軟體等措施與網路犯罪風險呈正相關，如惡意軟體感染風險增加兩倍（Exp. (B)=2.062）。可能原因包括使用者因安全感錯覺而從事高風險行爲，以及橫斷面研究設計的限制。另一方面，僅下載已知檔案可有效降低風險（Exp. (B)=0.791）。因此，研究建議使用者應採取多元策略，避免高風險行爲並保持警覺性。

四、綜合理論模式的構建

基於上述文獻，性別、年齡、教育程度等個人特性與網路被害型態有關聯

性，此外，過去的犯罪被害理論或相關研究亦發現網路生活型態（Herrero et al., 2021；Holt et al., 2016；Leukfeldt et al., 2017；Vakhitova et al., 2016）以及標的吸引與監控缺乏（陳玉書、王秋惠，2011；Cohen & Felson, 1979；Herrero et al., 2021；Mikkola et al., 2024；Ngo & Paternoster, 2011；Reyns, 2010）可有效解釋網路犯罪被害。本研究整合網路使用者的人口結構、網路生活型態和情境機會，以建構解釋網路被害的理論模式（參見圖1）。這一模式不僅關注個人特性與生活型態，還結合標的吸引力與監控缺乏的情境因素，企圖從多維度分析網路被害的成因，進一步爲預防網路犯罪被害提供理論支持。期能更全面解釋網路被害的發生機制。

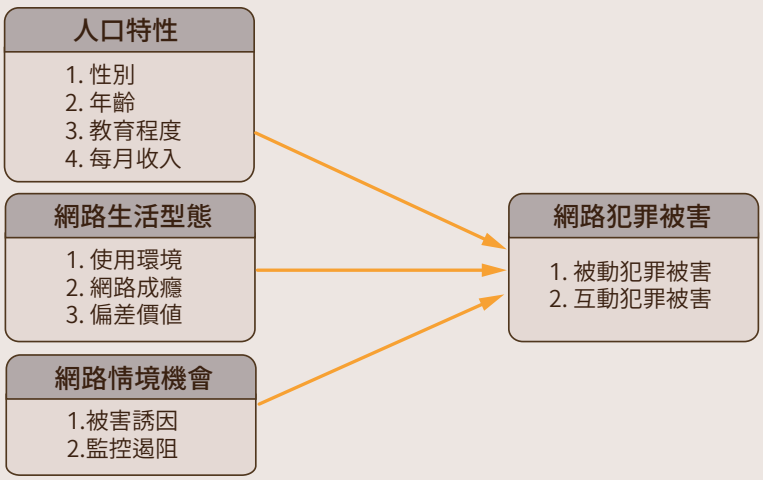

圖1 本研究概念架構

參、研究設計與實施

一、研究方法

本研究針對18歲以上的網路使用者，透過網路和街頭問卷調查進行。研究團隊編製「網路被害調查問卷」，並在正式調查前，根據科技部補助的專題研究計畫（2019/8-2020/7，108-2410-H-015-009）專家和學者的建議，完成初稿。問卷設計爲 Survey Cake 網路調查，於2020年12月11日至2021年1月24日進行預試，共完成163份樣本。根據預試結果，修改正式問卷，並規劃調查方式和無效樣本處理標準。

本研究於2021年2月8日至5月16日進行，調查對象爲居住於台澎金馬地區且年滿18歲之網路使用者，填答者可獲得100元7-11禮券作爲回饋。採用便利抽樣及滾雪球抽樣方式，主要透過 Facebook、PTT、Dcard 等社群平台公告，合作學校與校友會寄送電子郵件，以及學校群組與 LINE 社群公告問卷連結與 QR code，開放符合資格者自願填答。

本研究調查說明頁詳述研究目的、方式、時間、受訪者權益、匿名性及個人資料保護等資訊，受訪者需同意後方可參與。調查期間共有3,841人填答，最終有效樣本數爲3,056人，占97.26%（參見表1）。爲確保受測者身分，系統記錄填答 IP 位置，並排除境外或無法辨識之樣本。問卷亦設計篩選機制，自動剔除未滿18歲或填報出生年不符者。無效樣本包括未滿18歲、填答時間少於8分鐘、IP 重複、機器填答或答案不合邏輯等情況。

本研究爲避免單一資料來源可能造成偏誤，並提升樣本多元性與代表性，特別納入不同來源樣本，採配額抽樣以平衡性別、中低階層職業者及18至35歲年齡層比例。最終網路有效問卷2,942份（96.3%）、實體面訪114份（3.7%）。網路問卷中學生樣本計510份（詳見表2），其中44份由高三以上學生以面訪方式填寫。

表1 網路被害調查有效樣本分布

項目	整體受調查人數		完成受訪人數（不含隔離區）	
	人數	%	人數	%
符條件有效樣本	3,056	79.56	3,056	97.26
未滿18歲樣本	28	0.73	28	0.89
人工檢誤刪除無效樣本	58	1.51	58	1.85
隔離區樣本數	699	18.20	-	-
合計	3,841	100.00	3,142	100.00

註：隔離區樣本含進入調查網頁開始填答而未完成調查之受訪者。

二、研究樣本

本研究包含有效樣本數3,056人，其中女性1,581人（51.7%），男性1,475人（48.3%）。在年齡分組中，18至20歲占6.7%，21至30歲占27.7%，31至40歲占

26.9%，41至50歲占18.7%，51歲以上占18.4%。值得注意的是，21至40歲的受訪者合計占54.6%，爲樣本的主要年齡層。

在教育程度方面，大學或專科學歷的受訪者有1,705人（55.8%），研究所及以上學歷者有829人（27.1%），兩者合計占八成以上，顯示受訪者多爲高學歷族群。另外，在每月收入分布中，收入在4萬至未滿6萬元的比例最高，占25.7%；無收入者及收入未滿2萬元者合計占24.3%，顯示部分受訪者可能尚未穩定就業。最後，從職業類別中得知，軍公教人員占33.1%，爲樣本的最大職業類別；其次爲學生（16.7%）及服務業從業者（13.4%）。其他職業類別比例較分散，顯示樣本來源多元，但以特定職業爲主。

本研究樣本特徵顯示，多數受訪者爲年輕至中壯年、高學歷者，收入與職業分布呈現一定多樣性，這樣的多樣性有助於確保研究結果的代表性和可靠性，從而提供更全面的社會洞察。

表2本研究樣本人口特性分布表

變項	人數	%	變項	人數	%
性別（n=3,056）			教育分組（n-3,056）		
女生	1,581	51.7	國中畢（肄）業以下	43	1.4
男生	1,475	48.3	高中畢（肄）業	479	15.7
年齡（n=3,019）			大學或專科畢（肄）業	1,705	55.8
18-20歲	206	6.7	研究所以上	829	27.1
21-30歲	847	27.7	職業（n=3,056）		
31-40歲	821	26.9	學生	510	16.7
41-50歲	571	18.7	軍公教公務員	1,011	33.1
51歲以上	574	18.4	服務業	410	13.4
每月收入（n=3,056）			建築/營造/金融/保險	253	8.3
無收入	403	13.2	交通/運/輸行銷/傳播	87	2.8
未滿2萬元	339	11.1	醫療/法律	170	5.6
2萬至未滿4萬	695	22.7	資訊相關	131	4.3
4萬至未滿6萬	786	25.7	家管/退休	269	8.8
6萬至未滿8萬	476	15.6	其他（無業/農林漁牧等）	215	7.0
8萬以上	357	11.7	總樣本	3,056	100.0

三、研究概念測量

網路被害調查測量工具內容主要包括：人口特性、網路生活型態、網路情境機會和網路被害經驗等，研究概念測量與信度和效度概述如下（參見表3和表4）：

（一）人口特性

包括性別、年齡、教育程度、每月收入等，如表3所示。

表3 人口特性測量項目表

變項	名義變項分組
性別	男、女
年齡	18-20歲、21-30歲、31-40歲、41-50歲、51-60歲、61歲以上
教育程度	國中畢肄業以下、高中畢肄業、大學或專科畢肄業、研究所以上
每月收入	無收入、未滿2萬元、2萬 - 未滿4萬、4萬 - 未滿6萬、6萬未滿8萬、8萬以上

（二）網路生活型態

本構面整合「使用環境」、「網路成癮」與「偏差價值」三項測量構面，反映個體在網路使用中的行爲習慣、心理傾向與價值觀等特質，描繪其網路使用的生活樣貌與風險特徵。各題項採四點量表，依「從未」至「經常」分別給予1至4分。具體分述如下：

1、使用環境

「使用環境」指個體於網路世界中之功能性與娛樂性使用行爲，包含兩個因素：(1) 通訊管道：包括電子郵件、收看新聞及即時通訊等用途，因素負荷量介於 .655 至 .751，信度係數（Cronbach's Alpha）爲 .546，顯示分量表「尚可接受之內部一致性」或「具備基礎的一致性」與效度。(2) 休閒娛樂：涵蓋網路遊戲、社群媒體、影音娛樂及網路購物，因素負荷量介於 .463 至 .716，信度係數爲 .489，顯示分量表的內部一致性與效度良好。

2、網路成癮

「網路成癮」爲反映個體於網路使用上的強迫性與心理依賴傾向，包含兩個因

素：(1) 行爲成癮：包括無法抑制上網慾望、長時間上網、無法控制上網行爲，以及醒來後立即使用手機等情況，因素負荷量介於 .598 至 .773，信度係數爲 .892，展現分量表極高的內部一致性與效度。(2) 心理成癮：包含上網帶來的興奮感、人際互動減少、因上網影響作息等情形，因素負荷量介於 .552 至 .776，信度係數爲 .859，顯示該分量表具有高度一致性與效度。

3、偏差價值

「偏差價值」指評估個體對於具爭議性網路行爲之態度與認知傾向，包括下載盜版軟體、網路謾罵他人、因壓力而網路上發洩，以及說謊或網路詐騙合理化等行爲，因素負荷量介於 .428 至 .721，信度係數爲 .721，分析結果顯示該分量表具有穩定的內部一致性與效度。

（三）網路情境機會

本變數整合「被害誘因」與「監控遏阻」兩構面，對應情境犯罪理論與日常活動理論中「犯罪機會」與「監護能力」之概念，反映使用者在網路環境中所處的風險程度與自我防護能力。兩子構面經因素分析與信度檢驗建立，具備良好建構效度。各題項採四點量表計分，分別對應「從未」至「經常」給予 1 至 4 分。具體內容如下：

1、被害誘因

「被害誘因」爲衡量受訪者接觸或參與高風險網路活動之頻率，包括兩個因素：(1) 偏差資訊吸引：如線上賭博、網路援交、交易贓物或盜版軟體等，因素負荷量介於 .692 至 .802，信度係數爲 .798，顯示高一致性與效度。(2) 曝露風險：如公開打卡、暴露身分訊息等行爲，因素負荷量介於 .430 至 .809，信度係數爲 .518，表現出一定的內部一致性與效度。

2、監控遏阻

「監控遏阻」爲評估受訪者採取安全行爲或具備外部監控資源之程度，包含兩個因素：(1) 安全防護：包括隱私設置、WiFi 安全及官方網站的使用等，因素負荷量介於 .580 至 .779，信度係數爲 .772，顯示高一致性與效度。(2) 實體監控：如安

裝防毒軟體、設定密碼及家人關心等行爲，因素負荷量介於 .502 至 .742，信度係數爲 .573，具備一定的內部一致性。

表 4 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	轉軸後特徵值	轉軸後解釋變異量 %	內部一致性係數
網路生活型態	使用環境				
	通訊管道	.655-.751	1.769	25.27%	.546
	休閒娛樂	.463-.716	1.584	22.63%	.489
	網路成癮				
	行爲成癮	.598-.773	4.312	33.17%	.892
	心理成癮	.552-.776	3.577	27.52%	.859
	偏差價值				
	偏差價值	.428-.721	3.171	35.24%	.721
網路情境與機會	被害誘因				
	偏差資訊吸引	.692-.802	2.851	35.64%	.798
	曝露風險	.430-.809	1.588	19.85%	.518
	監控遏阻				
	安全防護	.580-.779	3.311	30.10%	.772
	實體監控	.502-.742	1.645	14.95%	.573
網路被害	被動犯罪被害	.458-.765	2.695	44.91%	.725
	互動犯罪被害	.463-.733	4.146	37.69%	.806

（四）網路被害經驗

網路被害係指個人使用電腦或通訊軟體網路，遭受到網路偏差或犯罪行爲的侵害；本研究參考周愫嫻（2014）將網路被害區分爲：「互動被害」（包括網購被騙、線上遊戲財物被竊），這些行爲皆需要青少年先與加害對象互動後，才可能發生，也就是「機會型的被害」；另一爲「被動被害」（包括電腦中毒、收到色情圖片和收到大量垃圾郵件）。回答「0 次」者給 0 分、「1 次」者給 1 分、「2 次」者給 2 分、「3 次」者給 3 分、「4 次以上」者給 4 分；其中被動犯罪被害：包括個資盜取、駭客攻擊、檔案盜取、資料刪改等，因素負荷量介於 .458 至 .765，信度係數爲 .725，顯示該分量表具良好的一致性與效度。互動犯罪被害：涵蓋網路詐騙、性騷擾、名譽受損及投資詐騙等，因素負荷量介於 .463 至 .733，信度係數爲 .806，展現高度內部一致性與效度。

肆、研究結果

一、網路被害經驗之分布

由圖2及表5網路被害態樣分布得知，在3,056位有效調查對象中，於過去1年內（2020年）曾經有被駭客攻擊之被害經驗者有824人（占26.96%，M=1.54，SD=1.08）為最多，其餘依序為檔案被盜取有798人（占26.11%，M=1.45，SD=0.92）；第3順位為購物被詐騙有455人（占14.89%，M=1.21，SD=0.59）；第4順位為資料被刪除或更動有259人（占8.48%，M=1.14，SD=0.52）；第5順位為被網路性騷擾有251人（占8.21%，M=1.17，SD=0.67）。每位受調查對象可重複選取被害經驗，經統計分析前5項高風險被害項目，累積已達2,587人次（占84.65%），顯見被駭客攻擊、檔案被盜取、購物被詐騙、被網路性騷擾、資料被刪除或更動等5種項目為最常見之網路被害型態。

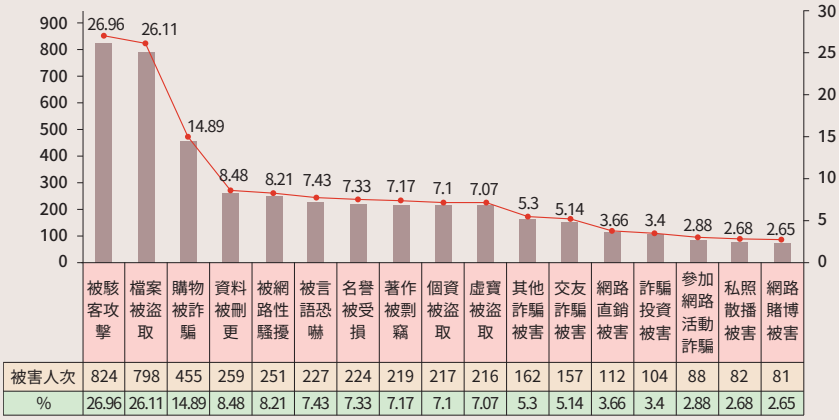

圖2 網路被害之分布圖

表5 網路被害類型之分布

類型	被害項目	被害經驗（人次）	%	平均值	標準偏差
被動犯罪被害	被駭客攻擊	824	26.96	1.54	1.08
	檔案被盜取	798	26.11	1.45	.92
	資料被刪更	259	8.48	1.14	.52
	虛寶被盜取	216	7.07	1.13	.56
	著作被剽竊	219	7.17	1.13	.54
	個資被盜取	217	7.10	1.12	.53

類型	被害項目	被害經驗（人次）	%	平均值	標準偏差
互動犯罪被害	購物被詐騙	455	14.89	1.21	.59
	被網路性騷擾	251	8.21	1.17	.67
	名譽被受損	224	7.33	1.13	.57
	被言語恐嚇	227	7.43	1.13	.54
	交友詐騙被害	157	5.14	1.09	.44
	其他詐騙被害	162	5.30	1.09	.42
	網路直銷被害	112	3.66	1.06	.36
	詐騙投資被害	104	3.40	1.06	.35
	網路賭博被害	81	2.65	1.05	.37
	私照散播被害	82	2.68	1.04	.30
	參加網路活動詐騙	88	2.88	1.04	.28

二、網路生活型態、情境機會與網路犯罪被害之關聯性

（一） 生活型態與網路犯罪被害之關聯性

表6爲網路生活型態與受訪者是否曾經遭受網路犯罪被害之關聯性；在網路使用環境方面，日常生活中較常利用網路從事遊戲或購物者，有較高的網路被動或互動被害風險；而以網路進行即時通訊、收發電子郵件、收看新聞或影音娛樂，與是否成爲網路被動犯罪被害者有顯著關聯，但與互動被害則無顯著關聯。

在網路成癮方面，行爲成癮與心理成癮各測量項目均與網路被動被害或互動被害有顯著關聯性，顯示網路成癮程度越嚴重的網路使用者，在網路上停留的時間越久，越依賴網路與人互動或從事休閒，並影響日常生活作息和心理健康，同時也更容易成爲網路犯罪的標的物。此外，網路偏差價值觀（如：詐騙是本事、被誘做壞事是正常、不實身分不會被發現等）或偏差行爲合理化（如：說壞話不傷人、壓力大可罵人、缺錢竊盜可原諒、非法下載軟體無傷、可對不誠實者說謊等），亦與網路互動被害有顯著關聯性；顯示偏差價值觀不但容易導致犯罪或偏差，亦可能使網路使用者在與人互動過程中被攻擊或詐騙。偏差價值觀各項目與網路被害類型皆呈現顯著關聯，尤以「非法下載軟體無傷害」、「不實身分不會被發現」、「網路上說人壞話無傷害」及「對不誠實者說謊剛好」等題項，在被動與互動被害中皆達顯著水準，且 Gamma 值呈現穩定的正向關聯。整體而言，無論是網路使用行爲（如遊戲與購物）、成癮傾向或偏差態度，多數測量項目與網路犯罪被害間皆有穩定關聯，顯示相關風險傾向具一致性。

表6 生活型態與網路犯罪被害之關聯性

有無被動犯罪被害經驗			有無互動犯罪被害經驗		
項目	χ^2	Gamma	項目	χ^2	Gamma
使用環境			使用環境		
即時通訊	9.557*	.155**	即時通訊	1.362	.023
社群媒體	5.822	.059	社群媒體	6.858	.051
影音娛樂	8.084*	.050	影音娛樂	1.055	.030
電子郵件	17.412**	.073*	電子郵件	1.153	.016
收看新聞	30.068***	.163***	收看新聞	.887	.829
網路遊戲	25.113***	.135***	網路遊戲	16.585**	.119***
網路購物	26.587***	.117***	網路購物	27.109***	.157***
網路成癮			網路成癮		
花太多時間上網	9.714*	.088**	花太多時間上網	32.829***	.167***
上網時間比較長	18.499***	.122***	上網時間比較長	28.198***	.165***
上網多時才滿足	45.030***	.186***	上網多時才滿足	48.083***	.211***
不能控制上網	33.848***	.158***	不能控制上網	57.603***	.220***
醒來第一上網	16.097**	.111***	醒來第一上網	31.345***	.167***
忍不住再上網	44.293***	.169***	忍不住再上網	63.731***	.237***
上網就有精神	27.636***	.147***	上網就有精神	32.477***	.168***
爲減少會沮喪	35.880***	.176***	爲減少會沮喪	57.660***	.233***
不上網坐立不安	49.226***	.191***	不上網坐立不安	59.398***	.224***
上網而互動減少	38.170***	.178***	上網而互動減少	29.448***	.161***
上網而休閒減少	45.042***	.189***	上網而休閒減少	29.230***	.151***
上網而未按時寢食	33.065***	.162***	上網而未按時寢食	42.231***	.193***
興奮感遠勝其他	52.646***	.209***	興奮感遠勝其他	56.167***	.214***
偏差價值			偏差價值		
非法下載軟體無傷害	34.116***	.138***	非法下載軟體無傷害	26.837***	.140***
說人壞話無傷害	19.022***	.135**	說人壞話無傷害	71.819***	.242***
不實身分不被發現	31.651***	.152***	不實身分不被發現	21.199***	.132***
詐騙成功是本事	8.526*	.094**	詐騙成功是本事	17.044***	.138***
誘惑做壞事是正常	6.558	.079	誘惑做壞事是正常	31.536***	.209***
缺錢騙盜可原諒	12.616**	.141*	缺錢騙盜可原諒	36.616***	.269***
對不誠實者說謊剛好	25.682***	.155***	對不誠實者說謊剛好	41.859***	.215***
壓力大可謾罵他人	17.166**	.168**	壓力大可謾罵他人	46.468***	.305***
無防護被入侵活該	16.739**	.120***	無防護被入侵活該	8.708*	.092**

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

（二）情境機會與網路犯罪被害之關聯性

表 7 爲機會情境與網路犯罪被害之關聯性；研究結果顯示，網路被害誘因各測量項目與網路被動或互動被害均存在極顯著關聯性；當網路使用者接觸到較多的盜版軟體、線上賭博、網路援交、販賣贓物或違禁物品等與犯罪有關的資訊，以及較常點開不明網址 / 檔案、公開打卡或公開個人身分等行爲而暴露自己的連結或身分，較容易成爲被動與互動網路被害的標的物，而成爲網路被害者。

而網路情境中的監控遏阻與網路犯罪被害之間的關聯，在顯著性上表現較不一致。在被動犯罪被害方面，例如「注意留下個資」、「瀏覽紀錄」或「使用安全 WiFi」的行爲，與降低被動被害風險呈現負向關聯；但「安裝防毒軟體」、「使用不同密碼」與「瀏覽工具使用說明」等變項，則與被害風險呈現正向顯著關聯。

表 7 情境機會與網路犯罪被害之關聯性

有無被動犯罪被害經驗			有無互動犯罪被害經驗		
項目	χ^2	Gamma	項目	χ^2	Gamma
被害誘因			被害誘因		
點開不明網址 / 檔案	57.154***	.243***	點開不明網址 / 檔案	71.343***	.289***
看到盜版軟體訊息	46.313***	.200***	看到盜版軟體訊息	63.140***	.240***
看到線上賭博訊息	46.474***	.196***	看到線上賭博訊息	63.555***	.245***
看到網路援交訊息	47.519***	.189***	看到網路援交訊息	70.344***	.242***
看到買賣贓物訊息	40.317***	.244***	看到買賣贓物訊息	70.649***	.315***
看到違禁物品訊息	39.604***	.272***	看到違禁物品訊息	79.731***	.381***
在網路公開打卡	31.139***	.124***	在網路公開打卡	31.467***	.173***
在網路公開身分	50.479***	.240***	在網路公開身分	78.982***	.278***
監控遏阻			監控遏阻		
家人關心上網內容	7.675	.076**	家人關心上網內容	18.268***	.113***
安裝防毒軟體	8.477*	.039	安裝防毒軟體	9.654*	.007
設定時數上網時數	2.907	-.026	設定時數上網時數	2.209	.026
注意留下個資情況	17.592**	-.020	注意個資留下個資	16.023**	-.038
檔案加密習慣	5.973	.046	檔案加密習慣	2.509	.023
使用不同密碼	19.560***	.040	使用不同密碼	8.190*	-.023
注意瀏覽紀錄 / 追蹤	8.138*	-.015	注意瀏覽紀錄 / 追蹤	5.655	-.066*
避免不明網站下載	26.029***	.032	避免不明網站下載	19.554***	-.043
使用安全 WiFi	17.203**	-.002	使用安全 WiFi	9.223*	-.066*

有無被動犯罪被害經驗			有無互動犯罪被害經驗		
項目	χ^2	Gamma	項目	χ^2	Gamma
提升工具隱私保護	6.923	.025	提升工具隱私保護	8.664*	-.088**
瀏覽工具使用說明	12.207**	.001	瀏覽工具使用說明	8.471*	-.057

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

值得注意的是，當卡方檢定與 Gamma 係數在顯著性或方向上出現差異時，需分別解讀其統計意涵。卡方檢定主要用來判斷變項間是否有顯著關聯，較易受樣本數影響；而 Gamma 係數則反映關聯的方向與強度，尤其適用於有序類別資料。以「注意瀏覽紀錄 / 追蹤」與互動犯罪被害爲例，卡方檢定未達顯著（χ^2=5.655），但 Gamma 呈現顯著負向（-.066*），顯示雖整體關聯性不高，但存在趨勢，可能代表愈注意紀錄的使用者，其互動被害風險略低。反之，「使用不同密碼」與被動被害的卡方結果達顯著（χ^2=19.560***），但 Gamma 值偏低（.040），表示雖然整體有關聯，但強度較弱，推論時應避免過度詮釋。

因此，如欲釐清上述安全防護措施與犯罪被害的因果關係，尚須進一步觀察所採取的監控遏阻措施爲被害前或被害後的作爲。在互動犯罪被害方面，注意留下個資、使用不同密碼、避免在不明網站下載、使用安全 WiFi、提升工具隱私保護和瀏覽工具使用說明等安全防護措施，可以有效提高監控力和減少互動被害風險。

三、各影響因子與網路犯罪被害之相關

（一）人口特性與網路犯罪被害之相關性

由表 8 人口特性與「被動犯罪被害」相關分析得知，性別（r=.078***）、每月收入（r=.090***）與被動犯罪被害有顯著正相關，年齡、教育程度與被動犯罪被害則未達顯著相關，表示被動犯罪被害次數愈高，愈可能是男性，每月收入較高；反之，被動犯罪被害次數愈低，愈可能是女性，每月收入較低，惟變項間之關聯性僅屬微弱低度相關。另由人口特性與「互動犯罪被害」相關分析得知，性別（r=.083***）與互動犯罪被害有顯著正相關，教育程度（r=-.062**）與互動犯罪被害有顯著負相關，年齡、每月收入與互動犯罪被害則未達顯著相關，表示互動犯罪被害機率愈高，愈可能是男性，教育程度較低；反之，互動犯罪被害機率愈低，愈可能是女性，教育程度較高，但變項間係屬於微弱的低度相關。

表 8 人口特性與網路犯罪被害之相關分析

變項	1	2	3	4	5	6
1. 被動犯罪被害	1					
2. 互動犯罪被害	.542***	1				
3. 性別	.078***	.083***	1			
4. 年齡	-.010	-.030	-.040*	1		
5. 教育程度	.016	-.062**	-.053**	.180***	1	
6. 每月收入	.090***	.015	.122***	.417***	.450***	1

註：性別爲類別變項（n=3,019；遺漏值 =37）：女 =0；男 =1；教育程度爲次序變項：1= 國中畢肄業以下；2= 高中畢肄業；3= 大學或專科畢肄畢；4= 研究所以上；每月收入爲次序變項：1= 無收入；2= 未滿 2 萬，3=2 萬至未滿 4 萬；4=4 萬至未滿 6 萬；5=6 萬至未滿 8 萬；6=8 萬以上。*p<.05；**p<.01；***p<.001

（二）網路生活型態、情境機會與網路犯罪被害之相關性

由表 9 得知，「被動犯罪被害」與「互動犯罪被害」二變項呈現顯著正相關（r=.542***），被動犯罪被害次數愈高，互動犯罪被害次數也愈高，二變項間屬於中度相關性。另「被動犯罪被害」與網路生活型態（r=.088***）、使用環境（r=.087***）、網路成癮（r=.153***）、偏差價值（r=.178***）、網路情境機會（r=.131***）、被害誘因（r=.252***）呈現顯著低度相關性，但監控遏阻與被動犯罪被害之相關性未達顯著水準。顯示使用網路愈頻繁、有偏差價值觀、網路成癮者、經常把自己曝露於風險之中的使用者，個人個資、檔案、資料、著作、虛擬寶物等遭盜取或剽竊的機會較高，換言之，該類型網路使用者，屬於「被動犯罪被害」高風險者。

另外，「互動犯罪被害」與網路生活型態（r=.065***）、網路成癮（r=.166***）、偏差價值（r=.227***）、網路情境機會（r=.165***）、被害誘因（r=.301***）呈現顯著低度相關性，但「互動犯罪被害」與使用環境、監控遏阻並未達顯著水準，表示網路使用者無論收發信件、收看新聞、使用即時通訊等通訊管道，還是利用網路上網購物、網路遊戲、社群媒體、觀賞影音等休閒娛樂，與是否容易陷入網路「互動犯罪被害」風險沒有關聯性。此外，有沒有使用安全防護與實體監控，亦不會與「互動犯罪被害」產生關聯。相反地，網路名譽受損、網路投資遭詐、私照遭散布、言語遭恐嚇、購物遭詐欺等具有互動性質的網路被害類型，與「網路成癮」、「偏差價值觀」、「被害誘因」等因素具有顯著的相關性。

因此，網路生活型態、網路情境機會與網路「被動」與「互動」犯罪被害有顯著關聯性，網路成癮性、偏差價值觀、處於高風險的被害誘因、監控能力不足等特徵，易產生較高的網路被害情境及機會，網路被害次數亦較高。

表9 網路生活型態、情境機會與網路犯罪被害之相關分析

	1	2	3	4	5	6	7	8	9
1. 被動犯罪被害	1								
2. 互動犯罪被害	.542***	1							
3. 網路生活型態	.088***	.065***	1						
4. 使用環境	.087***	.034	.556***	1					
5. 網路成癮	.153***	.166***	.877***	.319***	1				
6. 偏差價值	.178***	.227***	-.193***	.049***	.212***	1			
7. 網路情境機會	.131***	.165***	.252***	.351***	.238***	.151***	1		
8. 被害誘因	.252***	.301***	.288***	.269***	.369***	.285***	.636***	1	
9. 監控遏阻	-.001	.009	.130***	.270***	.058**	.003	.855***	.143***	1
平均值（M）	1.51	1.07	85.28	22.53	31.51	13.76	43.37	13.90	29.47
標準偏差（SD）	2.83	2.95	9.97	2.99	8.61	3.90	7.59	3.99	5.92

* p < .05；** p < .01；*** p < .001

四、網路犯罪被害迴歸分析

（一）網路「被動犯罪被害」之影響因素分析

由表10模式三可知，以人口特性、網路生活型態、情境機會對網路「被動犯罪被害」之影響效果。分析結果發現，整體模型可解釋網路「被動犯罪被害」變異中的8.9%，F=32.479，p<.001，表示此模式的解釋能力達顯著水準。控制人口特性及網路生活型態之後，網路情境機會可以增加3.3% 的網路「被動犯罪被害」解釋變異量。其中每月收入（β=.084；p<.001）、網路成癮（β=.059；p<.01）、偏差價值（β=.105；p<.001）、被害誘因（β=.208；p<.001）對網路「被動犯罪被害」有顯著影響。由標準化 β 值可知，對網路「被動犯罪被害」之影響因子中，以被害誘因最大、偏差價值次之，每月收入再次之，網路成癮影響力較小。綜上，對網路「被動犯罪被害」而言，網路被害誘因愈大，偏差觀念愈多，每月收入至少2萬元以上，且有網路成癮現象者，使用網路的被害機率皆會愈高。

表 10 網路被動犯罪被害影響因素之迴歸分析（ n=3,019）

自變項		模式一		模式二		模式三	
		B	β	B	β	B	β
人口特性	性別 [a]	.397***	.070	.260*	.046	.083	.015
	年齡	-.010*	-.047	.001	.003	.008+	.035
	教育程度 [b]	-.009	-.001	-.100	-.013	-.029	-.004
	每月收入 [c]	.675***	.102	.624***	.094	.555***	.084
網路生活型態	使用環境			.037*	.039	.016	.017
	網路成癮			.037***	.114	.019**	.059
	偏差價值			.103***	.142	.077***	.105
情境機會	被害誘因					.148***	.208
	監控遏阻					-.017+	-.035
（常數）		.554***		-2.982***		-3.346***	
F 值		10.911***		25.557***		32.479***	
df		4		7		9	
R^2 （ Adj R^2）		.014（.013）		.056（.054）		.089（.086）	

註： a 性別：0= 女性， 1= 男性，設定「女性」當參考組 ; b 教育程度：0= 高中職畢肄業以下，1= 大學及研究所以上，設定「高中職畢肄業以下」當參考組 ; c 每月收入二組：0= 無收入及未滿 2 萬元，1= 每月 2 萬元以上，設定「無收入及未滿 2 萬元」當參考組。d 人口特性，扣除 37 名遺漏值，故樣本數 n=3,019。e 本研究採用強迫輸入法（enter method），依據理論或邏輯推論，依序將自變項置入迴歸模型中，以檢驗各自變項對依變項之影響力。+p< .1; *p<.05; **p<.01; ***p<.001

（二）網路「互動犯罪被害」之影響因素分析

由表 11 模式三可知，以人口特性、網路生活型態、情境機會對網路「互動犯罪被害」之影響效果。分析結果發現，整體模型可解釋網路「互動犯罪被害」變異中的 12.4%，F=47.158，p<.001，表示此模式的解釋能力達顯著水準。控制人口特性及網路生活型態之後，網路情境機會可以增加 5.1% 的網路「互動犯罪被害」解釋變異量。其中年齡（β=.056；p<.01）、教育程度（β=-.072；p<.001）、使用環境（β=-.045；p<.05）、網路成癮（β=.065；p<.001）、偏差價值（β= .146；p<.001）、被害誘因（β=.261；p<.001）對網路「互動犯罪被害」有顯著影響。由標準化 β 值可知，對網路「互動犯罪被害」之影響因子中，以被害誘因最大、偏差價值次之，教育程度與網路成癮再次之，網路使用環境的影響力較小。

本研究發現，分析比較網路互動或被動犯罪被害的共同性，「被害誘因」、「偏差價值」及「網路成癮」皆容易造成網路被害的發生。綜上，對網路「互動犯罪

被害」而言，年齡較長、學歷較低、網路使用環境不安全、被害誘因愈大，偏差觀念愈多，且有網路成癮現象者，網路的被害機率皆會愈高。

表 11 網路互動犯罪被害影響因素之迴歸分析（ n=3,019）

自變項		模式一		模式二		模式三	
		B	β	B	β	B	β
人口特性	性別 [a]	.408***	.070	.222*	.038	-.020	-.003
	年齡	-.007	-.032	.003	.015	.013**	.056
	教育程度 [b]	-.588***	-.076	-.625***	-.080	-.561***	-.072
	每月收入 [c]	.263+	.039	.246	.036	.176	.026
網路生活型態	使用環境			-.009	-.009	-.044*	-.045
	網路成癮			.045***	.133	.022***	.065
	偏差價值			.144***	.192	.110***	.146
情境機會	被害誘因					.191***	.261
	監控遏阻					-.006	-.012
（常數）		1.771***		-1.645***		-2.397***	
F 值		9.488***		34.109***		47.158***	
df		4		7		9	
R^2（Adj R^2）		.012（.011）		.073（.071）		.124（.121）	

註： a 性別：0= 女性，1= 男性，設定「女性」當參考組；b 教育程度：0= 高中職畢肄業以下，1= 大學及研究所以上，設定「高中職畢肄業以下」當參考組；c 每月收入二組：0= 無收入及未滿 2 萬元，1= 每月 2 萬元以上，設定「無收入及未滿 2 萬元」當參考組。d 人口特性，扣除 37 名遺漏值，故樣本數 n=3,019。e 本研究採用強迫輸入法（enter method），依據理論或邏輯推論，依序將自變項置入迴歸模型中，以檢驗各自變項對依變項之影響力。+p< .1;*p<.05; **p<.01; ***p<.001

伍、結論與建議

新冠肺炎（COVID-19）的盛行，嚴重威脅民眾的健康與生命，亦改變人們的生活型態，使人們更依賴網路、通訊軟體和電子科技產品。本研究透過網路和實體問卷調查，觀察網路犯罪被害類型之分布，結合 LET 和 RAT 影響網路被害之顯著因子。研究結果發現，在虛擬世界中，網路與通訊軟體使用者，只要留下的連結，即可能成爲網路犯罪被動被害者（passive victim），如逾 26% 受訪者曾遭受駭客攻擊或檔案被盜取經驗，而刪除或更改和寶物被盜取等亦爲較常見的被動被害類型。此外，只要曾經與網友、網頁或軟體產生互動，即使在時間上有落後效應，在

空間或連結重疊情況下，亦可能遭受網路犯罪互動被害（interactive victim），如約15% 受訪者表示曾有購物詐騙被害經驗，約3%-5% 受訪者分別遭受交友詐騙、投資詐騙或其他詐騙被害，顯示網路詐騙爲互動被害的主要類型，且態樣相當多元；而網路性騷擾、名譽受損和言語恐嚇等亦爲較常見的網路互動被害類型（被害率約7.3%-8.2%）。

Hindelang 等人（1978）的 LET 普遍被應用於解釋實體社會的犯罪被害，並獲得相當穩定的實證資料支持；近年相關實證研究顯示，LET 亦能有效解釋網路犯罪被害（簡鳳容，2018；陳玉書等，2020; Reyns, 2013；Van Wilsem, 2013；Vakhitova et al., 2016；Reyns et al., 2011；Leukfeldt & Yar, 2016）。就被害者人口特性而言，本研究發現，男性網路使用者之網路被動或互動被害比率顯著高於女性，此項研究結果與葉雲宏（2008）、陳玉書等人（2020）和 Ndubueze 等人（2013）之研究結果一致 ，在控制教育和年齡等人口特性情況下，網路被害的性別差異相當顯著。此外，收入較高者亦較容易成爲網路被動犯罪被害的標的，而教育程度對網路互動被害有顯著負向影響力，隨著教育程度上升，互動犯罪被害的次數顯著下降。收入和教育程度均爲測量社會經濟地位的重要指標，可反應出個人的消費與生活娛樂模式，至於如何影響不同網路被害類型（如詐欺、被動被害或網路賭博等），尚須進一步分析觀察。

本研究以網路使用環境、網路成癮和偏差價值觀來衡量網路生活型態，無論以有無網路被動 / 互動犯罪被害經驗或被害次數爲依變項，網路成癮、偏差價值觀與網路被害均存在顯著關聯性，多元迴歸分析結果亦呈現穩定的負向影響力，顯示網路成癮使個人在心理和行爲上依賴網路與通訊軟體；而對網路偏差或犯罪等合理化的偏差價值觀，則使個人暴露於高風險情境。因此，網路成癮與偏差價值觀除導致網路犯罪或偏差行爲（曾淑萍、蘇桓玉，2011；王茜，2014；呂詩涵、胡嘉文，2015；徐文堂，2015；呂敏綺，2016；黃凱柔，2016），亦爲影響網路犯罪被害的顯著因子。另透過網路從事遊戲或購物者其是否遭受網路被害有顯著關聯，利用網路從事新聞、影音娛樂或傳收信件者，則較易成爲網路被動被害者。整體而言，本研究有關網路生活型態的結果相似（簡鳳容，2018；Van Wilsem, 2011；Reyns, 2013; Leukfeldt & Yar, 2016）；並呼應 Vakhitova 等人（2016）主張：須有正確之概念測量，方可驗證網路空間中接觸潛在犯罪者管道會影響犯罪被害的觀點。

在情境機會方面，網路環境中的身分暴露或受不安全 / 偏差訊息吸引，均可能使個人成爲合適標的物，本研究結果顯示，在網路上公開打卡、公開身分或接觸賭博、援交、違禁物品等訊息者較容易成爲網路犯罪被害者；且對網路被動或互動犯罪被害最具顯著性的影響因子，亦即被害誘因爲解釋網路犯罪被害的關鍵；此項結果與 Ngo 和 Paternoster（2011）的研究發現一致。但 Cohen 和 Felson（1979）的 RAT 如運用於解釋網路被動與互動犯罪被害事件，被害者、網路 / 通訊訊息、潛在加害者所扮演的 VIVA 功能，與實體社會可能有所不同，亦值得深入探討。在遏阻監控方面，各測量項目與有無網路被害經驗的關聯性檢定發現，使用不同密碼、安全 WiFi 或提升工具隱私等保護安全防護作爲與網路互動犯罪被害具有負向關聯性，亦即較能有效遏阻互動犯罪被害，此項發現與 Hollis 等人（2013）的研究結果相似；整體而言，實體監控可遏阻網路被害的假設僅部分獲得統計上的支持；有關遏阻監控的概念測量與被害經驗的時間順序，在未來研究中如有較妥適的測量，或能獲得較穩定的實證支持。

根據本研究有關網路被動與互動犯罪被害分析結果，就增加犯罪困難度、降低被害風險、減少犯罪誘因 / 刺激和去除犯罪藉口等四個面向，提出預防網路犯罪被害的對策（參見表 12）。未來有關網路被害之研究，可就個別網路犯罪被害型態進行深入探討，如網路霸凌、網路跟蹤騷擾、網路賭博和各類網路詐欺等，均爲重要的研究議題。

在研究工具方面，建議後續可透過專家諮詢強化問卷設計，同時納入其他被害者學理論，探討其與網路被害現象之間的關聯性。儘管本研究模型具統計上之預測效果，但整體解釋力仍有限。部分變項雖達顯著水準，效果量卻偏低，顯示社會人口背景對網路被害的影響有限。此外，監控遏阻構面中雖有些防護行爲與被害風險呈現顯著關聯，但在多變項迴歸中其獨立解釋力較弱，可能反映統計方法在控制變項與分析層次上的差異，也顯示網路被害的成因相當多元且複雜。

未來研究可進一步擴展範疇，納入人格特質、網路素養與社交網絡等潛在影響因素，並涵蓋更多類型的網路被害，區分被害者特性，進行情境差異分析，以提升模型的整體解釋力與對被害機制的理解。同時，亦應關注不同統計方法對結果詮釋的影響，避免過度依賴單一分析結果，以強化研究的理論深度與實務應用價值。

另一方面，樣本來源與調查方式亦爲本研究的限制之一。網路問卷雖具便利性，但可能集中特定族群，影響樣本代表性。本研究樣本在收入與職業上偏向中高收入與特定類別，可能與網路調查較易吸引具教育背景者參與有關。未來可考慮輔以實體調查，並採用分層或配額抽樣，以修正偏誤並提升樣本的多元性與代表性，進一步比較不同背景群體的差異。

表 12 網路犯罪被害情境預防措施

情境預防	網路犯罪被害預防措施
增加犯罪困難度	1. **強化標的防護力。**如：安裝防毒軟體、使用不同密碼 2. **管制連結網址 / 群組。**如：使用安全 WiFi、避免連結不明社群或群組（被動）；避免連結不安全新聞來源 / 影音（被動）；避免在不明網站下載資料（被動） 3. **安全傳輸資料。**如：避免向不安全 / 不明帳號傳送電子郵件（被動）
降低被害風險	1. **提高監控力。**如：注意瀏覽工具使用說明；家人關心上網內容（互動） 2. **降低暴露風險。**如：減少在網路公開打卡；避免在網路公開身分；檢視瀏覽紀錄 / 追蹤，定期刪減不使用紀錄（被動） 3. **提高匿名性。**如：注意留下個資狀況；提升工具隱私保護（互動）
減少犯罪誘因 / 刺激	1. **避免刺激物。**如：避免瀏覽偏差或犯罪訊息；避免下載不明網站資料 / 影音；避免點開不明網址 / 檔案。 2. **紓解壓力。**如：從事傳統休閒娛樂；選擇有益身心網路休閒或娛樂；養成良好網路使用習慣
去除犯罪藉口	1. **健全網路使用規範。**如：加強青少年網路規範和法制教育；落實網路分齡管制以免偏差價值影響；規範網路軟體 / 通訊 / 遊戲等守則，確立相關違法罰則； 2. **落實使用者身分聲明和簽署使用同意書提醒使用者違法處罰。**如：在網頁或連結上顯示使規範和身分限制（如：限成年）；在網頁或連結上顯示非法下載或散播罰則 3. **覺察 / 處理網路成癮問題。**如：協助家庭 / 學校覺察網路成癮傾者；提供網路成癮者身心治療訊息和管道

註：表中預防措施如僅限於被動被害預防以「被動」標示，如僅限於互動被害預防以「互動」標示，餘則通用於被動或互動網路犯罪被害預防。

陸、參考文獻

一、中文文獻

- 王秋惠（2007）。網路詐欺被害特性與被害歷程之研究。中央警察大學犯罪防治研究所碩士論文。

- 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?。臺北大學犯罪學研究所碩士論文。
- 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。
- 呂敏綺 (2016)。高中職霸凌受害學生個人特質及相關因素之研究—以嘉義市高中職生為例。中正大學犯罪防治學系碩士論文。
- 呂詩涵、胡嘉文 (2015)。面對網路霸凌的因應之道。臺灣教育評論月刊，4 (9)，57-62。
- 周愫嫻 (2014)。青少年網路虛擬身份分與網路被害、不當行爲。犯罪與刑事司法研究，(22)，45-73。
- 徐文堂 (2015)。國中學生 LINE 使用行為與人際關係、網路霸凌之研究。中華大學科技管理研究所碩士論文。
- 許春金、陳玉書、莫季雍 (2000)。台灣地區犯罪被害經驗調查研究。法務部、內政部警政署委託研究。
- 許春金、陳玉書 (2005)。台灣地區犯罪被害調查。內政部警政署委託研究。
- 許春金、陳玉書 (2010)。99 年台灣地區犯罪被害調查。內政部警政署。
- 陳玉書、王秋惠 (2011)。網路詐欺被害特性分析。執法新知論衡，7 (2)，11-31。
- 陳玉書、簡鳳容、呂豐足、劉士誠 (2020)。網路犯罪被害：人口特性與情境機會的影響 。刑事政策與犯罪研究論文集，23，113-148。
- 曾淑萍、蘇桓玉 (2011)。國中學生網路霸凌被害恐懼感之研究。青少年犯罪防治研究期刊，3 (2)，1-34。
- 黃文圳 (2024)。詐欺犯罪被害者個人特性與被害風險之分析—以「假冒公務機關」、「猜猜我是誰」、「假交友」詐欺為例。國立臺北大學碩士論文。https://hdl.handle.net/11296/wca2fh。
- 黃俊祥 (2007)。少年網路偏差與犯罪行爲成因之研究。中央警察大學犯罪防治研究所碩士論文。
- 黃祥益 (2006)。台灣地區少年網路犯罪與被害特性之研究。中央警察大學犯罪防治研究所碩士論文。
- 黃凱柔 (2016)。新移民與非新移民子女校園霸凌被害經驗之比較研究。國立中正大學犯罪防治學系碩士論文。
- 葉雲宏(2008)。網路詐欺犯罪被害影響因素之研究。中央警察大學犯罪防治研究所碩士論文。
- 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。國立中正大學犯罪防治所碩士論文。
- 簡鳳容 (2018)。網路偏差與被害特性及其影響因素之研究。中央警察大學犯罪防治研究所博士論文。

二、英文部分

- 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. Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American sociological review,* 588-608.

- Al-Hasani, Y. S., Zain, J. M., Azrag, M. A. K., & Edris, K. H. M. (2022). Relationship Between Consumer's Social Networking Behavior and Cybercrime Victimization Among the University Students. In *International Conference on Information Systems and Intelligent Applications* (pp. 683-694). Cham: Springer International Publishing.
- Auwal, A. M., & Lazarus, S. (2024). Sociological and Criminological Research of Victimization Issues: Preliminary Stage and New Sphere of Cybercrime Categorization. *Journal of Digital Technologies and Law,* 2(4), 915-942.
- Brinton, J., Langton, L., Krebs, C., & Casper, M. (2023). *An Environmental Scan of Cybercrime Measurement: Recommendations for the National Crime Victimization Survey.* RTI International. Bureau of Justice Statistics. https://bjs.ojp.gov/library/publications/environmental-scan-cybercrime-measurement
- Buil-Gil, D., & Barrett, E. (2022). The dynamics of business, cybersecurity and cyber-victimization: Foregrounding the internal guardian in prevention. In *The New Technology of Financial Crime* (pp. 5-34). Routledge.
- Clarke, R. V. (1980). Situational crime prevention: Theory and practice. *Brit. J. Criminology, 20,* 136.
- Cloward, R. A. (1959). Illegitimate means, anomie, and deviant behavior. *American sociological review,* 164-176.
- Cullen, F. T. (1983). *Rethinking crime and deviance theory: The emergence of a structuring tradition.* Totowa, NJ: Rowman & Allanheld.
- Eurostat. (2021). *EU statistics on income and living conditions (EU-SILC): Module on Internet and cyber security*. Retrieved from https://ec.europa.eu/eurostat
- Felson, M. (1998). *Crime and everyday life.* Thousand Oaks, CA: Sage.
- Fisher, B. S., Cullen, F. T., & Turner, M. G. (2002). Being pursued: Stalking victimization in a national study of college women. Criminology & Public Policy, 1(2), 257-308. https://doi.org/10.1111/j.1745-9133.2002.tb00091.x
- Guerra, C., & Ingram, J. R. (2022). Assessing the relationship between lifestyle routine activities theory and online victimization using panel data. *Deviant Behavior, 43*(1), 44-60.
- Herrero, J., Torres, A., Vivas, P., Hidalgo, A., Rodríguez, F. J., & Urueña, A. (2021). Smartphone addiction and cybercrime victimization in the context of lifestyles routine activities and self-control theories: The user's dual vulnerability model of cybercrime victimization. *International journal of environmental research and public health, 18*(7), 3763.
- Hindelang, M. J., Gottfredson, M. R., & Garofalo, J.(1978). *Victims of personal crime: An empirical foundation for a theory of personal victimization.* Cambridge, MA: Ballinger.
- Ho, H. T. N., & Luong, H. T. (2022). Research trends in cybercrime victimization during 2010–2020: a bibliometric analysis. *SN Social Sciences, 2*(1), 4. https://doi.org/10.1007/s43545-021-00305-4
- Hollis, M. E., Felson, M., & Welsh, B. C. (2013). The capable guardian in routine activities theory: A theoretical and conceptual reappraisal. *Crime Prevention & Community Safety, 15*(1), 65-79.
- Holt, T. J., & Bossler, A. M. (2008). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. Deviant behavior, 30(1), 1-25.
- Holt, T. J., Bossler, A. M., Malinski, R., & May, D. C. (2016). Identifying predictors of unwanted

online sexual conversations among youth using a low self-control and routine activity framework. *Journal of Contemporary Criminal Justice, 32*(2), 108-128.

- Lee, C. S., & Wang, Y. (2024). Typology of cybercrime victimization in Europe: A multilevel latent class analysis. *Crime & Delinquency, 70*(4), 1196-1223.
- Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017). Cybercriminal networks, social ties and online forums: Social ties versus digital ties within phishing and malware networks. *The British Journal of Criminology, 57*(3), 704-722.
- Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior, 37*(3), 263-280.
- Lin, K., Wu, Y., Sun, I. Y., & Qu, J. (2023). Telecommunication and cyber fraud victimization among Chinese college students: An application of routine activity theory. *Criminology & Criminal Justice,* 17488958221146144.
- Marttila, E., Koivula, A., & Räsänen, P. (2021). Cybercrime victimization and problematic social media use: Findings from a nationally representative panel study. *American Journal of Criminal Justice, 46*(6), 862-881.
- Mikkola, M., Kaakinen, M., Savela, N., Oksa, R., Savolainen, I., & Oksanen, A. (2024). Cybercrime target exposure, suitability, personality, and victimization: A longitudinal approach. *Finnish Journal of Social Research.*
- Mwiraria, D., Ngetich, K., & Mwaeke, P. (2024). Exploring Individual Factors Associated with the Prevalence of Cybercrime Victimization among Students at Egerton University, Kenya. *European Journal of Humanities and Social Sciences, 4*(5), 35-40.
- Ndubueze, P. N., Igbo, E. U. M., & Okoye, U. O. (2013). Cyber crime victimization among internet active Nigerians: An analysis of socio-demographic correlates. International Journal of Criminal Justice Sciences, 18(2), 225-234.
- Ngo, F. T. & R. Paternoster. (2011). Cybercrime victimization: An examination of individual and situational level factors. *International Journal of Cyber Criminology* , 5(1),773–793.
- Notté, R., Leukfeldt, E. R., & Malsch, M. (2021). Double, triple or quadruple hits? Exploring the impact of cybercrime on victims in the Netherlands. *International Review of Victimology, 27*(3), 272-294.
- Nzeakor, O. F., & Nwoke, C. N. (2023). Internet Access and Cybercrime Victimization Experience in Abia State, Nigeria. *Fuoye Journal of Criminology and Security Studies,* 2(1).
- Osgood, D. W., Wilson, J. K., O'Malley, P. M., Bachman, J. G., & Johnston, L. D. (1996). Routine activities and individual deviant behavior. *American Sociological Review, 61*(4), 635–655. https://doi.org/10.2307/2096397
- Özaşçılar, M., Çalıcı, C., & Vakhitova, Z. (2024). Examining cybercrime victimisation among Turkish women using routine activity theory. *Crime Prevention and Community Safety, 26*(1), 112-128.
- Parti, K. (2023). What is a capable guardian to older fraud victims? Comparison of younger and older victims' characteristics of online fraud utilizing routine activity theory. *Frontiers in Psychology, 14,* 1118741.
- Reep-van den Bergh, C. M. M. & Junger, M. (2018). Victims of cybercrime in Europe: A review of victim surveys. Crime Science, 7(1).

- Reynald, D. M. (2009). Guardianship in action: Developing a new tool for measurement. *Crime Prevention & Community Safety,* 11, 1-20.
- Reynald, D. M. (2010). Guardians on guardianship: Factors affecting the willingness to monitor, the ability to detect potential offenders and the willingness to intervene. *Journal of Research in Crime & Delinquency, 47,* 358-390.
- Reynald, D. M. (2011a). Factors associated with the guardianship of places: Assessing the relative importance of the spatio-physical and sociodemographic contexts in generating opportunities for capable guardianship. *Journal of Research in Crime & Delinquency, 48,*110-142.
- Reynald, D. M. (2011b). *Guarding against crime: Measuring guardianship within routine activity theory.* Farnham, UK: Ashgate.
- Reyns, B. W. (2010). A situational crime prevention approach to cyberstalking victimization: Preventive tactics for internet users and online place managers. *Crime Prevention &Community Safety, 12*(2), 99-118.
- Reyns, B. W. (2013). Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. *Journal of Research in Crime and Delinquency, 50*(2), 216-238.
- Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being pursued online: Applying cyber lifestyle–routine activities theory to cyberstalking victimization. *Criminal* justice and behavior, 38(11), 1149-1169.
- Reyns, B. W., Henson, B., & Fisher, B. S. (2016). Guardians of the cyber galaxy: An empirical and theoretical analysis of the guardianship concept from routine activity theory as it applies to online forms of victimization. *Journal of Contemporary Criminal Justice, 32*(2), 148-168.
- Smith, M. J., & Clarke, R. V. (2012). Situational crime prevention: Classifying techniques using "good enough" theory. *The Oxford handbook of crime prevention,* 291-315.
- Vakhitova, Z. I., Reynald, D. M., & Townsley, M. (2016). Toward the adaptation of routine activity and lifestyle exposure theories to account for cyber abuse victimization. *Journal of Contemporary Criminal Justice, 32* (2), 169-188.
- Van Wilsem, J. (2011). 'Bought it, but never got it' assessing risk factors for online consumer fraud victimization. *European Sociological Review, 29* (2), 168-178.
- Van Wilsem, J. (2013). Hacking and harassment—Do they have something in common? Comparing risk factors for online victimization. *Journal of Contemporary Criminal Justice, 29* (4), 437-453.
- Wang, D., Duan, Y., & Jin, Y. (2025). Navigating online perils: Socioeconomic status, online activity lifestyles, and online fraud targeting and victimization of old adults in China. *Computers in Human Behavior, 162,* 108458. DOI: 10.1016/j.chb.2024.108458
- Williams, M. L. (2016). Guardians upon high: An application of routine activities theory to online identity theft in Europe at the country and individual level. *British Journal of Criminology, 56* (1), 21-48.
- Yar, M. (2005). The Novelty of 'Cybercrime' an assessment in light of routine activity theory. *European Journal of Criminology, 2* (4), 407-427.