



A systematic literature review of profiling victims of cyber scams: setting up a framework for future research

Monica Therese Whitty

To cite this article: Monica Therese Whitty (2025) A systematic literature review of profiling victims of cyber scams: setting up a framework for future research, Cogent Social Sciences, 11:1, 2563781, DOI: [10.1080/23311886.2025.2563781](https://doi.org/10.1080/23311886.2025.2563781)

To link to this article: <https://doi.org/10.1080/23311886.2025.2563781>



© 2025 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group



Published online: 20 Sep 2025.



Submit your article to this journal



Article views: 2113



View related articles



View Crossmark data



Citing articles: 1 View citing articles

A systematic literature review of profiling victims of cyber scams: setting up a framework for future research

Monica Therese Whitty 

Software Systems and Cybersecurity, Monash University, Melbourne, Australia

ABSTRACT

Background: Cyber scams continue to rise worldwide, posing a significant concern due to the harm inflicted on individuals, both financially and psychologically, as well as on societies. Given that apprehending criminals is resource-intensive and challenging (as investigations require global cooperation), profiling victims is arguably more crucial than profiling criminals, starkly contrasting with other types of crimes.

Methods: This SLR examines various theories that have informed empirical, quantitative research on cyber scam victims and their psychological characteristics. We followed the PRISMA 2020 guidelines for systematic reviews. Eligible studies included peer-reviewed empirical studies between 2000 and 2025 that examined psychological profiles of cyber scam victims.

Results: In the final sample ($n=22$), the most prevalent theories employed were Personality Theory and Routine Activities Theory. Personality characteristics included addictive personality, impulsivity, internal locus of control, optimism, and low on openness.

Discussion: A model of predictors to guide future research was proposed, including personality, individual characteristics, behaviours, cognition, self-esteem and attitudes/beliefs.

Conclusions: Research may need to focus more attention on individual cyber scam types. Neglected theories that could have been considered include Information Processing Theory, Theory of Planned Behaviour, Protection Motivation Theory, and Social Identity Theory. This SLR offers a pathway to enhance future research.

ARTICLE HISTORY

Received 19 June 2025

Revised 20 August 2025

Accepted 15 September 2025

KEYWORDS

Cyber scam; cyber fraud, cyber crime; profiling victims; cybersecurity; personality; routine activities theory

SUBJECTS

General Psychology; Information Technology; Sociology & Social Policy; Criminology and Criminal Justice

Introduction

The past 15 years have witnessed an international surge of cyber scams (Lacey et al., 2024). In 2024 alone, it was reported that over \$1 trillion USD were lost to scam victims worldwide (Rogers, 2024). Although it is believed that scams are underreported (Houtti et al., 2024; Kolupuri et al., 2025), national reporting supports these high numbers. In 2024 in Australia, losses of over \$300 million AUD to 249,448 scam victims (National Anti-Scam Centre, 2024). In the UK in 2024, losses of over £11 billion GBP were reported by scam victims (CIFAS, 2024). Harms involve a double-hit of financial (including, in many cases, the loss of assets, such as houses) and psychological impact, such as stress, anxiety, shame, and depression (Whitty & Buchanan, 2012, 2016). These harms can be long-term, impacting victims and their families with life-changing financial harms, repeated victimisation and severe psychological trauma (Balcombe, 2025; Button et al., 2025; Whitty & Buchanan, 2016; Woods & Walter, 2022). There is also harm to the countries' economies from the money siphoned out to support organised criminals, often facilitating other crimes (e.g., terrorism and drug trafficking) (Grieco, 2023; Ryder, 2024; Whitty, 2018a).

Given the rising prevalence of cyber scams and the serious harm caused by them, researchers must urgently focus on this issue so that their findings can inform more effective policies and intervention strategies. Interventions are typically technical and human, aiming to detect and prevent cyber threats. Several reviews on cyber scam victimisation have been conducted; however, they primarily concentrated on anti-fraud policies and victim targeting, or specific cyber scams (Bilz et al., 2023; Desolda et al., 2022;;

CONTACT Monica Therese Whitty  monica.whitty@monash.edu  Software Systems and Cybersecurity, Monash University, Melbourne, Australia.

© 2025 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group
This is an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. The terms on which this article has been published allow the posting of the Accepted Manuscript in a repository by the author(s) or with their consent.

Lazarus et al., 2023; Norris et al., 2019). A useful mini-review conducted by Lacey et al. (2024) highlights several psychological factors influencing scam compliance; however, it lacks a thorough examination and consideration of theoretical approaches.

Although Lacey et al.'s mini review is helpful, a deeper dive into the predictors of cyber scam victimisation is necessary, including the range of characteristics and the theories that have informed cyber victimisation profiling. This is critical if we are to advance the science of profiling cyber scam victims. This paper, therefore, provides a comprehensive overview of state-of-the-art research and outlines a framework for future studies.

Background literature

Cyber scams in an online environment

This research focuses exclusively on cyber scams, rather than those occurring in the physical realm. A cyber scam is a deceptive scheme carried out through digital technologies, such as the Internet, email, social media, messaging apps, or other online platforms, with the intention of tricking individuals into giving away money. Cyber scams exploit psychological manipulation (e.g. urgency, trust, fear or greed) and technological affordances to deceive victims. Examples include phishing (fraudulent emails or messages designed to steal identity information), romance scams (criminals create fake profiles and develop a deep relationship with the victim and trick them out of money) and investment scams (promising high returns in fraudulent schemes such as cryptocurrency or fake trading platforms).

This focus stems from the discipline of cyberpsychology, which studies the psychological processes related to human interaction with digital technology and cyberspace (Joinson, 2002). Unlike traditional psychology, which primarily examines behaviour and cognition in offline contexts, cyberpsychology is uniquely positioned to interrogate how digital environments transform identity, perception, and social interaction (Attrill, 2015). It examines the ways in which technology influences and interacts with behaviour, cognition, emotion, and interpersonal relationships, thereby offering theoretical and empirical insights into how individuals construct and negotiate their sense of self online. These perspectives are particularly valuable in understanding the mechanisms of cybercrime and deception, as offenders often exploit features of online environments such as anonymity, reduced cues, and asynchronous communication (Joinson, 2002).

Research within cyberpsychology has demonstrated that the digital context amplifies certain vulnerabilities and introduces new forms of risk. For instance, individuals may disclose more personal information online than in face-to-face interactions, increasing their susceptibility to social engineering, romance fraud, or phishing attacks (Aiken et al., 2016;; Walther & Whitty, 2021). Findings from this field have also revealed psychological traits—such as impulsivity, loneliness, or trust propensity—that correlate with victim susceptibility, advancing victimology beyond criminological or sociological frameworks alone (Whitty & Young, 2017). In this sense, cyberpsychology provides a more granular understanding of why individuals respond to deceptive online cues, complementing and extending the explanatory scope of routine activity theory and rational choice models drawn from criminology (Leukfeldt, 2014).

Comparatively, scholarship from other domains—such as law, criminology, and computer science—has made important contributions in conceptualising cybercrime, mapping offender typologies, or designing technical security measures. However, these perspectives often lack attention to the subjective experiences of victims and the psychological processes underpinning their decision-making. Cyberpsychology fills this gap by centring the individual's cognitive and emotional landscape, thereby situating cybercrime within broader frameworks of human vulnerability, trust, and social influence (Aiken et al., 2016).

Notably, researchers have shown that individuals may be more vulnerable to online crimes than to those committed in the physical realm, as the affordances of cyberspace—such as anonymity, reach, and scalability—alter the risk landscape (Aiken et al., 2016). These insights not only advance theoretical understandings of crime but also inform prevention and intervention strategies, underscoring the importance of tailoring responses to the digital context (Caneppele & Aebi, 2019; Stalans & Finn, 2016). Given these potential differences and the prevalence of cyber scams, the present work centres on profiling victims.

Furthermore, it is important to clarify what is meant by fraud and scams in the 'physical realm', relative to those occurring in online environments. Traditionally, physical realm fraud encompasses crimes such as face-to-face investment fraud, doorstep scams, advance-fee fraud conducted at credit card skimming at

physical points of sale (Button et al., 2025). These offences typically involve direct interpersonal contact. In contrast, online fraud refers to deception mediated primarily through digital platforms. It is important to distinguish cyber scams from face-to-face scams, not only because the ubiquity of the Internet exposes individuals to a far greater volume of deceptive attempts, but also because the unique psychology of cyberspace shapes how these scams operate. As discussed above, online environments afford features such as anonymity, reduced social cues, and asynchronous communication, which can alter both offender strategies and victim responses. Consequently, the psychological profiles of victims of cyber scams may differ in significant ways from those of individuals targeted in traditional, face-to-face scams.

Trends and theories in researching cyber-scam victims' characteristics

Early work profiled victims demographically (Lee & Soberon-Ferrer, 1997). Researchers then turned to Routine Activity/Lifestyle-Exposure models to examine how online routines (e.g. remote purchasing, forum participation) might increase exposure to offenders, while insufficient 'guardianship' (weak platform safeguards, low social support) might heighten risk (Titus et al., 1995). Experimental studies, in the lab with non-victims, have suggested that self-control (impulsivity, risk-seeking) might explain cyber scam compliance (Mesch & Dodel, 2018). Laboratory studies are widely used to examine victim profiles in cyber scams—particularly phishing—but their ecological validity is limited; behaviour observed in role-play or simulated tasks often fails to generalise to operational environments, and field studies repeatedly show patterns (and variability) that differ from typical laboratory samples (Sommestad & Karlzén, 2024). This current study, therefore, focused on 'real' victims of cyber scams.

The importance of profiling victims of cybercrimes

The exponential growth of digital technologies has reshaped human interaction and simultaneously transformed the nature of crime and victimisation (Blythe & Johnson, 2021; Lee & Choi, 2022). As cybercrimes such as online fraud, cyberstalking, and phishing proliferate, academic and law enforcement agencies also focus on profiling offenders (Greco & Greco, 2020; Lickiewicz, 2011; Martineau et al., 2023). Cybercriminal profiling, which involves understanding perpetrators' motivations, methods, and characteristics, is considered essential for prevention and attribution (Warikoo, 2014). However, catching cybercriminals is challenging, as they are difficult to identify (Minnaar, 2014; Rao et al., 2024; Taleby Ahvanooey et al., 2022). When they are known, they are often in another country from where the crime was committed, making it expensive and challenging to extradite the accused (DeTardo-Bora & Bora, 2016; Guitton, 2012; Mugarua & Ssali, 2021). ; Arguably, therefore, other approaches to reducing cybercrimes are needed.

Technological solutions are an essential defence against cyber threats. This includes the implementation of firewalls, encryption, intrusion detection systems, endpoint protection, and multi-factor authentication (Leuprecht et al., 2016; Zhou et al., 2023). Organisations and individuals can reduce attack surfaces through regular software updates, patch management, and secure device configuration (Dissanayake et al., 2022; Furnell et al., 2014). However, these tools cannot eliminate cybercrime, as criminals can bypass these systems.

Cyber hygiene, the routine practices individuals must engage in to reduce cyber threats, is also critical. Behaviours such as strong passwords, multifactor authentication, and avoiding suspicious links reduce susceptibility to cyberattacks (Bayl-Smith et al., 2022; Cain et al., 2018; Creese et al., 2013; Pasquini et al., 2021). However, not all users adopt these cyber hygiene practices, and even when they do, they are often confronted with cyber scams (Mouncey & Ciobotaru, 2025). Therefore, understanding a victim's profile is essential to developing effective education and behavioural change programs and policies to prevent cybercrime victimisation (DeLiema et al., 2025;; Whitty, 2015).

Victimology and the digital context

Victimology has traditionally focused on understanding the consequences of victimisation, the victim-offender relationship, and systemic responses to victims of crime (Burgess et al., 2010; Heap, 2021). Unlike physical crimes, cyber victimisation can occur anonymously and repeatedly, often leaving victims without closure or justice. The psychological impacts may be amplified in online spaces due to the persistence of digital content and ambiguity around blame and justice (Kirwan & Power, 2013; Notté et al., 2021).

Psychological victimology focuses on understanding risk factors, including behaviours and psychological predispositions (e.g. traits, emotional states) that make individuals more susceptible to cyber victimisation. The psychological literature highlights that victim susceptibility is not solely a matter of naivety but often a function of emotional needs, cognitive biases and social isolation (Fonseca et al., 2022; Kirwan & Power, 2013). Understanding these psychological vulnerabilities is essential for designing effective interventions (such as inoculations), education campaigns and warning systems.

There is limited empirical research examining predictors of cyber scam victimisation. The most relevant work to date is Lacey et al. (2024) mini-review, which explores certain psychological factors influencing compliance but offers neither a comprehensive analysis of predictors nor a strong theoretical grounding. Unlike many other crimes, cybercrime prevention hinges on understanding vulnerabilities, as identifying, apprehending, and prosecuting offenders is both resource-intensive and challenging. Developing a robust, literature-informed framework to guide prevention strategies is therefore not only necessary but also timely.

Objectives

The overall objective of this research was to gain a comprehensive overview of the study on profiling victims of cyber scams. The intention is to gather an understanding of what has been carried out to date and where the gaps are that future researchers may consider. It does so by carrying out a systematic literature review (SLR). Drawing from these findings, a framework will be developed that identifies gaps for future research in this area. The research questions include:

RQ1: Which theories have informed the research on the profiling of cyber scam victims?

RQ2: What are the psychological characteristics of victims of cyber scams?

Methods

The present study aimed to collate and review all the empirical studies concerning the psychological profiling of cyber scam victims published between 2000 and 2025. The decision for the year 2000 was a cut because of the evolving nature of the Internet (e.g. it was around this time that the Internet evolved into an interactive Internet) and the changes in users over time (e.g. early adopters tended to be technically minded people) (Petrovic, 2025; Young & Whitty, 2012). Anything older than 2000, therefore, carries the risk of bias. It is also noted that the review was completed in about July 2025, so some papers may have been missed from later in the year. Nonetheless, it was a preference to include the most up-to-date research. The research followed the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines (Page et al., 2021). This method is popular in medicine, psychology, and the social sciences. It provides openness and clarity that can address research questions that could not be answered by an individual study. It also offers researchers the chance to create innovative frameworks for future studies.

Eligibility criteria

The study's eligibility criteria were defined based on the PECO framework, including Population, Exposure, Comparison, and Outcome (Morgan et al., 2018). The eligibility criteria were as follows:

- Population: The study must focus on adult victims of cyber scams, 18 years and older.
- Exposure: Participants must be tested on psychological measures (e.g. personality, beliefs, behaviours).
- Comparator: Cyber scam victims must be compared with non-victims or other types of victims.
- Outcome: The outcome must provide empirical data on the likelihood of being cyber scammed.

The exclusion criteria comprised studies not reported in academic peer-reviewed journals or full conference papers. The papers needed to be written in English. Only quantitative studies were included. Finally, any review paper summarising or synthesising existing literature was excluded.

Information sources

The systematic search included a comprehensive range of databases to ensure extensive coverage of the relevant literature. Search databases included Scopus, Web of Science, EBSCOhost, OVID, PsychINFO, and IEEE.

Search terms

The search string created for this study combined key terms representing the core aspects of the research questions. In relation to cyber scams, the search string included variations of terms including 'cyberscam*', 'cyber scam*', 'cyberfraud*', 'cyber fraud*', 'mass marketing fraud*', 'mass-marketing fraud*', 'Internet fraud*', 'Internet scam*', 'online fraud*' or 'online scam*'. These terms were combined using Boolean operators (AND, OR), with adjustments for each database's specific syntax requirements. They were combined with using AND with the following terms to capture psychological profiling of cyber scam victims, including 'personality', 'victim*', 'victim profile', 'profile', 'psychology', 'demographic*', 'belief*', and 'vulnerab*'.

Document selection

The management of references was conducted in EndNote (version 21). [Figure 1](#) applies the template developed by Page et al. (2021). The records identified through each database are set out, with the majority being identified via EBSCO and Scopus. After removing duplicate records ($n=743$), the initial set included 1611 records.

The records were then manually screened by title and abstract, where articles were excluded according to the criteria. At this stage, articles were excluded due to not being a journal article or a full conference paper ($n=564$), not being in English ($n=13$), or being out of scope ($n=1035$). Full papers were then assessed for eligibility ($n=107$). At this stage, articles were excluded because they were experimental, not including real victims ($n=21$), they were qualitative ($n=7$), or they were out of scope ($n=57$). A total of 22 studies were therefore included in the systematic review.

Dual review

To mitigate potential selection bias, the AI-assisted screening function in Rayyan ([n.d](#)) was employed to facilitate dual coding of the 1,611 articles retrieved from the initial search following de-duplication. Rayyan applies machine learning algorithms that iteratively learn from reviewers' inclusion and exclusion decisions to predict the relevance of unscreened records. Empirical evaluations have reported sensitivity values ranging from 87.6% to 99.5% and specificity values ranging from 88.7% to 99.6% (Sucaldito & Yu, [n.d](#); Trad et al., 2024; Valizadeh et al., 2022). While Rayyan is not infallible, its application can help reduce the risk of bias in the screening process. In this study, the reviewer identified 22 articles (see [Figure 1](#)), and Rayyan AI included the same 22 plus an additional 5, giving a Cohen's kappa=0.87, indicating very strong agreement (Landis & Koch, 1977). The additional five papers were reviewed in full, but did not meet the inclusion criteria and were therefore excluded from the final analysis.

Quality assessment

Quality assessment was conducted using an adapted Critical Appraisal Skills Programme Checklist (CASP, 2018). This considered the appropriateness of the study design, choice of outcome measure, statistical issues, reliability of measures used, recruitment processes and precision of the results. Risk of bias was separated into eight types of bias: aims, research questions, methodology, research design, recruitment, data collection, data analysis, and reporting bias, ([Table 1](#)) described below:

1. Aims: Was there a clear statement of the aims of the research?
2. Research Questions: Was there a clear statement of the research questions (RQs)?
3. Methodology: Was the appropriate methodology chosen?

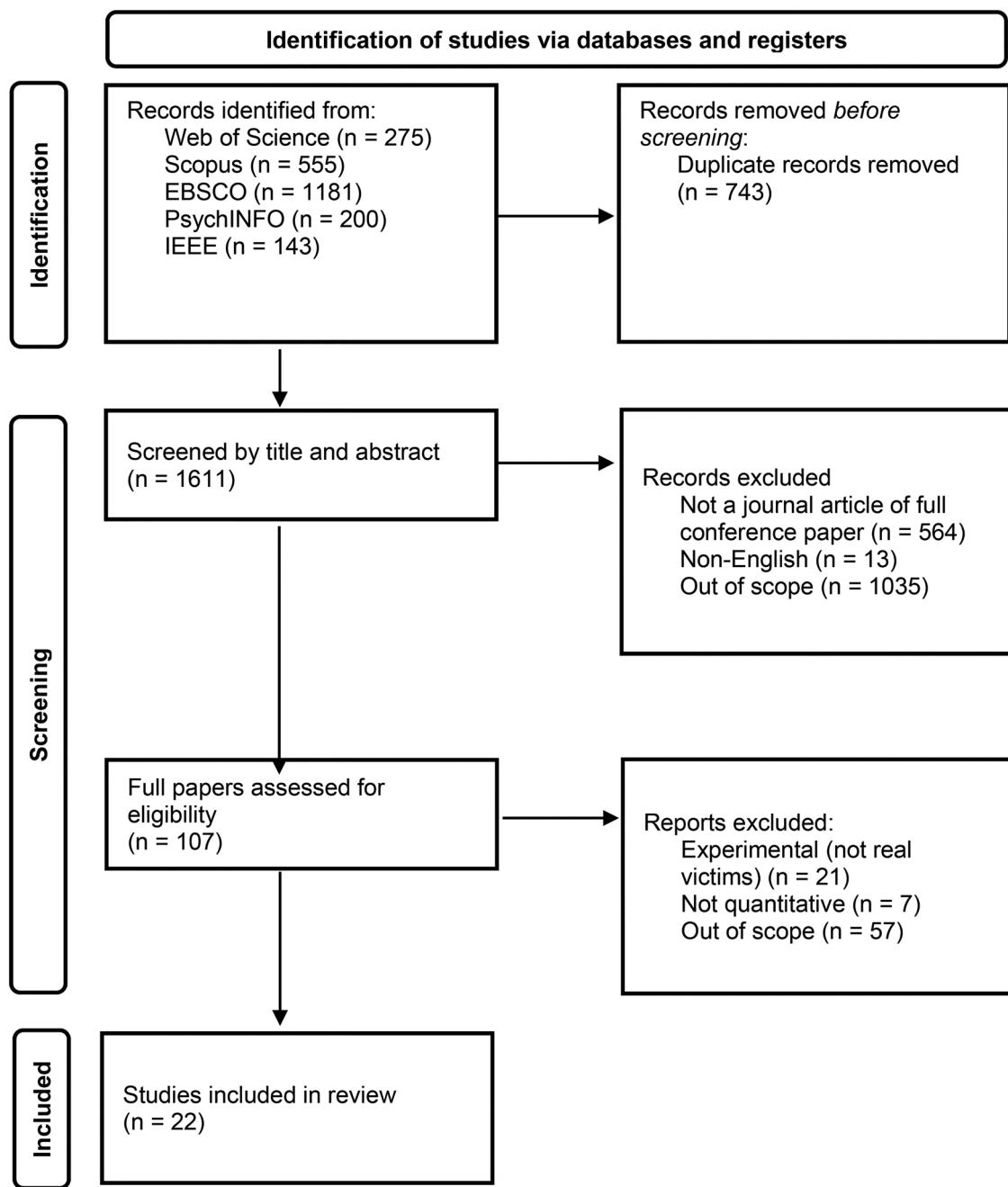


Figure 1. PRISMA flow diagram.

4. Research design: Was the research design appropriate to address the aims?
5. Recruitment: Was the recruitment strategy appropriate?
6. Data collection: Were the data collected in a way that addressed the research issue?
7. Data Analysis: Was the data analysis sufficiently rigorous?
8. Reporting bias: Was there a clear statement of findings?

A low risk was considered if 1–2 of the categories were violated, medium if 3–4, and high if 5–8. If a study obtained a high-risk rating for any of the categories, it was excluded from the review. Although a stringent criterion, it ensured the included studies were of high quality. Quality assessment was completed by two blinded peer reviewers. There were no discrepancies between reviewers. Given that the risk of bias was low for all cases, no studies were excluded (see Table 1).

Results

Description of selected studies

The 22 articles that met all the previously determined inclusion criteria were analysed (see [Table 2](#)). The table only includes the findings that addressed the research questions. The types of cyber scams focused on were either general ($n=11$), consumer ($n=2$), romance scams ($n=3$), multiple scams ($n=2$), investment ($n=1$), identity ($n=1$), phishing ($n=1$), and SNS ($n=1$). The methodologies included surveys ($n=18$), questionnaires ($n=2$), and longitudinal studies ($n=2$). The samples were drawn from the following countries: USA/Canada ($n=6$), UK ($n=4$), the Netherlands ($n=4$), Malaysia ($n=3$), China ($n=2$), Japan ($n=1$), Portugal ($n=1$), and Spain ($n=1$).

The operationalisation of the dependent variable, fraud victimisation, differed across studies (see [Table 3](#)). Most measured it using a single item, yet the exact wording was often omitted, and where reported, it varied considerably. The choice of independent variables also lacked uniformity (see [Table 2](#)). Standardised scales were employed for a range of psychological and personality constructs, including the Big Five traits, loneliness, sensation seeking, impulsivity, self-control, romantic beliefs, cognitive complexity, self-esteem, optimism, addiction, greed, gullibility, kindness, locus of control, trustworthiness, and cognitive flexibility and maturity. Other constructs were measured using items developed specifically for individual studies.

As shown in [Table 2](#), various statistical methods were employed to examine the studies' hypotheses. Furthermore, the studies did not always report all the statistics. These two aspects rendered the studies difficult to compare or to determine which variables might be more effective at predicting victimhood. The results section sets out the main predictors examined in these studies, which are represented in [Figure 4](#).

Comparisons across studies

Given the early stage of research in this area, there is currently substantial heterogeneity in the types of dependent and independent variables examined across studies (see [Tables 2 & 3](#)). These variables differ not only in their conceptual definitions but also in their operationalisation and measurement approaches. Such variability limits the comparability of findings and undermines the statistical assumptions required for meta-analysis, such as the need for a consistent set of effect size metrics and comparable constructs across studies (Borenstein et al., [2021](#)). As a result, synthesising the available evidence through quantitative meta-analytic techniques was not feasible.

Table 1. Analysis of risk bias.

	1	2	3	4	5	6	7	8	Concerns
Balakrishnan et al. (2025)	✓	✓	✓	✓	✓	✓	✓	✓	
Buchanan and Whitty (2014)	✓	✓	✓	✓	✓	✓	✓	✓	
Chen et al. (2017)	✓	x	✓	✓	✓	✓	✓	✓	Doesn't explicitly state RQs but does have hypotheses
DeLiema et al. (2023)	✓	✓	✓	✓	✓	✓	✓	✓	
DeLiema et al. (2020)	✓	x	✓	✓	✓	✓	✓	✓	Doesn't explicitly state RQs but does have hypotheses
Fonseca et al. (2022)	✓	✓	✓	✓	✓	✓	✓	✓	
Gainey et al. (2023)	✓	✓	✓	✓	✓	✓	✓	✓	
Goede et al. (2024)	✓	x	✓	✓	✓	✓	✓	✓	Doesn't explicitly state RQs but does set out models to test
Herrero et al. (2022)	✓	x	✓	✓	✓	✓	✓	✓	Doesn't explicitly state RQs but does have hypotheses
Junger et al. (2023)	✓	✓	✓	✓	✓	✓	✓	✓	
Kirwan et al. (2018)	✓	✓	✓	✓	✓	✓	✓	✓	
Koning et al. (2024)	✓	✓	✓	✓	✓	✓	✓	✓	
Leukfeldt (2014)	✓	✓	✓	✓	✓	✓	✓	✓	
Parti (2023)	✓	x	✓	✓	✓	✓	✓	✓	Doesn't explicitly state RQs but does have hypotheses;
Reyns & Randa (202)	✓	✓	✓	✓	✓	✓	✓	✓	
Saad and Abdullah (2018)	x	x	✓	✓	✓	✓	✓	✓	Doesn't state the aims or RQs – but summarises theory and implies the objectives
Suzuki (2024)	✓	x	✓	✓	✓	✓	✓	✓	Doesn't state the RQs- but objectives imply what is being asked
Whitty (2018b)	✓	✓	✓	✓	✓	✓	✓	✓	
Whitty (2019)	✓	✓	✓	✓	✓	✓	✓	✓	
Whitty (2020)	✓	✓	✓	✓	✓	✓	✓	✓	
Xin et al. (2024)	✓	x	✓	✓	✓	✓	✓	✓	Doesn't explicitly state RQs but does have hypotheses
Xu et al. (2024)	✓	x	✓	✓	✓	✓	✓	✓	Doesn't state the RQs- but objectives imply what is being asked.

Table 2. Overview of the articles included in the review.

Authors	Scam type	Design	Sample description	Theory	Independent variables	Key findings
Balakrishnan et al., 2025	General	Survey	Sample 1: Malaysia N = 820 Sample 2: Malaysia N = 629	Social Cognitive Theory	Attitude Safe practice Self-awareness	Sample 1: Overconfidence OR = 1.437; $p < .001$. Sample 2: Overconfidence OR = 1.453; $p = .005$.
Buchanan & Whitty, 2014	Romance scams	Questionnaire	Sample 1: UK N = 1250 Sample 2: UK N = 397	Personality Belief Systems	Big 5 Loneliness Romantic Beliefs Sensation Seeking	Sample 1: Romantic Beliefs, (Idealization) OR = 1.11; $p < .005$. Sample 2: Romantic Beliefs, (Idealisation); OR = 1.27; $p < .005$.
Chen et al., 2017	General	Survey	USA N = 11,534	Routine Activity Theory	Behaviours; downloading files information consumption, online information disclosure, opening emails from unknown sources, shopping, and willingness to make risky investments. Knowledge about Internet privacy	Information consumption $\beta = -0.04$; $p > .001$. Online information disclosure $\beta = 0.06$; $p > .001$. Opening emails from unknown sources $\beta = 0.08$; $p > .001$. Shopping $\beta = 0.04$; $p > 0.001$. Willingness to make risky investments; $\beta = 0.05$; $p > .001$.
Deliema et al., 2023	General	Survey	USA and Canada N = 1,347	Self-control theory	Awareness of scams Knowledge: Financial Loneliness Behaviours: Exposure to offenders Investment mindset	Awareness OR = 0.22; $p < .001$ Financial literacy (low) OR = 0.84; $p < .01$ Loneliness (high) OR = 1.17; $p < .01$ Favourable attitudes towards unregulated investments OR= 1.27; $p = .043$.
Deliema et al., 2020	Investment	Survey	USA N = 1,027	Routine Activity Theory		Materialism OR = 2.25; $p = 0.47$ Recommendations OR = 0.70; $p = .032$. Remote invest OR = 1.64; $p = .001$ Trading frequency OR = 1.56; $p < .001$
Fonseca et al., 2022)	Consumer	Survey	Portugal N = 1,710	General theory of crime Routine Activity Theory	Self-control Behaviours: capable guardianship, Exposure to motivated offenders, and risky behaviours.	Avoid putting personal info online OR = .845; $p < .01$ Interaction with strangers OR = 1.229; $p < .01$. Online purchasing OR = 1.415; $p < .001$. Visiting questionable websites, OR = 1.171; $p < .01$. Careful navigation $\beta = 0.922$; $p < .05$.
Gainey et al., 2023	General	Survey	USA N = 1,206	Routine Activity Theory	Exposure to motivated offender Protective factors	Equipment (more digital devices), $\beta = 1.122$; $p < .05$. Password caution $\beta = 0.872$; $p < .001$. Shopping OR = 1.633; $p < .01$. stream television (less likely) OR = 0.752, $p < .05$.
Goede et al., 2024	General	Longitudinal	Netherlands N = 1,886	Routine Activity Theory	Behaviours: Frequency of use, browsing, Personal use – banking, chatting, email, searching for information, shopping, social media, streaming.	Smart phone addiction * low social support, factor SR mean = 1.54, SE = 0.25, $p < .001$.
Herrero et al., 2022	General	Longitudinal	Spain N = 716	The theory of lifestyle and routine activities theory (L-RAT)	Social support Smart phone addiction	Fraud knowledge prevented 69%
Junger et al., 2023)	General	Survey	Netherlands N = 2,864	Absent	Participants' opinions on their vulnerability	Cognitive complexity, OR = .207; $p < .05$.
Kirwan et al., 2018	SNS scams	Questionnaire	Malaysia N = 320	Personality Routine Activity Theory	Big 5 Cognitive complexity Impulsivity SNS use	Number of devices, OR = .441; $p < .001$. SNS use, OR = .258; $p < .01$.

(Continued)

Table 2. Continued.

Authors	Scam type	Design	Sample description	Theory	Independent variables	Key findings
Koning et al., 2024	Multiple scams	Survey	Netherlands N = 2,864	Personality Routine Activity Theory	Behaviours: Dating, Internet use, Shopping, and Social media. Big5 Fraud knowledge Mental health Optimism Self-control Self-esteem Behaviours: Communication – email, chatting & MSN/Skype, Downloading, Internet use, Gaming, Shopping, SNSs, Targeted browsing	Optimism, OR = 0.866; $p < .05$. Self-control (investment) OR = 0.798, $p < .001$; (purchase) OR = 0.936; (debt) OR = 0.89; $p < .01$ (charity) OR = 0.886; $p < .001$; (dating) OR = 0.849, $p < .001$; (friend) OR = 0.847, $p < .001$, (phishing) OR = 0.86; $p < .001$; (spoofing) OR = 0.864 $p < .001$. Self-esteem OR = 0.944; $p < .001$. Social desirability OR = 0.849; $p < .001$. Targeted browsing, $\beta = 0.519$; $p < .05$.
Leukfeldt, 2014	Phishing	Survey	Netherlands N = 9,163	Routine Activity Theory	Computer familiarity Kruskal-Wallis H = 84.666; $p < .001$. Technical guardian Kruskal-Wallis H = 200.834; $p < .001$.	Computer familiarity (direct) $\beta = 0.103$; $p < 0.001$. Personal deviance (indirect via hacking) (19.5% total effects of personal deviance on identity fraud) Self control (direct effect) $\beta = 0.230$; $p = 0.033$. Self control (total effect) $\beta = 0.324$; $p = 0.003$. Self control (indirect effect) $\beta = 0.094$; $p < 0.001$. Cybercrime awareness correlated with romance scam victim ($r = 0.626$, $p < .01$) Computer skills correlated with romance scam victim ($r = 0.306$, $p < .01$) Contacting individuals met online $\beta = 1.533$ (p value not given)
Parti, 2023	General	Survey	USA N = 2,589	Routine Activity Theory		Peer deviance (direct) $\beta = 0.103$; $p < 0.001$. Personal deviance on identity fraud (19.5% total effects of personal deviance on identity fraud) Self control (direct effect) $\beta = 0.230$; $p = 0.033$. Self control (total effect) $\beta = 0.324$; $p = 0.003$. Self control (indirect effect) $\beta = 0.094$; $p < 0.001$. Cybercrime awareness correlated with romance scam victim ($r = 0.626$, $p < .01$) Computer skills correlated with romance scam victim ($r = 0.306$, $p < .01$) Contacting individuals met online $\beta = 1.533$ (p value not given)
Reyns & Randa, 2020	Identity fraud	Survey	USA N = 972	Routine Activity Theory		
Saad & Abdullah, 2018	Romance scam	Survey	Malaysia N = 280	Routine Activity Theory	Cybercrime awareness Computer skills	
Suzuki, 2024	Consumer fraud	Survey	Japan N = 1,782	Routine Activity Theory	Behaviours: using X, Facebook, Instagram, LINE and TikTok, and frequency of contacting people only meet online	
Whitty, 2018b	Romance Scam	Survey	UK N = 10,933	Personality	Addictive disposition Greed Gullibility Impulsivity Kindness Locus of control Trustworthiness	Addiction $\beta = 0.170$; $p < .001$. Kindness $\beta = -0.043$; $p < .01$. Sensation seeking $\beta = 0.089$; $p < .001$. Trustworthiness $\beta = -0.512$; $p < .05$. Urgency $\beta = 0.071$; $p < .001$.
Whitty, 2019	General	Survey	UK N = 11,780	Personality Routine Activity Theory	Addictive disposition, Behaviours: banking, Instant messaging, posting messages, posting pictures, shopping, and streaming media. Guardianship: viewed consumer advice sites Impulsivity Locus of Control	Addiction $\beta = 0.064$; $p < .001$. Guardianship $\beta = 0.207$; $p < .001$. Exposure online $\beta = 0.269$; $p < .001$. Lack of premeditation $\beta = -0.30$; $p < .001$. Locus of control, $\beta = -0.029$; $p < .001$. Sensation seeking $\beta = 0.031$; $p < .001$. Risky places, $\beta = 0.133$; $p < 0.05$. Urgency $\beta = 0.045$; $p < .001$. Repeat victims – online guardianship (greater); $\beta = 0.208$, $p < .001$; Investment scam victims higher on locus of control $F = 7.73$, $p < .001$ $\eta^2 = 0.04$.
Whitty, 2020	Multiple scams	Survey	UK N = 11,780	Personality	Addictive disposition Impulsivity Locus of Control	(Continued)

Table 2. Continued.

Authors	Scam type	Design	Sample description	Theory	Independent variables	Key findings
Xin et al., 2024	General	Survey	China N = 10,829	Routine Activity Theory	Previous fraud victimization	Previous victimization, 1,956%, 4,662%, 12,344%, 21,457%, $p < .001$
Xu et al., 2024	General	Survey	China N = 1000	Personality Critical Thinking	Analytical thinking Big 5 Cognitive flexibility Cognitive maturity Critical Thinking Inquisitiveness Materialism Open mindedness Perceived Benefits on risk Self-confidence Self-control Susceptibility to Persuasion Truth seeking	Inquisitiveness $t = -2.96; p < .01$. Open-mindedness $t = -3.31; p < .01$. Perceived benefits of risk $t = 2.69; p < .01$. Truth seeking $t = -4.60; p < .01$.

Note : the abbreviations in the table represent the following: OR (odds ratio), β (Beta value), SR (Standardised residual), SE (Standard Error), r (Pearson correlation coefficient), F (F-ratio), η^2 (eta squared), and t (t-test).

Table 3. Measurement of fraud victimisation across studies.

Authors	Dependent measured
Balakrishnan et al., 2025	Single item: Have you been a victim of any online fraud activity?
Buchanan & Whitty, 2014	1. Single item with options:No 2. Yes, but I never lost any money 3. Other people have said I was being scammed but I disagree
Chen et al., 2017	Single item: does not state the question
DeLiema et al., 2023	Single item: did you lose money to a scam
Deliema et al., 2020	Single item: does not state the question
Fonseca et al., 2022	People who had reported to the police
Gainey et al., 2023	1. Two items asking:Whether not anyone in the respondents' household had ever had any their listed fraud victimisation experiences 2. and if yes, had it occurred in the past year.
Goede et al., 2024	1. Two items:asking if they had become a victim of any cybercrime 2. and if yes, was it phishing, hacking, malware or online fraud
Herrero et al., 2022	Single item: Have you suffered any financial loss in the last 6 months due to possible cyberfraud.
Junger et al., 2023	Single item: does not state the question
Kirwan et al., 2018	Single item: doesn't state the question
Koning et al., 2024	Asked for each fraud category how often they fell victim to it in the year 2020.
Leukfeldt, 2014	Single item: does not state the question, but states that they were asked about phishing attacks that resulted in financial damage.
Parti, 2023	Multiple items: does not state the question, but states that they created multiple closed-ended questions describing specific fraud-scam events to measure financial fraud affectedness.
Reyns & Randa, 2020	Single item: Has anyone ever pretended to be you online, without your permission?
Saad & Abdullah, 2018	Multiple items: does not state, but does say they asked about the tendency to become a victim of cyber-love crime.
Suzuki, 2024	Single item: Did you experience cyber fraud, malicious business practices, and/or consumer damage last year?
Whitty, 2018b	Single item: does not state the question, but does say they were asked whether they had been scammed by the romance scam.
Whitty, 2019	Single item: Does not state the question, but does say they were asked whether they had been scammed by a cyberscam and if yes if this had been for more than one cyberscam.
Whitty, 2020	Single item: Does not state the question, but does say they were asked whether they had been scammed by a cyberscam and if yes they were given a list of scams, including consumer, charity, investment and romance scams or other (with a text box to describe).
Xin et al., 2024	Single item: Has someone tried to defraud you in the last year?
Xu et al., 2024	Single item: does not state the question, but does say they asked whether they had incurred any financial losses due to fraudulent activities.

Although it is challenging to compare data and not possible to conduct a meta-analysis, statistical findings from the included studies were extracted and are summarised in [Table 2](#). As shown in [Table 2](#), there is an inconsistency in the statistical tests employed and the reporting of statistical data across studies, reflecting the aforementioned methodological heterogeneity. Furthermore, not all studies reported effect sizes, and where such information was available, it is presented in the table. It is also important to note that the scope of these studies was not always exclusively focused on profiling cyber-crime victims; in several cases, victim-related analyses formed only part of a broader research agenda. Accordingly, only those statistical results that were directly relevant to the present review's research questions are reported, ensuring that the synthesis remains focused.

Theories

In addressing RQ1, which inquired about the theories that informed the research on profiling, Routine Activities Theory ($n=16$) and Personality ($n=7$) emerged as the most prevalent theoretical approaches (see [Table 4](#)). Additionally, studies utilised multiple theories, the most common combination being Routine Activities Theory and Personality Theory ($n=4$). Notably, two of the studies did not employ any theoretical lens.

Psychological characteristics of cyber scam victims

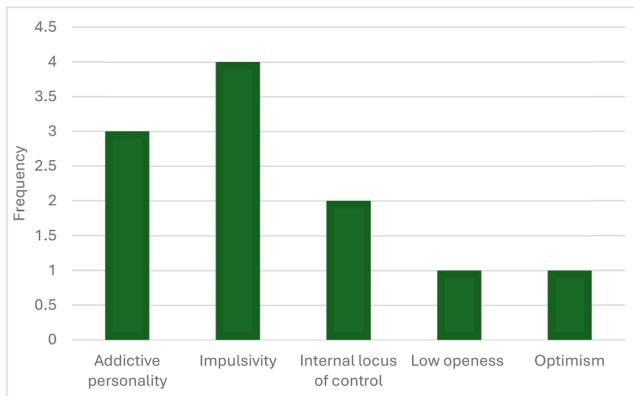
The second research question focused on psychological characteristics. The findings can be categorised into several groups, including personality, individual characteristics, behaviours, cognitive abilities and knowledge, self-esteem/overconfidence, and attitudes/beliefs.

Table 4. Theories employed to inform the investigation of psychological profiling of cyber scam victims.

Theory	f
Routine Activities Theory/ The Theory of Lifestyle and Routine Activities Theory (L-RAT)	16
Personality	7
Social Cognitive Theory	1
Belief systems	1
Self Control Theory	1
General Theory of Crime	1
Critical Theory	1

Table 5. Personality traits.

Personality	Significant results
Addictive personality	Addictive personality
Conscientiousness	
Extraversion	
Impulsivity	Impulsivity
Introversion	
Locus of Control	Internal locus of control
Openness	Low openness
Optimism	Optimism
Neuroticism	

**Figure 2.** Frequency of findings of personality traits across papers.

Personality

Table 5 sets out each personality characteristic examined in the studies in this SLR and the ones that were significant, and Figure 2 represents this visually (demonstrating the frequency of these findings). The work demonstrates that the following traits play a role in predicting victimhood of cyber scams: addictive personality, impulsivity, internal locus of control, scoring low on openness, and optimism.

Individual characteristics

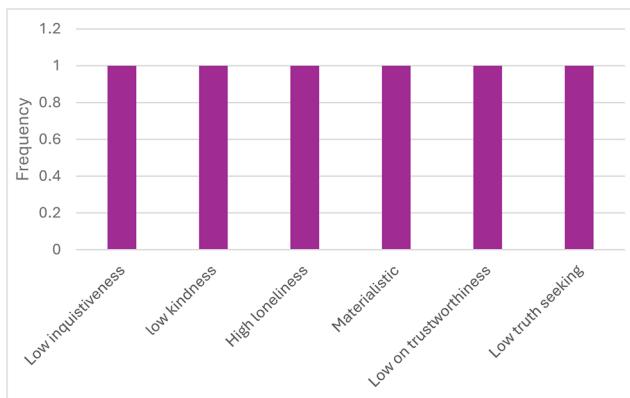
Table 6 outlines the individual characteristics examined and the ones which were significant, and Figure 3 represents this visually (demonstrating the frequency of these findings). The significant traits included low inquisitiveness, kindness, loneliness, materialism, trustworthiness, and truth-seeking. It is also worth noting that some variables, such as impulsivity and loneliness, were significant in certain studies but did not achieve significance in others.

Behaviours

Given that Routine Activities Theory is the most frequently applied theoretical framework, it is unsurprising that behaviours were measured more routinely than other variables. Nonetheless, no standardised methodology exists for the measurement of behaviours. At times, behaviours were more explicitly associated with Routine Activities Theory by examining guardian or exposure behaviours, for instance.

Table 6. Individual characteristics.

Individual characteristics	Significant results
Greed	
Gullibility	
Inquisitiveness	Low inquisitiveness
Kindness	Low kindness
Loneliness	High Loneliness
Materialistic	Materialistic
Mental health	
Overconfidence	
Susceptibility to persuasion	
Trustworthy	Low on trustworthiness
Truth seeking	Low truth seeking

**Figure 3.** Frequency of findings of individual characteristics across papers.

However, due to the myriad of methods employed by researchers to measure behaviours, a thematic analysis was conducted on the items to categorise them into coherent clusters (refer to [Table 7](#)).

Notably, Thematic Analysis (TA) is a flexible (Braun & Clarke, 2024; Terry et al., 2017), recursive approach to analysing qualitative data that proceeds through six interlinked phases: familiarisation with the dataset; coding, theme generation, theme review, theme definition and naming and report writing. Notably, although TA can be conducted from diverse epistemological positions, contemporary reflexive TA treats coding and theming as interpretive, rather than purely mechanical acts, emphasising the analyst's theoretical positioning and reflective engagement throughout (Braun & Clarke, 2024). Quality in TA is therefore demonstrated less by inter-coder reliability and more by conceptual coherence and transparency of decision-making.

In the present study, the corpus comprised routine behaviours reported across the 22 studies included in the SLR. Working at the semantic level, coded verbatim behaviour descriptors were extracted (rather than extended narrative text) and, through iterative comparison, the codes were organised into higher-order clusters that captured patterned meanings relevant to cyber-scam victimisation. The analytic documentation included reflexive notes to develop the themes. The final thematic structure comprised: financial transactions (behaviours involving payments, transfers, or account management), communication and social interaction (contact initiation, messaging, and relationship maintenance), information seeking (searching, verifying, or researching content and sources), general internet use (routine platform or device use not otherwise specified), risky practices (actions increasing exposure or susceptibility, such as sharing credentials or engaging with unsolicited links), and safe behaviours (security- and safety-oriented behaviours, such as multi-factor authentication and verification steps). This conceptualisation offers an organised lens on behavioural patterns in the literature and clarifies priorities for future research and intervention design.

Cognitive abilities/knowledge

Knowledge that a scam existed and individuals' cognitive abilities were other independent variables measured in these studies. The results on awareness were inconsistent (DeLiema et al., 2023), with one study

Table 7. Behaviours.

Online routine cluster	Items - Online routine activities	Significant results regarding online activities
Financial transactions	<ul style="list-style-type: none"> • Shopping • Banking • Investing • Selling stock • Investments made on the recommendations of others • Using auction websites • Using social media for financial purposes • Risky investments • Donations 	<ul style="list-style-type: none"> • Investments • Risky investments • Shopping • Trading • Investments made on recommendations of others • Donations
Communications/Social	<ul style="list-style-type: none"> • Sending emails • Communicating with strangers • Posting and sending messages • Provided strangers with personal information • Dating • Social media use • Streaming • Posting pictures 	<ul style="list-style-type: none"> • Online disclosure • Communicating with strangers • Steaming • Social media use • Dating
Seeking information	<ul style="list-style-type: none"> • Downloading files • Information consumption/browsing • Reading newspapers • Travel information • Work, study, education • Browsing 	• Low on Information consumption/browsing
General internet use	<ul style="list-style-type: none"> • Frequency of use • Own personal digital devices • Diversity of use 	<ul style="list-style-type: none"> • Frequency of use • Own personal digital devices • Diversity of use
Risky behaviours	<ul style="list-style-type: none"> • Opened attachments from unfamiliar emails/unknown sources • Opened any file or attachment they received through instant messages sent by strangers • Clicked on popup messages • Visiting questionable websites • Usually make payments via a personal computer or phone • Use personal information to create a password • Share passwords • Use similar passwords • Uploading personal content • Misbehaviour (e.g. hacking) • Weak passwords 	<ul style="list-style-type: none"> • Opened attachments from unfamiliar emails • Visiting questionable websites • Uploading personal content • Visiting questionable websites • Misbehaviour (e.g. hacking) • Risky behaviours, in general • Weak passwords
Safe behaviours	<ul style="list-style-type: none"> • Ask friends/family for advice about computer security • Make payments through safe means (e.g. Paypal) • Regularly change passwords for security reasons • Use complex passwords • Antivirus software • Read public education about cybercrimes • Careful about clicking links • Use security alerts for email and social media accounts • Update passwords frequently • Use a password manager • Strong passwords 	• Technical safeguards, in general

finding awareness to be a protective factor and another finding it to be a risk factor (Saad & Abdullah, 2018). Cognitive complexity, measured by questions about individuals' dislike of complex problems, was also found to be a predictor of victimhood (Kirwan et al., 2018).

Self-esteem/overconfidence

Studies explored the relationship between self-esteem and Internet abilities as a predictor of cyber scam victimhood. High self-esteem was found to be a protective factor; however, overconfidence was found to be a risk factor.

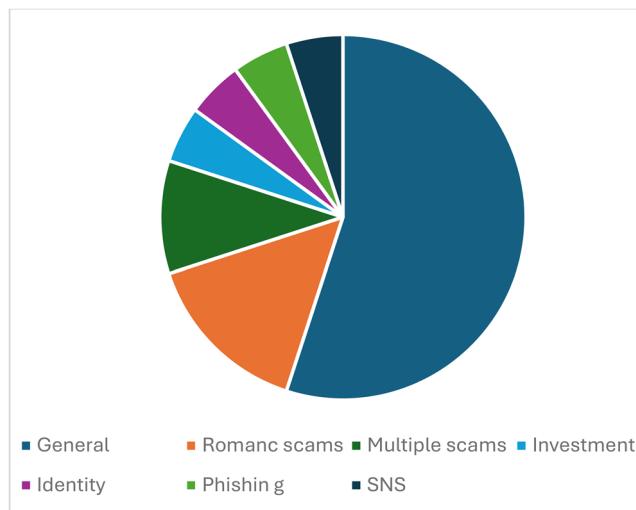


Figure 4. The number of papers which investigated a particular scam.

Attitudes/beliefs

Finally, specific attitudes and beliefs were found to predict cyber scam victimhood. Romantic beliefs, in particular idealisation, were found to predict romance scam victimhood (Buchanan & Whitty, 2014). A favourable attitude towards unregulated investments was found to predict Investment scam victimhood (Deliema et al., 2020).

Discussion

This systematic literature review addressed two questions: (1) Which theories have informed research on profiling victims of cyber scams? and (2) What psychological characteristics are associated with cyber-scam victimisation? The review covered studies published between 2000 and 2025, of which 22 met the inclusion criteria. The analysis revealed substantial heterogeneity in the theoretical frameworks employed, as well as in the operationalisation of outcomes (dependent variables) and predictors (independent variables). By synthesising these disparate approaches, the review clarifies points of convergence, highlights conceptual and methodological gaps, and delineates priorities to guide future research in this area.

The final SLR set comprised 22 studies spanning multiple cyber-scam modalities (e.g. phishing, romance, investment fraud) as well as papers that examined cyber scams in general; these distributions are shown in [Figure 4](#). Researchers primarily examined cyber scams in general (50%) (Balakrishnan et al., 2025; Chen et al., 2017; DeLiema et al., 2023; Gainey et al., 2023; Goede et al., 2024; Herrero et al., 2022; Junger et al., 2023; Parti, 2023; M. T. Whitty, 2019; Xin et al., 2024; Xu et al., 2024), while those focusing on a single scam targeted either romance scams (14%) (Buchanan & Whitty, 2014; Saad et al., 2018; Whitty, 2018b) or investment scams (9%) (Deliema et al., 2020). Studies adopting a general 'cyber-scam' lens were the most prevalent, yet the corpus exhibited substantial heterogeneity in theoretical framing and in the operationalisation of both outcomes (and predictors). These different foci make it challenging to compare studies.

Because different scam typologies plausibly exploit distinct vulnerabilities (Langenderfer & Shimp, 2001; Whitty, 2020) future work should explicitly compare predictors across scam types and populations using consistent theory-driven measures. Such designs can help distinguish common risk factors (e.g. impulsivity, low security self-efficacy) from scam-specific vulnerabilities (e.g. attachment needs in romance scams), enabling more targeted prevention and intervention strategies.

Two primary theoretical lenses were employed to investigate cyber scam victimhood: Personality and Routine Activities Theory. Personality theory refers to the family of conceptual frameworks that describe, predict, and explain relatively enduring patterns of cognition, affect, motivation and behaviour, as well as the psychological mechanisms that generate those patterns across time and situations (Mischel &

Shoda, 1995). Routine Activities Theory (RAT), in contrast, explains variation in criminal event by focusing on everyday patterns of activity that structure criminal opportunity. Rather than locating causes in offender pathology, RAT emphasises how social and technological arrangements of daily life redistribute opportunities for crime (Cohen & Felson, 1979). The findings from this SLR demonstrate that personality and routine activities serve as important predictors; however, other aspects, such as cognitive abilities, self-esteem, and beliefs (which held some promise), are rarely considered as significant independent variables. There was no consistency in the types of behaviours measured, prompting a thematic analysis in this paper to suggest a new approach in understanding particular clusters of behaviours. Developing questionnaires to measure the more significant variables emphasised in this paper may aid in advancing this research, allowing for more effective comparisons across studies.

Theoretical approaches

As stated above, the Personality (Cervone & Pervin, 2022) and Routine Activities Theory (Leukfeldt & Yar, 2016) were the typical lens to guide the research on cyber scam victimisation. However, other theoretical approaches may also be considered in the future. Table 8 shows suggestions for additional approaches. While acknowledging that other theories, in addition to those proposed in this paper, may also be helpful, these are some suggestions for advancing research into predicting cyber scam victimhood (see Table 8).

Cognitive Theory (Beck & Haigh, 2014) may be beneficial, given that research has found that the way a victim thinks about security and aspects related to a scam (e.g. romantic relationships, investments) can place them at risk of being scammed. As shown in Table 6, two theories that may be useful include the Theory of Planned Behaviour (Ajzen, 1991) and Information Processing Theory (Payne, 1980; Wickens & Carswell, 2021).

Social/Cognitive Theories may also provide important insights. Protection Motivation Theory (Boer & Seydel, 1996), for instance, may also play a role in prediction, given that it considers social and cognitive aspects. It has previously been applied to the consideration of protection factors for becoming scammed by romance scams (Luu et al., 2017) and has already demonstrated some promise in this field.

Psychological characteristics

Personality traits, individual characteristics, and behaviours were the most frequently considered predictors of cyber scam victimhood. The research, however, demonstrated little agreement on which factors to consider, even when employing the same theories.

Table 8. Proposed theories.

Theory	Rationale
• Cognitive TheoryTheory of Planned Behaviour (TPB) (Ajzen, 1991)	TPB offers a robust framework for understanding and predicting human behaviour across a wide range of context. Its application in this area is relevant because cyber scams exploit psychological, social and behavioural tendencies.
• Cognitive TheoryInformation Processing Theory (IPT) (Payne, 1980)	IPT focused on how individuals perceive, interpret and response to online stimuli. It focuses on how people process incoming information and make decisions based on that processing. Given that individuals need to make decisions about whether content or a person that are interacting with is genuine this may be a useful theory to employ in the prediction of cyber scam victimisation.
• Social/CognitiveProtection Motivation Theory (PMT) (Boer & Seydel, 1996)	PMT was developed to explain how people respond to threats and how they are motivated to protect themselves. PMT may explain why some individuals take protective action to avoid cyber scams and why others fail to act.
• Social/CognitiveSocial Identity Theory (SIT) (Tajfel, 2010)	SIT offers a compelling socio-psychological lens for understanding cyber scam victimhood, particular in terms of group affiliation, belongingness and ingroup/outgroup dynamics. With respect to cyber scams it may be applied to consider the identity cues criminals manipulate to create trust, simulate group membership or exploit social vulnerabilities.

Personality

These studies examined a mix of personality traits. Unsurprisingly, the Big Five (Zell & Lesick, 2022) was considered in a few studies; however, this did not yield any significant findings. Perhaps the most interesting results, worthy of further investigation, were impulsivity and addictive personality (which are related to one another). Impulsivity can be measured in several ways, as it is understood to have multiple components (Whiteside et al., 2005). Self-control was the most frequently measured aspect of impulsivity across these studies, which has been associated with other internet problems (Zahrai et al., 2022). Addiction is an interesting but underutilised predictor variable (Whitty, 2020). It may be important to consider further that if cyber scam victims tend to have an addictive personality, then building resilience to cyber scams may involve implementing techniques to support individuals with an addiction (e.g. support groups, abstaining from specific behaviours) (Carminati et al., 2023).

Individual characteristics

Across the included studies, researchers examined a wide array of individual-difference characteristics, yet relatively few showed consistent associations with cyber-scam victimisation. Many candidate variables appeared to be selected based on popular narratives about victims—such as greed, gullibility, materialism, or loneliness—rather than firm theoretical grounding (Xu et al., 2024). Several associations were also counterintuitive (e.g. lower inquisitiveness, low on kindness, trustworthiness). These patterns may reflect genuine mechanisms—for instance, prosocial or trust-oriented dispositions could increase compliance in social-engineering encounters—but they may also be artefacts of cross-sectional, self-report designs, post-event shifts in self-perception, or unmeasured confounding (e.g. differential exposure to scams). To clarify whether such characteristics are pre-dispositional risk factors or consequences of being scammed, future research should prioritise theory-driven studies (Burghardt & Bodansky, 2021), considering the findings highlighted in this paper.

Behaviours

How people behave online is clearly important to understand if we are to predict cyber scam victimhood. Behaviours were the most frequently considered independent variable; however, the studies demonstrate that despite the importance of examining behaviours, much more thought is needed into which behaviours need to be examined and how to measure them. A thematic analysis was carried out in this research to determine clusters of behaviours: Financial transactions, Communication/Social, Seeking information, General use, Risky Behaviours, and Safe Behaviours. Future research might consider developing questionnaires that measure each of these clusters. Some of these are clearly linked to theories, such as the Routine Activity Theory. However, they also suggest that other theories, such as the Information Processing Theory, the Theory of Planned Behaviour, the Protection Motivation Theory and Social Identity Theory (suggested in Table 6), may be important.

Dependent variable: measuring fraud victimisation

This review also identified substantial inconsistency in how fraud victimisation is operationalised. As summarised in Table 3, approaches varied widely: some studies defined ‘fraud’ and asked respondents whether they believed they had been victimised; others distinguished between cases involving financial loss and self-identified victimisation without monetary loss; and several did not report the exact items used. Time frames were likewise inconsistent, with some instruments referencing the previous 12 months and others assessing lifetime experiences. To improve comparability, future research should work toward a consensus definition and a standardised measurement protocol—specifying the reference period, item wording, and criteria for financial loss versus perceived victimisation. It is acknowledged that standardised measurement for routine behaviours may be challenging due to variation in behaviours that may need to be considered according to cyber scam type (e.g. romance scam online exposure behaviours may be very different to investment scams), nonetheless, a standardised list with agreed wording would be helpful to enable comparisons across studies.

Summary of predictors

Figure 5 provides a visual synthesis of the principal predictors identified in this SLR. Owing to substantial heterogeneity in study designs, operational definitions, and measurement instruments, the figure is offered as a heuristic model rather than a meta-analytic summary, and predictors are not weighted. Its purpose is to guide hypothesis generation and the selection of constructs in future research by organising the evidence into interpretable domains. The model also foregrounds plausible future studies. For instance, personality characteristics (e.g. impulsivity) and attitudes toward risk and security may moderate the link between routine online activities and victimisation outcomes, such that similar exposure patterns yield different risk profiles across individuals. Cognitive appraisals may function as mediators between dispositional factors and behaviour. Future studies can test these propositions using interaction terms and moderated (or mediated) models—e.g. hierarchical logistic regression, structural equation modelling, or moderated mediation—to estimate direct and indirect effects.

Limitations

There are a number of shortcomings of this research that need to be acknowledged. Although the search covered the period from 2000 to 2025, the earliest relevant studies identified were published in 2014, indicating that this research domain remains in its formative stages. Moreover, of the 22 papers included, 19 had different first authors, suggesting a limited pool of researchers contributing to the field. This relatively narrow time frame and dispersed authorship may constrain the theoretical perspectives available for consideration, potentially limiting the depth and coherence of theoretical development.

Despite searching a wide range of databases for this systematic literature review, it is possible that relevant findings reported in grey literature (e.g. police reports, government documents, or unpublished studies) were not captured. While this limitation is partly justified by the review's deliberate focus on peer-reviewed sources to ensure methodological rigour and quality assurance, grey literature may nonetheless offer valuable supplementary insights. Inclusion of such sources in future research could provide a more comprehensive understanding of the topic and reduce the potential for publication bias.

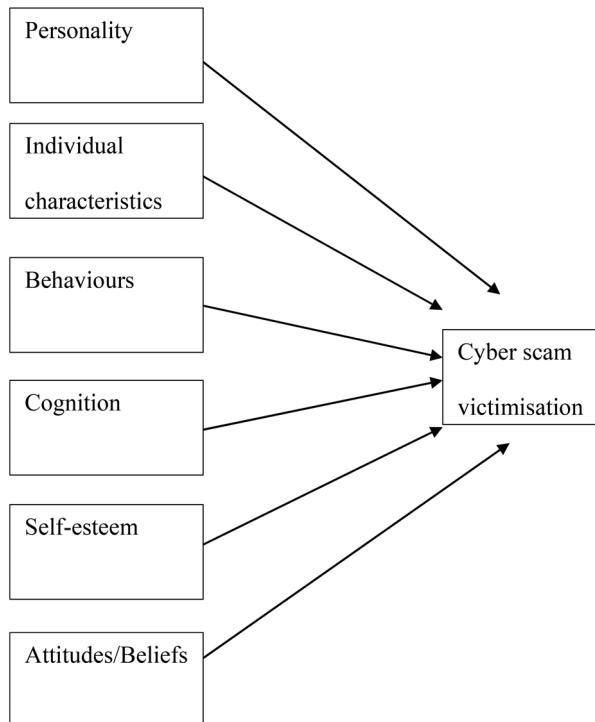


Figure 5. Summary of predictors.

It is also noteworthy that the sample sizes (N) across the included studies varied considerably, ranging from 280 to 11,534 participants. Such wide variation in sample size introduces challenges for drawing strong, generalisable conclusions from the body of evidence. Smaller studies may be more susceptible to sampling error and yield unstable estimates, while larger studies may dominate the synthesis despite potential methodological differences (Borenstein et al., 2021). This heterogeneity in study precision complicates cross-study comparisons and may contribute to variability in effect sizes, further limiting the strength of the inferences that can be drawn from the review's findings.

Several studies offered only limited methodological detail, providing brief descriptions of participant recruitment procedures and the measurement instruments used to assess predictor variables. Insufficient reporting of these elements reduces transparency and hinders the ability to evaluate the methodological quality of individual studies (Moher et al., 2010). Without details on sampling, inclusion criteria, and instrument validity and reliability, assessing generalisability or comparing studies is challenging. This lack of detail also constrains the potential for replication and limits the precision of cross-study synthesis, as methodological variations that may influence effect sizes or observed relationships cannot be adequately accounted for.

Although statistical results are reported from individual studies (e.g. odds ratios, regression coefficients), the analysis was unable to construct an aggregated synthesis that applied weighting by sample size, methodological rigour, or effect magnitude. Across studies, there was substantial inconsistency in construct operationalisation, statistical models, and outcome metrics, alongside frequent omissions of the information required to compute comparable effect sizes (e.g. standard errors, confidence intervals) or to perform quality- or precision-weighted analyses (Nikpeyma et al., 2020). Under these conditions, quantitative pooling would risk producing misleading summary estimates (Borenstein et al., 2021). In line with guidance for reviews encountering marked heterogeneity and incomplete reporting, a narrative synthesis was presented. This is also, however, acknowledged as a limitation. The absence of a formal meta-analytic aggregation precludes influence diagnostics, sensitivity analyses, and quantitative assessment of small-study or publication bias. Future primary studies should adhere to reporting standards that enable effect-size calculation (including variance estimates) and provide sufficient methodological detail to support quality appraisal and transparent weighting in evidence syntheses (Nikpeyma et al., 2020).

Conclusions

Building resilience—both pre-emptively to reduce susceptibility and post-incident to limit cascading harm—should be central to cyber-scam prevention agendas. Generic, ‘one-size-fits-all’ programs are unlikely to be effective because risk exposure, resources, and recovery needs vary markedly across populations; targeted approaches that account for sociodemographic factors, platform use, and access to support are therefore warranted (Southwick et al., 2014; Monica T. Whitty, 2019). This SLR indicates that victim profiling—defined here as identifying non-stigmatising constellations of psychological and behavioural risk factors—remains under-researched and methodologically heterogeneous. Evidence further suggests that attention to scam typologies (e.g. romance, investment, phishing) is essential because distinct scams plausibly exploit different vulnerabilities and affordances (Koning et al., 2024; Whitty, 2020).

To date, as shown in this SLR, studies most commonly draw on Personality frameworks and Routine Activities Theory (RAT). It is proposed here that complementary perspectives could offer additional, testable mechanisms: Protection Motivation Theory and the Theory of Planned Behaviour link threat/coping appraisals and perceived control to protective actions; information-processing models of persuasion specify when people rely on heuristic versus systematic cues (Whitty, 2013); and Social Identity Theory highlights how group norms and identity-congruent messaging may shape compliance or resistance online (Ajzen, 1991; Petty & Cacioppo, 1986; Tajfel, 2010). Consistent with opportunity-based explanations, RAT remains useful for modelling how exposure, target suitability, and (lack of) guardianship converge in digital ‘places’ to produce victimisation (Cohen & Felson, 1979).

To enable cumulative science, the field needs standardised outcome definitions (e.g. reference periods; criteria distinguishing monetary loss from self-identified victimisation) and a core battery of validated, multi-item measures for routine online activities, exposure, and psychological predictors. In this study, Figure 5 proposes a heuristic predictor model—spanning personality, individual characteristics, behaviours,

cognition, self-esteem, and attitudes/beliefs—to guide variable selection and theory testing. Notably, attitudes and beliefs remain under-examined despite emerging evidence that they may meaningfully condition risk and protective behaviour (Buchanan & Whitty, 2014). Finally, because transnational offenders, low reporting, and rapid platform change limit deterrence, victim-centred prevention—grounded in theory-informed profiling and non-stigmatising resilience building—should complement offender-focused strategies. This study highlights the need for adequately powered, and longitudinal designs (including moderated/mediated models across scam types) with transparent effect-size reporting to accelerate robust synthesis and actionable intervention design. This SLR provides a pathway to enhance future research into ways to protect cyber scam victims.

Disclosure statement

There are no competing interests to declare

Author contributions

Credit: **Monica Therese Whitty**: Conceptualization, Formal analysis, Investigation, Methodology, Writing – original draft, Writing – review & editing.

Funding

This research is supported by a Maureen Brunt Fellowship at Monash University

About the author

Professor Monica Whitty holds a Professorship in Human Factors in Cyber Security at Monash University. She is also a Maureen Brunt Fellow, which supports the top women researchers at Monash University. She is an expert in cybersecurity and cybercrimes, having led large interdisciplinary projects focused on cyber scams, insider threats, online deception, cybersecurity practices, education, awareness raising, and detecting and preventing disinformation. In 2025, she won the lifetime achievement award for her research in cyberpsychology and cybersecurity at the 28th Annual CyberPsychology, CyberTherapy & Social Networking Conference. She has been an expert witness on 10+ court cases for scam victims (especially victims who were unknowingly tricked into becoming a drug mule). She was a member of the Global Futures Communities for Cyber Security for the World Economic Forum. Prof Whitty is the author of 5 books and over 100 articles. Examples of her books include: 'Cyberspace Romance: The Psychology of Online Relationships' (2006, Palgrave) with Adrian Carr, and 'Truth, Lies and Trust on the Internet' (2009, Routledge) with Adam Joinson and 'Cyberpsychology: the study of individuals, society and digital technologies' (2008, John Wiley & Sons) with Garry Young.

ORCID

Monica Therese Whitty  <http://orcid.org/0000-0001-8143-289X>

Data availability statement

The data that support the findings of this study are available from the corresponding author, upon reasonable request.

References

- Aiken, M., Mc Mahon, C., Haughton, C., O'Neill, L., & O'Carroll, E. (2016). A consideration of the social impact of cybercrime: Examples from hacking, piracy, and child abuse material online. *Contemporary Social Science*, 11(4), 373–391. <https://doi.org/10.1080/21582041.2015.1117648>
- Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179–211. [https://doi.org/10.1016/0749-5978\(91\)90020-T](https://doi.org/10.1016/0749-5978(91)90020-T)
- Attrill, A. (2015). *Cyberpsychology*. Oxford University Press.
- Balakrishnan, V., Ahmed, U., & Basheer, F. (2025). Personal, environmental and behavioral predictors associated with online fraud victimization among adults. *PloS One*, 20(1), e0317232. <https://doi.org/10.1371/journal.pone.0317232>
- Balcombe, L. (2025). The Mental Health Impacts of Internet Scams. *International Journal of Environmental Research and Public Health*, 22(6), 938. <https://www.mdpi.com/1660-4601/22/6/938> <https://doi.org/10.3390/ijerph22060938>

- Bayl-Smith, P., Taib, R., Yu, K., & Wiggins, M. (2022). Response to a phishing attack: Persuasion and protection motivation in an organizational context. *Information & Computer Security*, 30(1), 63–78. <https://doi.org/10.1108/ICS-02-2021-0021>
- Beck, A. T., & Haigh, E. A. (2014). Advances in cognitive theory and therapy: The generic cognitive model. *Annual Review of Clinical Psychology*, 10(1), 1–24. <https://doi.org/10.1146/annurev-clinpsy-032813-153734>
- Bilz, A., Shepherd, L. A., & Johnson, G. I. (2023). Tainted Love: A Systematic Literature Review of Online Romance Scam Research. *Interacting with Computers*, 35(6), 773–788. <https://doi.org/10.1093/iwc/iwad048>
- Blythe, J. M., & Johnson, S. D. (2021). A systematic review of crime facilitated by the consumer Internet of Things. *Security Journal*, 34(1), 97–125. <https://link.springer.com/article/10.1057/s41284-019-00211-8> <https://doi.org/10.1057/s41284-019-00211-8>
- Boer, H., & Seydel, E. R. (1996). *Protection motivation theory*. In *Predicting health behaviour: Research and practice with social cognition models*. eds. Mark Conner, Paul Norman (pp. 95–120). Open University Press.
- Borenstein, M., Hedges, L. V., Higgins, J. P., & Rothstein, H. R. (2021). *Introduction to meta-analysis*. John Wiley & Sons.
- Braun, V., & Clarke, V. (2024). Supporting best practice in reflexive thematic analysis reporting in Palliative Medicine: A review of published research and introduction to the Reflexive Thematic Analysis Reporting Guidelines (RTARG). *Palliative Medicine*, 38(6), 608–616. <https://doi.org/10.1177/02692163241234800>
- Buchanan, T., & Whitty, M. T. (2014). The online dating romance scam: Causes and consequences of victimhood. *Psychology Crime & Law*, 20(3), 261–283. <https://doi.org/10.1080/1068316X.2013.772180>
- Burgess, A. W., Regehr, C., & Roberts, A. R. (2010). *Victimology: Theories and Applications*. Jones and Bartlett.
- Burghardt, J., & Bodansky, A. N. (2021). Why psychology needs to stop striving for novelty and how to move towards theory-driven research. *Frontiers in Psychology*, 12, 609802. <https://doi.org/10.3389/fpsyg.2021.609802>
- Button, M., Shepherd, D., Blackbourn, D., Sugiura, L., Kapend, R., & Wang, V. (2025). Assessing the seriousness of cybercrime: The case of computer misuse crime in the United Kingdom and the victims' perspective. *Criminology & Criminal Justice*, 25(2), 670–691. <https://doi.org/10.1177/17488958221128128>
- Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications*, 42, 36–45. <https://doi.org/10.1016/j.jisa.2018.08.002>
- Caneppele, S., & Aebi, M. F. (2019). Crime drop or police recording flop? On the relationship between the decrease of offline crime and the increase of online and hybrid crimes. *Policing: A Journal of Policy and Practice*, 13(1), 66–79. <https://doi.org/10.1093/police/pax055>
- Carminati, J.-Y. J., Ponsford, J. L., & Gould, K. R. (2023). "This group... I felt like I was medicating myself from this cyberscam illness that was living with me." A qualitative evaluation of co-designing cybersafety training resources with and for people with acquired brain injury. *Disability and Rehabilitation*, 45(22), 3719–3729. <https://doi.org/10.1080/09638288.2022.2139418>
- CASP. (2018). <https://casp-uk.net/>
- Cervone, D., & Pervin, L. A. (2022). *Personality: Theory and research*. John Wiley & Sons.
- 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 [Human Factors Engineering 4010]. *Computers in Human Behavior*, 70, 291–302. <https://doi.org/10.1016/j.chb.2017.01.003>
- CIFAS. (2024). Annual Report 2024. <https://www.cifas.org.uk/ar24>
- Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, 44(4), 588–608. <https://doi.org/10.2307/2094589>
- Creese, S., Hodges, D., Jamison-Powell, S., & Whitty, M. (2013). Relationships between Password Choices, Perceptions of Risk and Security Expertise. In L. Marinos & I. Askoxylakis, *Human Aspects of Information Security, Privacy, and Trust Berlin*. https://doi.org/10.1007/978-3-642-39345-7_9
- DeLiema, M., Gao, S., Brannock, D., & Langton, L. (2025). The Effects of Risky Behaviors and Social Factors on the Frequency of Fraud Victimization Among Known Victims. *Innovation in Aging*, 9(2), igae111. <https://doi.org/10.1093/geroni/igae111>
- DeLiema, M., Li, Y., & Mottola, G. (2023). Correlates of responding to and becoming victimized by fraud: Examining risk factors by scam type [Article. *International Journal of Consumer Studies*, 47(3), 1042–1059. <https://doi.org/10.1111/ijcs.12886>
- Deliema, M., Shadel, D., & Pak, K. (2020). Profiling Victims of Investment Fraud: Mindsets and Risky Behaviors. *Journal of Consumer Research*, 46(5), 904–914. <https://doi.org/10.1093/jcr/ucz020>
- Desolda, G., Ferro, L. S., Marrella, A., Catarci, T., & Costabile, M. F. (2022). Human factors in phishing attacks: A systematic literature review. *ACM Computing Surveys*, 54(8), 1–35. <https://doi.org/10.1145/3469886>
- DeTardo-Bora, K. A., & Bora, D. J. (2016). Cybercrimes: An overview of contemporary challenges and impending threats. *Digital Forensics*, 119–132. <https://doi.org/10.1016/B978-0-12-804526-8.00008-3>
- Dissanayake, N., Jayatilaka, A., Zahedi, M., & Babar, M. A. (2022). Software security patch management - A systematic literature review of challenges, approaches, tools and practices. *Information and Software Technology*, 144, 106771. <https://doi.org/10.1016/j.infsof.2021.106771>
- Fonseca, C., Moreira, S., & Guedes, I. (2022). Online consumer fraud victimization and reporting: A quantitative study of the predictors and motives [Criminal Behavior & Juvenile Delinquency 3236.]*Victims & Offenders*, 17(5), 756–780. <https://doi.org/10.1080/15564886.2021.2015031>
- Furnell, S., van Niekerk, J., & Clarke, N. (2014). The price of patching. *Computer Fraud & Security*, 2014(8), 8–13. [https://doi.org/10.1016/S1361-3723\(14\)70521-4](https://doi.org/10.1016/S1361-3723(14)70521-4)

- Gainey, R. R., Albanese, J. S., Vandecar-Burdin, T., Hawdon, J., Dearden, T. E., & Parti, K. (2023). Routine citizen Internet practices and cyber victimization: A state-wide study in Virginia [Behavior Disorders & Antisocial Behavior 3230]. *Criminal Justice Studies*, 36(3), 228–250. <https://doi.org/10.1080/1478601X.2023.2254094>
- Goede, M. S. V., van de Weijer, S., & Leukfeldt, R. (2024). Explaining cybercrime victimization using a longitudinal population-based survey experiment. Are personal characteristics, online routine activities, and actual self-protective online behavior related to future cybercrime victimization? *Journal of Crime and Justice*, 47(4), 472–491. <https://doi.org/10.1080/0735648X.2023.2222719>
- Greco, F., & Greco, G. (2020). Investigative Techniques in the digital age: Cybercrime and criminal profiling. *European Journal of Social Sciences Studies*, 5(3). <https://doi.org/10.46827/ejss.v5i3.821>
- Grieco, E. (2023). White-Collar Crime and terrorism: examining the Links and Challenges. In *Countering terrorist and criminal financing* (pp. 127–138). CRC Press.
- Guitton, C. (2012). Criminals and cyber attacks: The missing link between attribution and deterrence. *International Journal of Cyber Criminology*, 6(2), 1030–1043.
- Heap, V. (2021). Exploring the effects of long-term anti-social behaviour victimisation. *International Review of Victimology*, 27(2), 227–242. <https://doi.org/10.1177/0269758020961979>
- Herrero, J., Torres, A., Vivas, P., & Urueña, A. (2022). Smartphone addiction, social support, and cybercrime victimization: A discrete survival and growth mixture model [Substance Abuse & Addiction 3233]. *Psychosocial Intervention*, 31(1), 59–66. <https://doi.org/10.5093/pi2022a3> (Intervencion Psicosocial)
- Houtti, M., Roy, A., Gangula, V. N. R., & Walker, A. M. (2024). A survey of scam exposure, victimization, types, vectors, and reporting in 12 countries. arXiv Preprint, arXiv:2407.12896.
- Joinson, A. (2002). *Understanding psychology Internet behaviour: Virtual worlds, real lives*. Palgrave Macmillian.
- Junger, M., Koning, L., Hartel, P., & Veldkamp, B. (2023). In their own words: Deception detection by victims and near victims of fraud. *Frontiers in Psychology*, 14, 1135369. <https://doi.org/10.3389/fpsyg.2023.1135369>
- Kirwan, G., & Power, A. (2013). *Cybercrime: The psychology of online offenders*. Cambridge University Press.
- Kirwan, G. H., Fullwood, C., & Rooney, B. (2018). Risk Factors for Social Networking Site Scam Victimization Among Malaysian Students. *Cyberpsychology, Behavior and Social Networking*, 21(2), 123–128. <https://doi.org/10.1089/cyber.2016.0714>
- Kolupuri, S. V. J., Paul, A., Bhowmick, R. S., & Ganguli, I. (2025). Scams and Frauds in the Digital Age: ML-Based Detection and Prevention Strategies. *Proceedings of the 26th International Conference on Distributed Computing and Networking*, <https://doi.org/10.1145/3700838.3703672>
- Koning, L., Junger, M., & Veldkamp, B. (2024). Risk factors for fraud victimization: The role of socio-demographics, personality, mental, general, and cognitive health, activities, and fraud knowledge. *International Review of Victimology*, 30(3), 443–479. <https://doi.org/10.1177/02697580231215839>
- Lacey, D., Campbell, A., Goode, S., & Ridout, B. (2024). The cyberpsychology of deception: A mini review of the psychological factors influencing scam compliance. *Annual Review of CyberTherapy and Telemedicine*, 22, 34–41.
- Landis, J. R., & Koch, G. G. (1977). An application of hierarchical kappa-type statistics in the assessment of majority agreement among multiple observers. *Biometrics*, 33(2), 363–374. <https://doi.org/10.2307/2529786>
- Langenderfer, J., & Shimp, T. A. (2001). Consumer vulnerability to scams, swindles, and fraud: A new theory of visceral influences on persuasion. *Psychology & Marketing*, 18(7), 763–783. <https://doi.org/10.1002/mar.1029>
- Lazarus, S., Whittaker, J. M., McGuire, M. R., & Platt, L. (2023). What do we know about online romance fraud studies? A systematic review of the empirical literature (2000 to 2021). *Journal of Economic Criminology*, 2, 100013. <https://doi.org/10.1016/j.jeconc.2023.100013>
- Lee, H., & Choi, K.-S. (2022). Interrelationship between Bitcoin, ransomware, and terrorist activities: Criminal opportunity assessment via cyber-routine activities theoretical framework. In *The New Technology of Financial Crime*. (pp. 82–103). Routledge.
- Lee, J., & Soberon-Ferrer, H. (1997). Consumer vulnerability to fraud: Influencing factors. *Journal of Consumer Affairs*, 31(1), 70–89. <https://doi.org/10.1111/j.1745-6606.1997.tb00827.x>
- Leukfeldt, E. R. (2014). Phishing for Suitable Targets in The Netherlands: Routine Activity Theory and Phishing Victimization. *Cyberpsychology, Behavior and Social Networking*, 17(8), 551–555. <https://doi.org/10.1089/cyber.2014.0008>
- Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, 37(3), 263–280. <https://doi.org/10.1080/01639625.2015.1012409>
- Leuprecht, C., Skillicorn, D. B., & Tait, V. E. (2016). Beyond the Castle Model of cyber-risk and cyber-security. *Government Information Quarterly*, 33(2), 250–257. <https://doi.org/10.1016/j.giq.2016.01.012>
- Lickiewicz, J. (2011). Cyber Crime psychology-proposal of an offender psychological profile. *Problems of Forensic Sciences*, 2(3), 239–252.
- Luu, V., Land, L., & Chin, W. (2017). Safeguarding against romance scams—using protection motivation theory.
- Martineau, M., Spiridon, E., & Aiken, M. (2023). A Comprehensive Framework for Cyber Behavioral Analysis Based on a Systematic Review of Cyber Profiling Literature. *Forensic Sciences*, 3(3), 452–477. <https://www.mdpi.com/2673-6756/3/3/32> <https://doi.org/10.3390/forensicsci3030032>
- Mesch, G. S., & Dodel, M. (2018). Low self-control, information disclosure, and the risk of online fraud. *American Behavioral Scientist*, 62(10), 1356–1371. <https://doi.org/10.1177/0002764218787854>
- Minnaar, A. (2014). Crackers', cyberattacks and cybersecurity vulnerabilities: The difficulties in combatting the'new'cybercriminals. *Acta Criminologica: African Journal of Criminology & Victimology*, 27(sed-2), 127–144.

- Mischel, W., & Shoda, Y. (1995). A cognitive-affective system theory of personality: Reconceptualizing situations, dispositions, dynamics, and invariance in personality structure. *Psychological Review*, 102(2), 246–268. <https://doi.org/10.1037/0033-295x.102.2.246>
- Moher, D., Liberati, A., Tetzlaff, J., Altman, D. G., & Group, P, PRISMA Group. (2010). Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. *International Journal of Surgery (London, England)*, 8(5), 336–341. <https://doi.org/10.1016/j.ijsu.2010.02.007>
- Morgan, R. L., Whaley, P., Thayer, K. A., & Schünemann, H. J. (2018). Identifying the PECHO: A framework for formulating good questions to explore the association of environmental and other exposures with health outcomes. *Environment International*, 121(Pt 1), 1027–1031. <https://doi.org/10.1016/j.envint.2018.07.015>
- Mouncey, E., & Ciobotaru, S. (2025). Phishing scams on social media: An evaluation of cyber awareness education on impact and effectiveness. *Journal of Economic Criminology*, 7, 100125. <https://doi.org/10.1016/j.jeconc.2025.100125>
- Mugarura, N., & Ssali, E. (2021). Intricacies of anti-money laundering and cyber-crimes regulation in a fluid global system. *Journal of Money Laundering Control*, 24(1), 10–28. <https://doi.org/10.1108/JMLC-11-2019-0092>
- National Anti-Scam Centre. (2024). Targeting scams: Report of the National Anti-Scam Centre on scams data and activity 2024 <https://www.scamwatch.gov.au/system/files/targeting-scams-report-2024.pdf>
- Nikpeyma, N., Maroufizadeh, S., & Esmaeili, M. (2020). The importance of reporting the effect size in quantitative studies. *Nursing Practice Today*, 8(1), 4–6. <https://doi.org/10.18502/npt.v8i1.4486>
- Norris, G., Brookes, A., & Dowell, D. (2019). The Psychology of Internet Fraud Victimization: A Systematic Review [Article. *Journal of Police and Criminal Psychology*, 34(3), 231–245. <https://doi.org/10.1007/s11896-019-09334-5>
- 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. Article 02697580211010692 <https://doi.org/10.1177/02697580211010692>
- Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., ... Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *Systematic Reviews*, 10(1), 89. <https://doi.org/10.1186/s13643-021-01626-4>
- 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. <https://doi.org/10.3389/fpsyg.2023.1118741>
- Pasquini, D., Gangwal, A., Ateniese, G., Bernaschi, M., & Conti, M. (2021). 24–27. May 2021. *Improving Password Guessing via Representation Learning. 2021 IEEE Symposium on Security and Privacy (SP)*,
- Payne, J. W. (1980). Information processing theory: some concepts and methods applied to decision research. In T. S. Wallsten (Ed.), *Cognitive processes in choice and decision behavior*. (pp. 1–21). Routledge.
- Petrovic, L. (2025). The Linguistic Evolution of Internet Communication: Trends and Implications. *American Journal of Philological Sciences*, 5(04), 1–4. <https://inlibrary.uz/index.php/ajps/article/view/84499>
- Petty, R. E., & Cacioppo, J. T. (1986). *Communication and persuasion: Central and peripheral routes to attitude change*. Springer-Verlag.
- Rao, C. V. G., Chisty, N. M. A., Mishra, S. K., Sathe, M., Rizvi, S., & Soni, M. (2024). 22-23 March 2024)Innovations, Difficulties, and Approaches for Next-Generation Cybersecurity: Protecting the Digital Future. 2024 International Conference on Trends in Quantum Computing and Emerging Business Technologies, Rayyan. (n.d). <https://www.rayyan.ai/>
- Reyns, B. W., & Randa, R. (2020). No honor among thieves: Personal and peer deviance as explanations of online identity fraud victimization. *Security Journal*, 33(2), 228–243. <https://doi.org/10.1057/s41284-019-00182-w>
- Rogers, S. (2024). International scammers steal over \$1 Trillion in 12 months in global state of scams report 2024 Retrieved 31/3/25, from <https://www.gasa.org/post/global-state-of-scams-report-2024-1-trillion-stolen-in-12-months-gasa-feedzai>
- Ryder, N. (2024). To Report or Not to Report? An Analysis of the Relationship Between Defence Against Terrorism Financing Suspicious Activity Reports and Fraud in the United Kingdom. In D. Goldbarsht & L. de Koker (Eds.), *Financial Crime, Law and Governance: Navigating Challenges in Different Contexts*. (pp. 169–202). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-59547-9_8
- Saad, M. E., Norul, S., & Zamri, M. (2018). Cyber Romance Scam Victimization Analysis using Routine Activity Theory Versus Apriori Algorithm. *International Journal of Advanced Computer Science and Applications*, 9(12), 479–485. <Go to ISI>://WOS:000456778600067 <https://doi.org/10.14569/IJACSA.2018.091267>
- Saad, M. E., & Abdullah, S. N. H. S. (2018 13-15 Nov. 2018) *Victimization Analysis Based On Routine Activity Theory for Cyber-Love Scam in Malaysia* [Paper presentation].2018 Cyber Resilience Conference (CRC), <https://doi.org/10.1109/CR.2018.8626818>
- Sommestad, T., & Karlzén, H. (2024). The unpredictability of phishing susceptibility: Results from a repeated measures experiment. *Journal of Cybersecurity*, 10(1), tyae021. <https://doi.org/10.1093/cybsec/tyae021>
- Southwick, S. M., Bonanno, G. A., Masten, A. S., Panter-Brick, C., & Yehuda, R. (2014). Resilience definitions, theory, and challenges: Interdisciplinary perspectives. *European Journal of Psychotraumatology*, 5(1), 25338. <https://doi.org/10.3402/ejpt.v5.25338>
- Stalans, L. J., & Finn, M. A. (2016). Understanding How the Internet Facilitates Crime and Deviance. *Victims & Offenders*, 11(4), 501–508. <https://doi.org/10.1080/15564886.2016.1211404>

- Sucaldito, M. S. F., & Yu, K. C. (n.d.). Diagnostic performance of artificial intelligence tools for article screening during literature review: A systematic review.
- Suzuki, A. (2024). Routine activities and consumer fraud victimization: Findings from a social survey in Chiba Prefecture, Japan. *Crime Prevention and Community Safety*, 26(4), 373–384. <https://doi.org/10.1057/s41300-024-00219-2>
- Tajfel, H. (2010). *Social identity and intergroup relations*. (Vol. 7). Cambridge University Press.
- Taleby Ahvanooy, M., Zhu, M. X., Mazurczyk, W., Kilger, M., & Choo, K.-K. R. (2022). Do Dark Web and Cryptocurrencies Empower Cybercriminals?. In P. Gladyshev, S. Goel, J. James, G. Markowsky, & D. Johnson, *Digital Forensics and Cyber Crime*.
- Terry, G., Hayfield, N., Clarke, V., & Braun, V. (2017). Thematic analysis. *The SAGE Handbook of Qualitative Research in Psychology*, 2(17-37), 25.
- Titus, R. M., Heinzelmann, F., & Boyle, J. M. (1995). Victimization of persons by fraud. *Crime & Delinquency*, 41(1), 54–72. <https://doi.org/10.1177/001128795041001004>
- Trad, F., Yammine, R., Charafeddine, J., Chakhtoura, M., Rahme, M., Fuleihan, G. E.-H., & Chehab, A. (2024). Streamlining Systematic Reviews: A Novel Application of Large Language Models. *arXiv preprint arXiv:2412.15247*
- Valizadeh, A., Moassefi, M., Nakhostin-Ansari, A., Hosseini Asl, S. H., Saghab Torbati, M., Aghajani, R., Maleki Ghorbani, Z., & Faghani, S. (2022). Abstract screening using the automated tool Rayyan: Results of effectiveness in three diagnostic test accuracy systematic reviews. *BMC Medical Research Methodology*, 22(1), 160. <https://doi.org/10.1186/s12874-022-01631-8>
- Warkoo, A. (2014). Proposed Methodology for Cyber Criminal Profiling. *Information Security Journal: A Global Perspective*, 23(4-6), 172–178. <https://doi.org/10.1080/19393555.2014.931491>
- Walther, J. B., & Whitty, M. T. (2021). Language, psychology, and new media: The hyperpersonal model of mediated communication at twenty-five years. *Journal of Language and Social Psychology*, 40(1), 120–135. <https://doi.org/10.1177/0261927X20967703>
- Whiteside, S. P., Lynam, D. R., Miller, J. D., & Reynolds, S. K. (2005). Validation of the UPPS impulsive behaviour scale: A four-factor model of impulsivity. *European Journal of Personality*, 19(7), 559–574. <https://doi.org/10.1002/per.556>
- Whitty, M. T. (2013). The Scammers Persuasive Techniques Model: Development of a Stage Model to Explain the Online Dating Romance Scam. *British Journal of Criminology*, 53(4), 665–684. <https://doi.org/10.1093/bjc/azt009>
- Whitty, M. T. (2015). Mass-Marketing Fraud: A Growing Concern. *IEEE Security & Privacy*, 13(4), 84–87. <https://doi.org/10.1109/MSP.2015.85>
- Whitty, M. T. (2018a). 419 - It's just a Game: Pathways to cyber-fraud criminality emanating from West Africa. *International Journal of Cyber Criminology*, 12(1), 97–114. <https://doi.org/10.5281/zenodo.1467848>
- Whitty, M. T. (2018b). Do You Love Me? Psychological Characteristics of Romance Scam Victims. *Cyberpsychology, Behavior and Social Networking*, 21(2), 105–109. <https://doi.org/10.1089/cyber.2016.0729>
- Whitty, M. T. (2019). Predicting susceptibility to cyber-fraud victimhood [Article]. *Journal of Financial Crime*, 26(1), 277–292. <https://doi.org/10.1108/JFC-10-2017-0095>
- Whitty, M. T. (2019). Who can spot an online romance scam? *Journal of Financial Crime*, 26(2), 623–633. <https://doi.org/10.1108/JFC-06-2018-0053>
- Whitty, M. T. (2020). Is There a Scam for Everyone? Psychologically Profiling Cyberscam Victims [Article]. *European Journal on Criminal Policy and Research*, 26(3), 399–409. <https://doi.org/10.1007/s10610-020-09458-z>
- Whitty, M. T., & Buchanan, T. (2012). The online dating romance scam: A serious crime. *Cyberpsychology, Behavior and Social Networking*, 15(3), 181–183. <https://doi.org/10.1089/cyber.2011.0352>
- Whitty, M. T., & Buchanan, T. (2016). The online dating romance scam: The psychological impact on victims – both financial and non-financial [Article]. *J. Criminology & Criminal Justice: An International Journal*, 16(2), 176–194. <https://doi.org/10.1177/1748895815603773>
- Whitty, M. T., & Young, G. (2017). *Cyberpsychology: The Study of Individuals, Society and Digital Technologies* [Book] <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85186969783&partnerID=40&md5=180422fafdad1487d0403fd3050c86b6>
- Wickens, C. D., & Carswell, C. M. (2021). Information processing. In *Handbook of human factors and ergonomics* (pp. 114–158). John Wiley & Sons.
- Woods, D. W., & Walter, L. (2022). *Reviewing Estimates of Cybercrime Victimization and Cyber Risk Likelihood* [Paper presentation]. 2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW).
- Xin, Y., Xia, Y., & Chai, Y. (2024). Routine activities and fraud re-victimization among older adults: Do types of routine activities matter?. *Criminology and Criminal Justice*. <https://doi.org/10.1177/17488958241257860>
- Xu, L., Wen, X., Wang, J., Li, S., Shi, J., & Qian, X. (2024). Psychological predictors of online fraud victimhood in China: A machine learning approach. *Psychology, Crime and Law*, 1–24. <https://doi.org/10.1080/1068316X.2024.2389187>
- Young, G., & Whitty, M. (2012). *Transcending Taboos: A moral and psychological examination of cyberspace*. Routledge. <https://doi.org/10.4324/9780203126769>
- Zahrai, K., Veer, E., Ballantine, P. W., de Vries, H. P., & Prayag, G. (2022). Either you control social media or social media controls you: Understanding the impact of self-control on excessive social media use from the dual-system perspective. *Journal of Consumer Affairs*, 56(2), 806–848. <https://doi.org/10.1111/joca.12449>
- Zell, E., & Lesick, T. L. (2022). Big five personality traits and performance: A quantitative synthesis of 50+ meta-analyses. *Journal of Personality*, 90(4), 559–573. <https://doi.org/10.1111/jopy.12683>
- Zhou, Y., Hu, Z., & Li, F. (2023). Searchable Public-Key Encryption With Cryptographic Reverse Firewalls for Cloud Storage. *IEEE Transactions on Cloud Computing*, 11(1), 383–396. <https://doi.org/10.1109/TCC.2021.3095498>