

Article

Unpacking Internet-Based Social Engineering Victimization on Social Networking Sites: An Interdisciplinary Qualitative Framework of Individual, Social, and Platform Factors

Saad Saleh Alshammari ^{1,2} , Ben Soh ^{1,*}  and Alice Li ³

¹ Department of Computer Science and Information Technology, School of Computing, Engineering and Mathematical Sciences, La Trobe University, Bundoora, VIC 3086, Australia; s.alshammari@latrobe.edu.au

² Department of Computer Science, Faculty of Computer Science & Engineering, University of Hail, Hail 55476, Saudi Arabia

³ La Trobe Business School, La Trobe University, Bundoora, VIC 3086, Australia; a.li@latrobe.edu.au

* Correspondence: b.soh@latrobe.edu.au

Abstract

Despite extensive research on social engineering victimisation on social networking sites (SNSs) across the Internet, user susceptibility continues to increase, indicating that existing explanatory models remain incomplete. Previous studies have predominantly examined susceptibility through isolated factors, including individual traits, message characteristics, or source attributes, while often overlooking how evolving Internet-based SNS environments interact with human and social factors. To address this gap, this study presents an interdisciplinary qualitative investigation into emerging determinants of user susceptibility to social engineering cyberattacks (SECAs) on Internet-enabled SNS platforms. Drawing on in-depth interviews with 18 experts from cybersecurity, psychology, sociology, criminology, and linguistics, the study captures perspectives that are rarely integrated within a single analytical framework. Using NVivo 14 and inductive thematic analysis, six core themes and seven sub-themes were identified, revealing previously underexplored cognitive-emotional, social-relational, and platform-mediated mechanisms of victimisation. The key contribution of this research is not the identification of entirely new susceptibility factors, but the development of an interdisciplinary framework that integrates these previously disconnected dimensions. By foregrounding the role of SNS design affordances within the broader Internet ecosystem and their interaction with human cognition and social dynamics, this study advances current understanding beyond fragmented models of user vulnerability. The findings provide a novel conceptual foundation for future empirical research and inform the design of more effective, context-aware mitigation and awareness strategies for SECAs on Internet-based SNSs.

Keywords: social engineering; social network deception; user susceptibility; social networking sites; cyber literacy; cybersecurity behaviour



Academic Editors: Wei Zong and Yang-Wai Chow

Received: 18 May 2026

Revised: 17 June 2026

Accepted: 19 June 2026

Published: 25 June 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

1. Introduction

Social networking sites (SNSs) have become integral to global communication, connecting 5.24 billion users, approximately 63.9% of the global population [1,2]. While these platforms facilitate social interaction, content sharing, and the sharing of feelings, passions, and experiences [2], this digital connectivity also exposes users to cyber threats. Thus, SNSs have become prime targets for cybercriminals, particularly through SECAs [2,3].

Social engineering remains one of the most prevalent and sophisticated forms of cyber threats on SNSs. Relying on psychological manipulation techniques rather than technical exploits, attackers deceive individuals into divulging sensitive information or performing specific actions [4,5]. Because it is easier to deceive users than to breach secure systems, understanding user susceptibility on SNSs is essential.

Although the study of social engineering spans multiple disciplines [6–9], the persistent increase in SECAs reveals critical gaps in our current understanding. While various technical protection measures can reduce certain social engineering threats, they remain insufficient [10]. Therefore, addressing this growing risk requires moving beyond purely technical defences to adopt a holistic, interdisciplinary, and human-centred approach [6].

To address this gap, this study conducted a qualitative, semi-structured investigation involving 18 experts from diverse disciplines, including cybersecurity, psychology, sociology, criminology, and linguistics. This study aims to identify emerging factors influencing users' susceptibility to SECAs on SNSs and to provide recommendations to mitigate such attacks. Specifically, the study examined user vulnerabilities, SNS features that facilitate victimisation, source characteristics, message characteristics, and future research directions. This qualitative study is guided by the following research question: What are the emerging factors that contribute to the current occurrence of social engineering cyberattacks on social networking sites?

Based on these expert insights, this study proposes a novel framework that overcomes the highly fragmented nature of existing susceptibility models. Specifically, this study makes the following novel contributions to the literature:

- Unlike prior studies that isolate specific variables (e.g., source characteristics, message features, or user traits), this research proposes a holistic framework that integrates these previously disconnected dimensions into a single, cohesive model.
- The proposed framework expands beyond traditional cognitive variables by modelling acute emotional mechanisms, such as fear, empathy, and trust, that shape users' decision-making during social engineering attacks.
- The study provides a systematic inclusion of structural platform factors such as interface design, algorithms, and privacy controls to demonstrate how technological design directly influences susceptibility.
- The proposed framework offers a more reliable foundation for understanding user susceptibility by re-examining variables that have yielded inconsistent findings in the existing literature.

The remainder of this paper is organised as follows. Section 2 reviews related work. Section 3 introduces the proposed conceptual framework. Section 4 outlines the methodology used in this study. Section 5 presents and discusses the study's findings. Finally, Section 6 concludes the paper by summarising the key contributions and outlining directions for future research.

2. Related Work

Susceptibility to social engineering refers to the likelihood that an individual would be deceived by social engineering manipulation techniques [11]. User susceptibility to such attacks on SNSs has been extensively investigated. Previous studies have examined various influencing factors, including source characteristics, message characteristics, and user vulnerability. This section organises existing studies around the four main elements of a social engineering attack: the source that launches the attack, the message containing the request from the source, the target user, and the social networking site used as the medium for delivering the request, as shown in Figure 1.

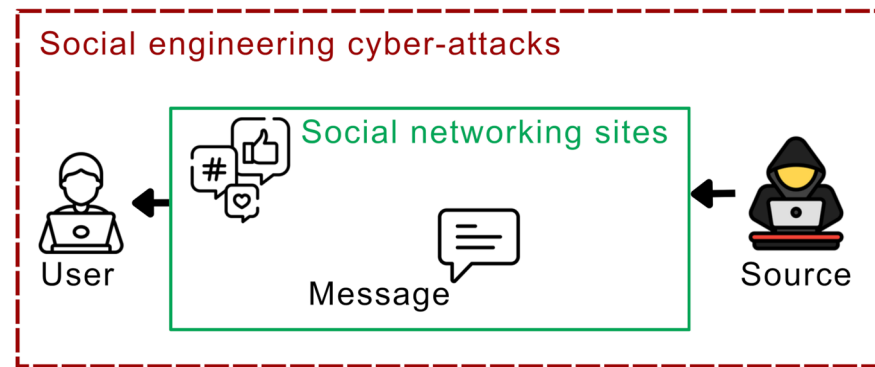


Figure 1. Main elements of a social engineering attack.

2.1. Source Characteristics

Existing research has examined the influence of source characteristics on users' susceptibility to social engineering victimisation. In particular, studies by Algarni et al. [12] on Facebook and Alturki et al. [13] on X (formerly Twitter), demonstrated that impersonating users who display specific attributes, such as number of friends, number of posts, real name, celebrity status, wealth, sexual compatibility, and authority, affects users' perceptions of source credibility and their judgments of message trustworthiness on SNSs. In contrast, Kano and Nakajima [14] argued that profile-based cues have no significant impact on user trust. Instead, they found that negative responses to a source's posts are the strongest predictor of perceived trustworthiness.

2.2. Message Characteristics

Attackers invest considerable effort and time in crafting convincing messages to maximise the effectiveness of their deception. The quality of a message's writing and design plays a critical role in determining its ability to mislead users. Existing research shows that message characteristics influence users' susceptibility to SECAs on SNSs. In examining the effects of central and peripheral routes of persuasion, as well as perceived risk, Algarni [11] found that characteristics such as message length, message organisation, spelling and grammar quality, the inclusion of supporting pictures or videos, and the number of likes all increase user susceptibility to social engineering victimisation. Similarly, Alturki et al. [13] reported that message style, message content interaction, and message content positively affect user vulnerability to SECAs.

2.3. User Vulnerability Factors

The individual user represents the primary target of SECAs. Algarni [11] emphasised that such attacks cannot succeed unless users accept, comply with, and perform the requested actions. Therefore, attackers seek to identify and exploit vulnerabilities at the user level. A substantial body of research has examined these vulnerabilities from multiple perspectives. These include socio-demographic factors such as age, gender, education, family structure and cultural background [15–18], as well as personality-based factors, particularly the Big Five traits, including openness, conscientiousness, extraversion, agreeableness and neuroticism [15,19–22].

In addition, user vulnerability has been examined through socio-emotional dimensions, including trust in SNS providers and trust in SNS users, as well as motivation, confidence, and impulsivity [17,20,21,23–26]. Habitual factors have also been considered, such as usage habits, frequency and duration of using SNS, and level of involvement [15,18,21–26]. Furthermore, perceptual and cognitive factors, including risk perception, privacy and security awareness, social network experience, competence, self-efficacy, and cybercrime experience, have been identified as significant determinants of vulnerability [15,18,19,21,23,24,27].

Recent SNS and security literature highlights that user susceptibility to SECAs is influenced by a combination of behavioural, cognitive, and social factors. For instance, Klütsch et al. [28] found that messages appearing to originate from known senders significantly increase user trust and phishing susceptibility, particularly among individuals with high levels of Fear of Missing Out (FoMO). This aligns with broader arguments by Kaur et al. [29], who posit that the structural design of SNS environments facilitates cybercrime by encouraging trust-based interactions and rapid information sharing. Beyond purely social triggers, professional motivations can blind users to security risks. Alotaibi [30] found that LinkedIn users seeking career advancement or increased professional visibility were significantly more likely to engage with suspicious messages and malicious connection requests. Furthermore, Alameeri and AlMourad [31] highlighted how vulnerability varies across demographic groups. Although their study lacks empirical validation, they suggest that younger and older adults, as well as women, may be particularly susceptible to SECAs.

Concurrently, recent studies also highlight the limitations of existing countermeasures and the need for more comprehensive approaches to mitigating SECA risks. Traditional intervention strategies, such as standard cyber awareness programs, frequently fail to translate knowledge into secure habits. Mouncey and Ciobotaru [32] found that while these awareness programs successfully enhance digital literacy, they often fail to produce meaningful behavioural change when users encounter sophisticated, real-world phishing attacks. This gap between awareness and behaviour is further evidenced by Blancaflor et al. [33], who showed that students frequently engaged with malicious links embedded in familiar social media contexts, despite their awareness of cybersecurity risks. This behavioural vulnerability is actively exploited by attackers, as Panda [34] argues that attackers have evolved from generic phishing techniques to highly targeted, psychologically manipulative strategies that bypass many traditional technical defences. Thus, as emphasised by both Kaur et al. [29] and Alameeri and AlMourad [31], current mitigation strategies remain insufficient because they overlook these platform-specific influences and human-centred vulnerabilities.

2.4. Gaps in Existing Research

Existing research on social engineering victimisation within SNSs has provided valuable insights into attackers' techniques and the wide range of factors that influence user susceptibility. Yet, much of this work has maintained a relatively narrow focus, concentrating primarily on source characteristics, message features, and user-level psychological variables, including personality traits. As SECAs continue to evolve and user victimisation rates remain persistently high, these trends expose a critical gap in the literature and highlight the need for a more holistic, integrated understanding of the phenomenon. Accordingly, this study seeks to address several key gaps in existing literature:

2.4.1. Limited Integration of Individual, Message, and Platform Factors

Recent studies have advanced understanding of phishing susceptibility, online trust, cyberpsychology, and human-centred cybersecurity. However, susceptibility continues to be examined primarily through isolated perspectives, such as individual traits, message characteristics, or source credibility. Relatively limited attention has been paid to the interaction between these factors and SNS platform affordances, including algorithmic recommendation systems, engagement-driven interface design, privacy controls, and content amplification mechanisms. As a result, current models provide only a partial understanding of the socio-technical processes that shape susceptibility to social engineering attacks.

2.4.2. Limited Focus on Individual Emotions

Although user susceptibility has been extensively examined in the literature, the emotional dimensions of user behaviour remain comparatively underexplored. A deeper investigation is required to understand how users' emotional responses, such as fear, anger, empathy, or trust, shape decision-making processes in social engineering contexts. This would provide a more nuanced understanding of the psychological mechanisms that underpin vulnerability to manipulation on SNSs.

2.4.3. Limited Focus on SNS Platform-Level Factors

Despite extensive research examining victimisation in SNS environments, empirical studies examining how platform-level characteristics influence user susceptibility remain limited and fragmented. [11]. In particular, the relationship between SNS design features, such as interface architecture, algorithmic structures, and privacy controls, and user judgment remains insufficiently understood. Addressing this gap is essential for developing a more comprehensive understanding of how technological affordances influence vulnerability to SECAs.

2.4.4. Variables with Inconsistent Empirical Effects in the Literature

As reported by Alshammari et al. [35], although numerous studies have examined variables influencing user susceptibility to SECAs on SNSs, findings for several variables remain inconsistent or inconclusive. The findings in Table 1 indicate considerable inconsistency across several variables examined in the existing literature on SNS phishing susceptibility.

Table 1. Variables with mixed findings across studies on their effect on susceptibility to SECAs.

Variable	Positive Effect	Negative Effect	No Effect
Age	[15,22]		[18]
Education		[15]	[16,18,24]
Trust	[15,23]		[18]
Motivation	[15]		[18,23]
Frequency of use	[15,22,27]		[24]
Risk perception	[11]	[15,18]	[21,23]
Cybercrime experience	[18,23]	[15]	
Competence		[23]	[18]
Message content	[13]	[14]	
Number of connections	[15,18,26,27]	[23]	

Variables such as risk perception, cybercrime experience, message content, and number of connections demonstrated contradictory effects across studies. For example, risk perception was reported to have a positive effect in [11], a negative effect in [15,18], and no significant effect in [21,23]. Similarly, cybercrime experience showed positive effects in [18,23] but a negative effect in [15]. Message content also produced mixed findings, with [13] identifying a positive effect and [14] reporting a negative effect. In addition, the number of social connections was associated with increased susceptibility in [15,18,26,27], whereas [23] found a negative effect. Other variables, including age, education, trust, motivation, frequency of use, and competence, also showed inconsistent relationships across studies. These conflicting findings highlight the fragmented and inconclusive nature of the current literature and underscore the need for further investigation.

2.4.5. Lack of Interdisciplinary Integration

Few studies have integrated insights from cybersecurity, psychology, sociology, criminology, and linguistics within a single explanatory framework. As SNS ecosystems become increasingly complex and incorporate AI-driven content generation and recommendation technologies, a more comprehensive socio-technical understanding of social engineering victimisation is required.

2.4.6. Lack of a Holistic Susceptibility Framework

To address these gaps and overcome the limitations of existing susceptibility models, this study proposes a robust, expert-informed model that spans three key dimensions: individual, social, and platform-level factors. The main novelty of this framework lies in moving beyond the highly fragmented models that have dominated prior research. Rather than examining source characteristics, message features, or user traits in isolation, the proposed framework integrates these established variables with two critical but understudied dimensions: emotional mechanisms and SNS platform design.

In addition, the framework also re-examines variables that have previously produced inconsistent results in prior research. By integrating these dimensions into a unified model, the framework offers a more comprehensive and cohesive understanding of user susceptibility and captures the complex interactions between human behaviour, social dynamics, and technological design that contribute to vulnerability to SECAs.

To illustrate the limitations of existing approaches and demonstrate how the proposed framework addresses them, Table 2 maps the dominant models in the literature to the dimensions of the proposed framework. As shown, prior research has focused predominantly on source characteristics, message features, and psychological trait, while emotional mechanisms and platform-level factors have largely been missing from integrated susceptibility models.

Table 2. Comparison of previous susceptibility models and the proposed framework.

[Study]	Source Characteristics	Message Characteristics	User Traits	Emotional Mechanisms	SNS Platform Factors
[36]	✓				
[15]			✓	~ *	
[11]		✓			
[23]			✓	~ *	
[37]			✓		
[20]			✓		
[18]			✓	~ *	
[13]	✓				
[21]			✓		
Proposed Framework	✓	✓	✓	✓	✓

* Note: (~) denotes partial coverage (only one or two emotional factors examined).

3. Proposed Conceptual Qualitative Framework

Building on the research gaps identified in Section 2, we propose a conceptual qualitative framework. It integrates emergent themes into a theoretically grounded model encompassing individual, social, and platform-related influences.

Figure 2 illustrates this framework, developed through thematic analysis of semi-structured interview data. The framework synthesises the key themes and sub-themes that emerged inductively from participants' narratives and organises them into a coherent, theoretically informed structure. Rather than simply categorising themes, the framework conceptualises the dynamic relationships among individual, social, and platform-related factors that shape the phenomenon under investigation.

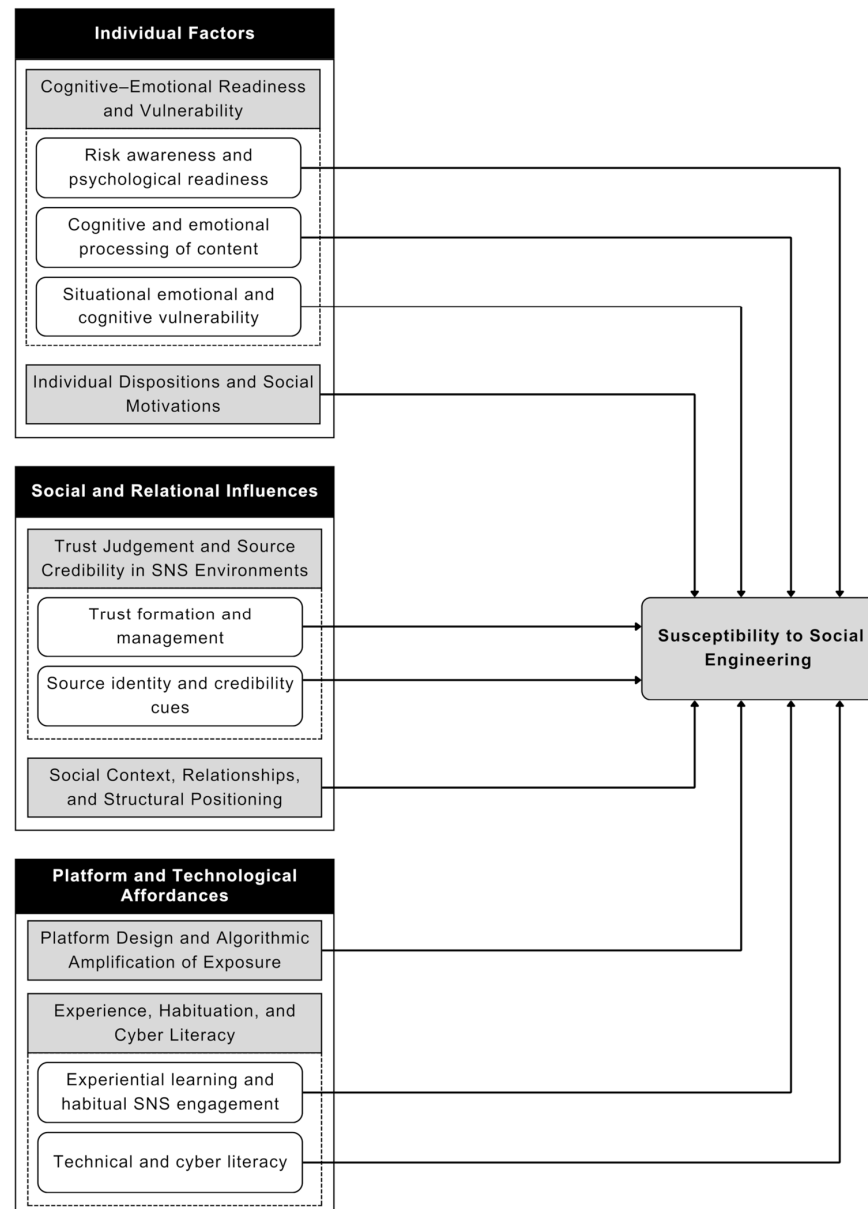


Figure 2. Research conceptual model.

3.1. Theoretical Positioning

The framework adopts an interdisciplinary perspective to develop a comprehensive understanding of the phenomenon under investigation. It draws on behavioural psychology to explain how cognitive biases, heuristics, and emotional triggers shape decision-making processes and contribute to susceptibility to manipulation. It also incorporates insights from sociology and communication studies to examine social influence, trust formation, and relational dynamics in online interactions. In addition, concepts from cybersecurity and information systems, including platform affordances, digital literacy, and system design, are used to clarify how technological structures can enable or constrain user

behaviour. The framework is further informed by criminology and victimology, especially theories of situational vulnerability, offender tactics, and routine activity theory, which illuminate how motivated offenders exploit opportunities within specific contexts. Taken together, these disciplinary perspectives underscore the complexity of SECAs, which cannot be adequately explained through a single lens. The framework, therefore, moves beyond purely technical or purely psychological explanations and instead conceptualises susceptibility as the outcome of interacting individual, social, and platform-related processes.

3.2. Core Domains of the Framework

The proposed framework is organised around three interrelated domains, as illustrated in Figure 2. Each domain represents a cluster of thematically connected factors that emerged from the data.

3.2.1. Individual-Level Factors

This domain captures the personal characteristics and internal psychological processes that shape how individuals perceive, interpret, and respond to potential threats. It focuses on cognitive and affective mechanisms that influence decision-making, particularly in contexts involving uncertainty, perceived risk, or persuasive manipulation. Key sub-themes include cognitive biases and heuristics, emotional states and affective responses, digital literacy and prior experience, risk perception, and threat appraisal. These factors can increase susceptibility to misleading information or deceptive cues by encouraging reliance on mental shortcuts, emotional reactions, or inaccurate assessments of harm. Participants also emphasised that susceptibility is not determined solely by knowledge deficits; rather, emotional urgency, assumptions about trust, and cognitive shortcuts can override rational evaluation. This highlights the importance of conceptualising vulnerability as situational and dynamic rather than static.

3.2.2. Social and Relational Factors

This domain highlights the influence of social context on behaviour in online environments. Social dynamics play a crucial role in how messages are interpreted and how decisions are made, often mediating the boundary between scepticism and compliance. Trust is frequently established through perceived familiarity, shared identity, or relational closeness. Participants noted that users are more likely to accept messages or requests that appear to originate from known contacts, familiar communities, or individuals with similar backgrounds or values. Peer norms and relational obligations can further guide compliance, as social expectations may prompt individuals to respond positively even when uncertainty persists. Additionally, social proof and authority cues, such as endorsements, institutional symbols, or claims of expertise, can enhance message credibility, reduce critical scrutiny, and increase the likelihood of engagement. This domain demonstrates that victimisation risk is embedded within social ecosystems, especially in digitally mediated environments like SNSs, where identity cues and relational signals can be strategically manipulated.

3.2.3. Technological and Platform Affordances

This domain addresses the technological structures and platform-level features that shape user behaviour in digital environments. It examines how platform architecture, system design, and embedded affordances can either facilitate or mitigate exposure to exposure. Design features such as messaging systems, anonymity options, and algorithmic amplification may lower barriers to interaction, enable identity concealment, and rapidly disseminate content to wide audiences. SNSs' mechanisms for prioritising or recommending content can influence the visibility and perceived legitimacy of malicious messages. Usability and interface cues, such as layout, visual indicators, prompts, and notification

styles, can subtly guide users' attention and decision-making. Visibility and privacy settings likewise affect how much personal information users inadvertently disclose, shaping both perceived safety and actual vulnerability. Finally, security controls and user awareness mechanisms, such as warning notifications, authentication processes, and reporting tools, play an essential role in supporting informed decision-making. Experts frequently described how these platform affordances can reduce users' vigilance or create unwarranted assurances of legitimacy. As such, the framework positions technology not as a neutral backdrop but as an active mediator of risk.

3.3. *Dynamic Interactions and Process Orientation*

A key contribution of the framework lies in its process-oriented design. Rather than prototyping influencing factors as isolated predictors of susceptibility, Figure 2 conceptualises them as dynamically interconnected components operating within an evolving decision-making process. This perspective emphasises how individual, social, and platform-related elements interact in real time to shape users' perceptions, judgements, and behavioural outcomes. For example, platform affordances can intensify social influence cues by enhancing the visibility of indicators such as popularity, legitimacy, or authority. Similarly, emotional triggers often interact with cognitive biases to accelerate decision-making, as emotions such as fear, urgency, excitement, or trust may increase reliance on heuristics and reduce the depth of deliberative processing. These cognitive and affective mechanisms therefore operate synergistically rather than independently. By foregrounding these interdependencies, the framework provides a more holistic understanding of susceptibility and victimisation within socio-technical environments.

The framework conceptualises susceptibility as a dynamic socio-technical process rather than a static individual trait. It proposes that vulnerability unfolds through a sequence of interconnected stages shaped by interactions among personal, social, and platform-level factors. The process begins with exposure to a stimulus, such as a message, notification, or online interaction. This initial encounter is conditioned by platform affordances, visibility settings, and situational context, which determine how and when the stimulus reaches the user. Following exposure, individuals engage in cognitive–emotional appraisal. At this stage, they interpret the content, assess its relevance and credibility, and experience emotional responses such as curiosity, urgency, fear, or trust. Cognitive biases and heuristics may further influence this appraisal, particularly under conditions of time pressure, distraction, or cognitive load. The subsequent stage involves social interpretation. Here, individuals evaluate the message within a broader relational and social framework, taking into account perceived familiarity, shared identity, authority cues, and prevailing peer norms. Social context influences whether the stimulus is perceived as legitimate, expected, or socially endorsed. Ultimately, the process culminates in a behavioural response. Depending on the combined effects of appraisal and interpretation, individuals may choose to comply, ignore, verify, report, or respond in other ways to the stimulus. This behavioural outcome reflects the cumulative influence of interacting socio-technical factors operating across the preceding stages. Importantly, feedback loops may emerge over time, as prior experiences recalibrate users' perceptions of risk and shape subsequent coping strategies.

3.4. *Conceptual Contribution*

The proposed framework offers three principal contributions to both theory and practice. First, it provides theoretical integration by unifying psychological, social, and platform-related perspectives within a single conceptual model. This integrative approach moves beyond fragmented explanations of susceptibility and yields a more comprehensive understanding of how individual cognition, social dynamics, and platform design

intersect to shape user vulnerability. Second, the framework advances a process-oriented understanding of susceptibility by conceptualising vulnerability as emerging through dynamic interactions and evolving decision pathways rather than as the result of static or isolated risk factors. This shift foregrounds the temporal, contextual and relational dimensions of decision-making across the sequential stages of exposure, appraisal, interpretation, and response. Third, the framework demonstrates practical relevance by generating actionable insights for intervention. At the individual level, it informs the development of targeted educational initiatives and digital literacy programs. At the social level, it supports strategies aimed at shaping social norms and strengthening collective awareness. At the platform level, it identifies opportunities for improving system design and implementing user-centred security mechanisms. Although Figure 2 provides a structural overview of the relationships among these domains, the detailed empirical substantiation, supported by illustrative participant excerpts, is presented in Section 5, where each component is analysed in depth.

4. Methodology

This study employed a qualitative research design to investigate emerging factors that influence user susceptibility to SECAs on SNSs. A qualitative approach was selected to capture in-depth expert insights into complex and evolving socio-technical phenomena that remain insufficiently theorised in the existing literature. The research process was guided by Kvale’s seven-stage interview model [38], thematising, designing, interviewing, transcribing, analysing, verifying, and reporting, which provided a systematic and coherent structure for the study. Figure 3 illustrates the methodological process followed in this study.

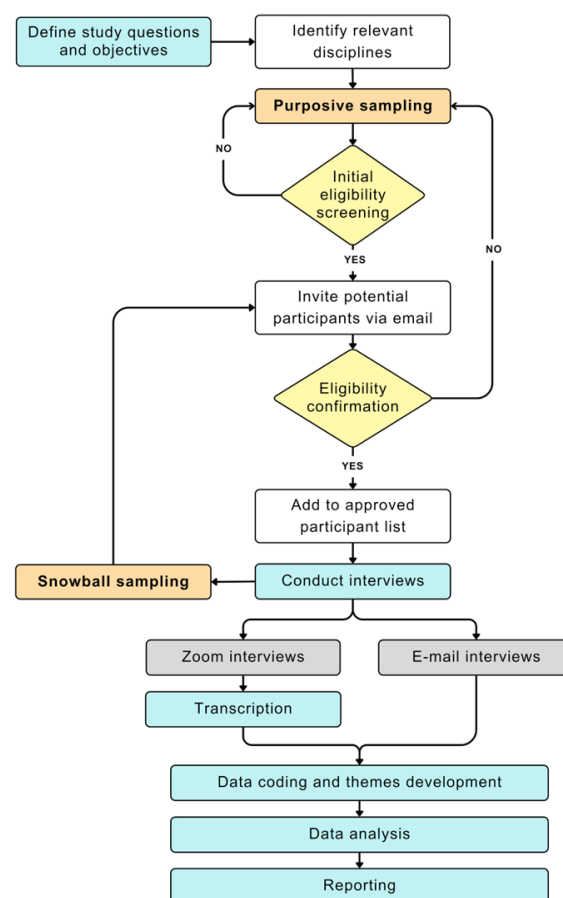


Figure 3. Research methodology flowchart.

4.1. Research Design and Participants

Data were collected through semi-structured expert interviews conducted between September and November 2025. As shown in Figure 4, a total of 18 experts participated in the study, representing five disciplines closely aligned with social engineering research: cybersecurity (n = 4), psychology (n = 4), criminology (n = 5), linguistics (n = 4), and sociology (n = 1). Although only one participant was classified as a sociologist, several criminology experts also had expertise in sociology and were categorised according to their primary area of expertise. Most participants held doctoral degrees, possessed extensive professional experience (typically exceeding 15 years), and demonstrated long-term engagement with SNSs.

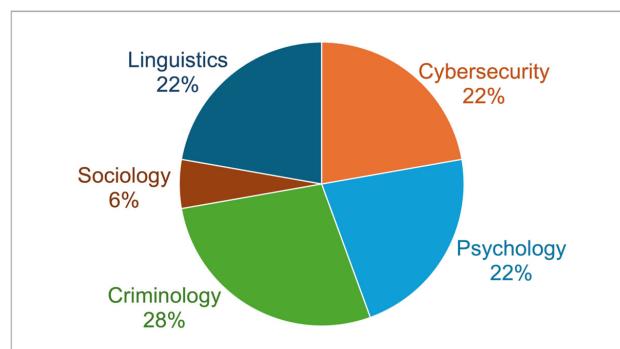


Figure 4. Total experts per discipline.

To be eligible for inclusion, participants were required to have a minimum of three years of professional experience in their respective fields and at least three years of active SNS use. These criteria ensured that the interviewees brought both substantive domain expertise and practical familiarity with SNS environments [39]. Table 3 provides a detailed overview of participant characteristics.

Table 3. Overview of expert participants.

Participant ID	Level of Education	Years of Professional Experience	Years of Using SNSs	Discipline	Current Role
Expert 1	PhD	25	15	Cybersecurity	Lecturer of Cybersecurity
Expert 2	Masters	NA *	NA *	Cybersecurity	PhD researcher
Expert 3	Masters	5	10	Cybersecurity	Cybersecurity Researcher
Expert 4	PhD	31	20	Cybersecurity, psychology, engineering, & business	Dean of the School of Cyber Security and Information Technology
Expert 5	PhD	18	20–25	Psychology	Professor of Cyber Resilience
Expert 6	PhD	30	20	Psychology	Professor of Psychology
Expert 7	PhD	25	17	Psychology	Professor of Psychology
Expert 8	PhD	25	20	Cyber psychology/ psychology	Senior lecturer in cyber psychology
Expert 9	PhD	27	25	Law, sociology, criminology and criminal justice	Associate professor of sociology

Table 3. Cont.

Participant ID	Level of Education	Years of Professional Experience	Years of Using SNSs	Discipline	Current Role
Expert 10	PhD	11	14	Criminal justice, criminology	Full professor of sociology and criminology
Expert 11	PhD	10	5	Criminology & cybersecurity	Cybersecurity investigator
Expert 12	PhD	17	20	Cybersecurity & criminology	Cybersecurity Cybercrime Researcher & Cybersecurity expert consultant
Expert 13	PhD	4	10	Criminology	Professor of Criminology
Expert 14	Master's	15	21	Linguistics	Lecturer of English
Expert 15	PhD	35	20	Linguistics	Professor of Linguistics
Expert 16	PhD	22	15	Linguistics and criminology	Professor in Criminology and Justice Studies
Expert 17	PhD	20	25	Data Science and Linguistics	Professor of linguistics
Expert 18	PhD	20	17	Criminology	Professor of Criminology

* Note: Expert 2 confirmed meeting the minimum inclusion criteria prior to participation, but opted not to disclose the exact figures.

4.2. Sampling Size and Recruitment

4.2.1. Sampling Size

Determining an appropriate number of interviews in qualitative research depends on the purpose and depth of a study. Kvale [38] suggests that researchers should conduct “as many as necessary to find out what you need to know”. Mason [9] reports that qualitative PhD studies typically include between 15 and 50 interviews. Similarly, Blandford [40] notes that semi-structured interviews in the information systems field, particularly in human–computer interaction (HCI), typically involve 10–20 participants.

In this study, 15–20 semi-structured interviews were targeted, with participants distributed across the selected disciplines of cybersecurity, psychology, sociology, criminology, and linguistics. This approach aimed to include approximately three to four participants from each discipline to ensure a diversity of perspectives. The sample size was guided by the principle of data saturation, defined as the point at which additional interviews no longer yield new insights [41]. Although Guest et al. [41] found that saturation often occurs after 12 interviews for relatively homogeneous samples, the interdisciplinary and exploratory nature of this study required a broader range of expertise. Therefore, a sample of 15 to 20 participants was considered sufficient to achieve both conceptual depth and thematic variation, while remaining feasible within the study's time and resource constraints.

Regarding the recruitment process, a two-stage sampling strategy was employed, combining purposive and snowball sampling techniques.

4.2.2. Purposive Sampling

Purposive sampling was used to identify and screen eligible experts based on their professional backgrounds, publication records, or institutional roles. This assessment was conducted using publicly available sources, including Google Scholar, ResearchGate, LinkedIn, and relevant university or organisational websites. Eligible candidates were selected based on their expertise and their potential to contribute to the study's objectives [39].

The second part of this sampling involved confirming participant eligibility and willingness to participate. Experts who met the initial screening criteria were contacted via email and invited to take part in the study. The invitation included a participant information statement outlining the study's purpose, the rationale for their selection, the expected interview duration, and the selection criteria, as well as a consent form. An interview guide detailing the questions was also provided to allow participants to prepare in advance. Interested participants were asked to respond to the email to confirm their willingness to participate.

Once participation was confirmed, the researcher began scheduling interviews via Zoom at times convenient for participants and sent them digital calendar invitations. Participants were also reminded of the importance of submitting their signed consent form prior to the commencement of the interview.

4.2.3. Snowball Sampling

Snowball sampling was employed to recruit additional participants through expert referrals. Following each interview, participants were asked to recommend colleagues or professional contacts who might be suitable and willing to participate. The researcher then contacted these referred individuals using the same recruitment procedure as in the initial stage. This approach facilitated access to specialised professional networks that may not have been readily identifiable through public sources [39]. A total of 3 participants were recruited through this sampling approach. Recruitment continued until an appropriate disciplinary balance was achieved and thematic saturation was reached.

4.3. Data Collection

Semi-structured interviews were selected to provide flexibility in exploring expert perspectives while ensuring consistent coverage of key dimensions of SECAs. Interviews were conducted either synchronously via Zoom ($n = 8$) or asynchronously via email ($n = 10$), depending on participant availability. Zoom interviews were audio-recorded with participants' consent and later transcribed verbatim, whereas email interviews consisted of written responses to the same set of questions. As noted by Hawkins [42] and Meho [43], e-mail-based interviews represent a feasible and effective approach for qualitative data collection, especially when participants have limited availability or when the research aims to describe experiences, as was the case in this study.

The interview guide comprised eight questions addressing core dimensions of SECAs, including user vulnerability, platform characteristics, message and source credibility, prevention strategies, and emerging trends (see Table A1). While the questions were slightly adapted to accommodate participants' disciplinary backgrounds, consistency across interviews was maintained to ensure comparability of responses.

4.4. Data Analysis

Data were analysed using inductive thematic analysis, following Braun and Clarke's six-phase framework [44]. The analytic process began with familiarisation with the dataset, reading the transcripts multiple times to gain a comprehensive understanding (Phase 1). Initial coding was then performed using NVivo 14, a qualitative data analysis software

package, to facilitate the data management and theme development [45]. This process generated 279 initial codes (Phase 2). Initial coding and clustering were conducted collaboratively by the researcher and an academic colleague who was familiar with the research topic and with substantial experience in the area, to enhance intercoder reliability. The researcher subsequently reviewed these codes, merging similar ones and eliminating those that were too general or irrelevant to the main research question and sorted them into clusters to support theme development.

In Phase 3, similarities, connections, and patterns among codes were identified to form overarching themes, resulting in 24 initial themes. A codebook comprising all the codes was exported from NVivo to Excel for further analysis. The researcher used a matrix to organise and categorise codes by their characteristics before developing themes. Phase 4 involved reviewing and refining these themes by examining their relationship to the full dataset and identifying any overlooked data. This process combined smaller related themes, divided larger themes into distinct ones, or eliminated themes lacking sufficient support. The number of themes was reduced from 24 to 10, and after further refinement, to 6 final distinct themes and 7 sub-themes. The final thematic codebook is available as Supplementary Material.

In phase 5, each theme was clearly defined and named to capture its essence and the aspect of the data it represented. Repeated codes and sub-themes were excluded. To assess whether the themes were well-defined, the final thematic structure was discussed with the supervisory team to incorporate their input and suggestions. After the initial themes were developed, the supervisory team was also consulted to review and validate the thematic structure, providing independent feedback on theme clarity, distinctiveness, and relevance to the dataset. Once complete agreement was reached on the clarity and distinctiveness of the themes, the thematic structure was finalised. Phase 6 involved writing the final report.

This process yielded six final themes and seven associated sub-themes, which were organised into three higher-level domains: (a) individual cognitive–emotional factors, (b) social and relational influences, and (c) platform and technological affordances. The final thematic structure was reviewed and validated in consultation with the supervisory team. Figure 5 presents an overview of Braun and Clarke’s six phases for thematic analysis.

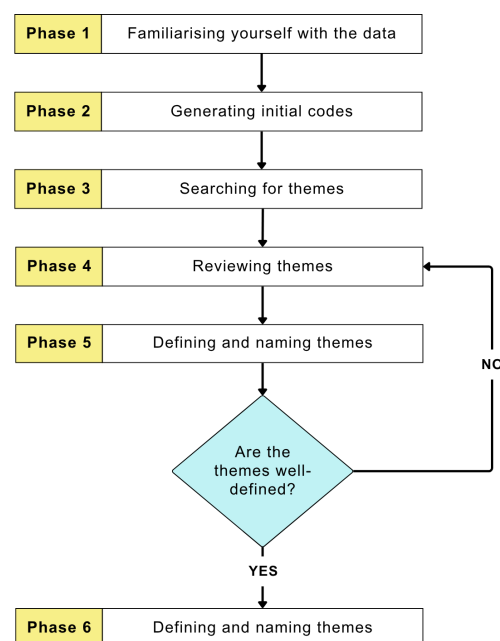


Figure 5. Braun and Clarke’s six-phase framework.

4.5. Ethical Considerations

Ethical approval for this study was obtained from the La Trobe University Human Research Ethics Committee (HEC25333). Participation was voluntary, and informed consent was secured from all participants prior to data collection. Confidentiality was ensured using pseudonyms and the anonymisation of all identifying information. All data were stored securely on La Trobe University's Research DataSpace [46], with access restricted to the researcher and the principal supervisor.

5. Findings and Discussion

This study delves into the insights gleaned from the collected data to clarify the factors and challenges that contribute to SECAs on SNSs. A thematic analysis of the dataset yielded six overarching themes and seven sub-themes, which were developed from the coded narratives provided by the participating experts. Sub-themes were identified through close attention to the contextual patterns within the data (see Table A2). The themes and sub-themes were subsequently grouped into three high-level domains reflecting key dimensions of user susceptibility: (a) the individual-level characteristics, (b) social influences, and (c) platform-level factors (see Figure 6). Together, they capture experts' insights and perspectives on the multifaceted elements underpinning users' vulnerability to SECAs. Table 4 presents an overview of the domains, themes and sub-themes that emerged from this analysis. Each theme represents a recurring pattern within the dataset and is explored in greater depth in the following section.

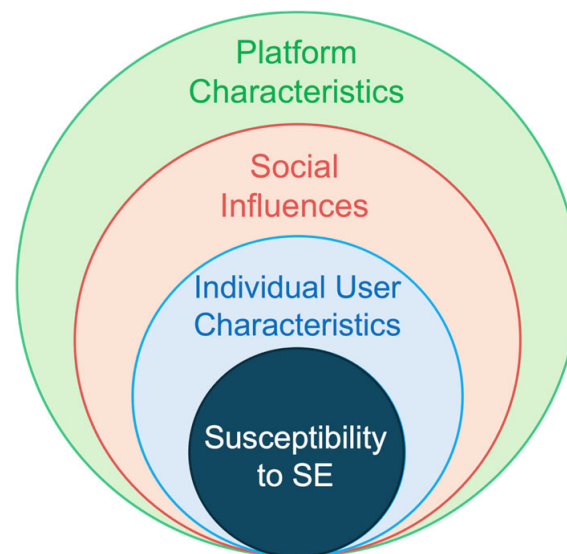


Figure 6. The three high-level domains.

Figure 7 illustrates the themes and associated codes generated in NVivo, showing both the number of participants who contributed to each code (sources) and the number of statements linked to that code (references). The source count reflects how many experts addressed a given concept, whereas the reference count captures the total number of coded excerpts provided. In some instances, a single expert contributed multiple references to the same code.

Table 4. Domains, themes and sub-themes developed from this study.

Domains	Themes	Sub-Themes
Individual cognitive–emotional factors	Cognitive–emotional readiness and vulnerability	Risk awareness and psychological readiness
		Cognitive and emotional processing of content
Social and relational influences	Trust judgement and source credibility in SNS environments	Situational emotional and cognitive vulnerability
		Trust formation and management
Platform and technological affordances	Individual dispositions and social motivations	Source identity and credibility cues
		Trust formation and management
Platform and technological affordances	Platform design and algorithmic amplification of exposure	Source identity and credibility cues
		Trust formation and management
Platform and technological affordances	Experience, habituation, and cyber literacy	Trust formation and management
		Source identity and credibility cues

Name	Files	References	Created by
Domain A — Individual Cognitive–Emotional Factors	34	299	S
Theme 1 — Cognitive–Emotional Readiness and Vulnerability	34	271	S
Sub-theme 1.1 — Risk awareness and psychological readiness	20	44	S
Overconfidence	2	2	S
Oversharing of personal information	15	21	S
Phishing awareness training and education	10	16	S
Potential risks	1	2	S
Psychological awareness and Resilience	2	2	S
Security fatigue	1	1	S
Sub-theme 1.2 — Cognitive and emotional processing of content	31	162	S
Communication style	15	31	S
Content interaction	21	76	S
Emotional language	15	28	S
Message quality	8	13	S
Narrative plausibility	8	9	S
Social proof	5	5	S
Sub-theme 1.3 — Situational emotional and cognitive vulnerability	20	65	S
Anxiety	2	2	S
Blackmail	1	1	S
Cognitive capacity	2	3	S
Curiosity	3	3	S
Digital addiction	1	1	S
Fear	8	9	S
Feeling lonely and isolated	3	3	S
Greed	8	12	S
Habit	3	4	S
Time using SNSs	2	2	S
Urgency or time pressure	8	25	S
Theme 2 — Individual Dispositions and Social Motivations	11	28	S
Agreeableness	1	1	S
Attractiveness	6	7	S
Being rich	2	2	S

Figure 7. An example of codes generated in NVivo.

Table 5 illustrates how our findings align with and extend existing research. First, consolidated support is evident across most elements of the framework. Specifically, key aspects of user susceptibility, such as trust, risk awareness, and social motivation, are well established in the literature and consistently corroborated by our expert interviews. Second, extended support emerges in aspects with relatively limited prior research. In particular, existing studies have partially examined how a user’s technical skills and emotional states

can contribute to their vulnerability to SECAs, whereas our findings provide additional insight and empirical depth. Finally, the most notable highlight in the table is the novel empirical support for Theme 5 (Platform Design and Algorithms). Although platform-level features have previously been discussed primarily at a conceptual level, our study offers concrete empirical evidence demonstrating how these features interact with other factors to shape user vulnerability.

The comprehensive literature review established an initial understanding of the diverse factors influencing user susceptibility to SECAs, but it also revealed inconsistencies across studies. Insights from expert interviews provided crucial interpretive depth, clarifying these inconsistencies and extending current models by highlighting contextual, emotional, and platform-specific nuances. These findings contribute to a holistic susceptibility framework that integrates theoretical and empirical perspectives.

Table 5. Integrated thematic synthesis of literature review and interview findings on SNS phishing susceptibility factors.

Themes	Sub-Themes	Literature Support	Interview Findings	Overall Assessment
Cognitive–emotional readiness and vulnerability	Risk awareness and psychological readiness	Strong support [11,15,18,21,47,48]	Validated	Consolidated Support
	Cognitive and emotional processing of content	Strong support [11,13,49,50]	Validated	Consolidated Support
	Situational emotional and cognitive vulnerability	Limited support [21,22,51]	Extended	Extended Support
Individual dispositions and social motivations	-	Strong support [12,13,19–21,37,50,52]	Validated	Consolidated Support
Trust judgement and source credibility in SNS environments	Trust formation and management	Strong support [14,18,23,24,49,50]	Validated	Consolidated Support
	Source identity and credibility cues	Strong support [12–14,24,26,51,52]	Validated	Consolidated Support
Social context, relationships, and structural positioning	-	Strong support [12,16,18,22,24,49–52]	Validated	Consolidated Support
Platform design and algorithmic amplification of exposure	-	Limited conceptual support; no empirical tests identified [31]	Discovered	Novel empirical support
Experience, habituation, and cyber literacy	Experiential learning and habitual SNS engagement	Strong support [18,19,22–25]	Validated	Consolidated Support
	Technical and cyber literacy	Limited support [18,19,23]	Extended	Extended Support

Hierarchy Charts

Graphical representations, including hierarchy charts, are used in the following sections to provide a comprehensive overview of the findings and to visually illustrate the range of perspectives within the data. The use of charts and graphs enhances the clarity and visualisation of qualitative results [45]. Due to space limitations, the discussion focuses on the three most prominent codes within each theme or sub-theme identified by the experts. These codes are supported by illustrative quotations and highlighted in the hierarchy charts presented below. The remaining codes are provided in Table A2 (Appendix A). Further

visualisations are also provided in Appendix A, including a word tree (Figure A1) and a word cloud (Figure A2).

A. Individual Cognitive–Emotional Factors

The first high-level domain, *individual cognitive-emotional factors*, encompasses two themes and three sub-themes that captured key characteristics influencing users' susceptibility to SECAs. Theme 1: cognitive–emotional readiness and vulnerability comprises three sub-themes: Sub-theme 1.1: risk awareness and psychological readiness; Sub-theme 1.2: cognitive and emotional processing of content; and Sub-theme 1.3: situational emotional and cognitive vulnerability. Theme 2: individual dispositions and social motivations highlights the personal traits and motivational drivers that shape user behaviour and contribute to vulnerability. The themes and sub-themes are discussed in detail below.

5.1. Theme 1: Cognitive–Emotional Readiness and Vulnerability

Figure 8 illustrates the codes that informed the development of Theme 1. This theme examines how emotional manipulation and cognitive strain create exploitable conditions that increase users' susceptibility to SECAs on SNSs. Analysis of expert insights reveals three interrelated sub-themes: individuals' cyber risk awareness, their cognitive-emotional processing of online content, and their situational emotional and cognitive vulnerabilities. These elements together shape the extent to which users may be influenced or deceived by social engineering attempts.

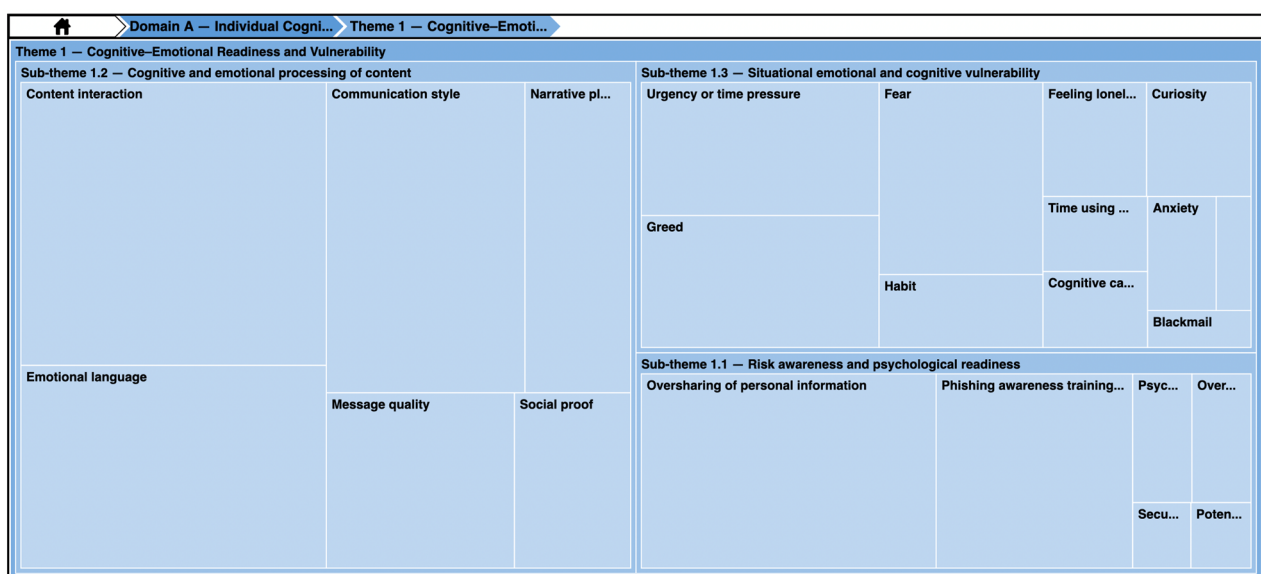


Figure 8. Theme 1 generated codes.

The existing literature reinforces the importance of these dynamics. Austin et al. [53] define emotional manipulation as the ability to influence the emotions and behaviours of others for personal advantage, while Albers [54] describes cognitive strain as a state in which mental demands exceed available cognitive capacity. Consequently, when such emotional and cognitive pressures are present, users' psychological readiness is compromised, making them more vulnerable to exploitation and deceptive online interactions.

5.1.1. Risk Awareness and Psychological Readiness

Risk awareness and psychological readiness refer to users' understanding of potential threats and vulnerabilities, as well as their capacity to recognise, interpret, and respond appropriately to them. This involves not only possessing relevant information and knowledge

but also applying that understanding to make careful, informed decisions that support risk identification and mitigation [55]. This sub-theme underscores the importance of social engineering awareness training and education, perceptions of potential risks, and users' psychological resilience. It also addresses behavioural tendencies such as oversharing of personal information that can inadvertently increase exposure to manipulation. Importantly, the findings suggest that awareness alone may be insufficient, as factors such as overconfidence or security fatigue can erode users' vigilance and compromise their ability to enact effective protective behaviours.

- **Phishing Awareness**

Ten experts highlighted phishing awareness training and education as a critical factor shaping user vulnerability to SECAs on SNSs. They emphasised the importance of equipping users with the knowledge and skills needed to recognise and resist manipulative tactics. As Expert 1 observed, *"Strategies like phishing awareness training, digital literacy programs, and simulated attack exercises help users recognise and resist manipulation."* In contrast, several experts expressed scepticism regarding the effectiveness of current awareness initiatives. Expert 4 cautioned that *"Most of us get cyber security awareness once, maybe twice a year, if we're lucky, but you're likely to fall victim after that,"* highlighting the inadequacy of infrequent or outdated training. Similarly, Expert 10 remarked, *"We need to educate folks. But I honestly don't think education is all that useful,"* underscoring concerns that existing approaches may not keep pace with evolving attack strategies.

These perspectives suggest that infrequent, outdated, or poorly designed awareness programs may have limited impact, ultimately leaving users exposed to sophisticated forms of social engineering. Additionally, several experts stressed the importance of broadening educational efforts beyond individuals to include families and communities to address knowledge gaps among vulnerable groups. As Expert 9 explained, *"We have to educate not just the target population, . . . , but also their family members, multiple generations, within their families, their friends, their trusted neighbours, and the whole community"*.

- **Oversharing of Personal Information**

Fifteen experts emphasised that users are more likely to fall victim to SECAs when they overshare personal or sensitive information on SNS platforms. Several experts, including Expert 1, 9 & 12, noted that SNSs often encourage detailed personal disclosure as part of their design and user-engagement strategies. When users share information such as sufficient birthdays, workplaces, daily routines, or photos of their homes and vehicles, especially those containing identifiable details, threat actors can easily collect, infer and exploit this data to facilitate targeted attacks. Such poor information-sharing practices increase users' exposure to manipulation, as oversharing enables scammers to craft personalised and highly convincing narratives that closely mimic legitimate interactions. One expert explained and cautioned:

"... Especially if they are a constant and repeated poster multiple times a day, you can get an idea whether they are at work or at home. Are they en route to home, or are they going to the kids' soccer game? And so they just give you a profile of who they really are. And these things can really help people become more susceptible to phishing." (Expert 4)

This perspective underscores how behavioural patterns like frequent posting can inadvertently provide attackers with rich contextual insights. This, in turn, increases the likelihood that users will be susceptible to SECAs.

- **Overconfidence**

While several experts emphasised the importance of enhancing user awareness and digital literacy, others, including Expert 6 & Expert 9, observed that some users become

overconfident in their perceived ability to identify cyber threats. This overconfidence can lead individuals to underestimate the sophistication of social engineering tactics and to overlook cues that would otherwise signal potential risk. As a result, highly confident users may let their guard down more readily than those who approach online interactions with greater caution. Expert 6 stated:

“... Overconfidence: Some users believe they can easily identify fraudulent content, which leads them to underestimate risks and overlook subtle manipulation techniques.”

This observation highlights the paradox that increased familiarity with digital environments does not always translate into improved cybersecurity behaviour. In some cases, however, it may increase user vulnerability.

5.1.2. Cognitive and Emotional Processing of Content

Cognitive and emotional processing of content refers to the internal mental and emotional mechanisms through which users evaluate and engage with messages on SNSs. This construct captures the decision-making processes users employ when assessing message content, interaction cues, communication style, message quality, emotional language, and indicators of social proof. Ineffective or superficial assessment of such content can substantially increase users' vulnerability to SECAs.

- **Content Interaction**

Some online platforms may lower users' vigilance toward deception due to the nature of the content they promote. For example, online marketplaces and dating applications often appeal to personal desires, emotional needs, or financial incentives, which can heighten impulsivity and reduce critical judgement. Experts stressed the importance of encouraging users to slow down and think critically before engaging with and responding to potentially deceptive messages. Experts 2 and 18 noted that scams are becoming increasingly sophisticated, particularly when text and imagery are combined, prompting users to respond impulsively rather than carefully evaluating the content. To mitigate this risk, Experts 7 and 10 advised that users cultivate contextual awareness of the types of content typical to each platform and remain attentive to deviations from expected norms. As they explained:

“... You have to be quite, quite lazy in your thinking sometimes just to survive, just navigate the world.” (Expert 7)

“... the big thing to educate folks on is to slow down. Slow down because most social engineering attacks are dependent on you making a snap decision, or will actively encourage you to make a quick decision, and it's just to get people to slow, like, don't respond to the thing immediately.” (Expert 10)

- **Communication Style**

Several experts highlighted that scam attempts frequently reveal themselves through distinctive communication patterns, including overly polite phrasing, emotionally manipulative language, and repetitive message formats. The primary purpose of such messages is to extract sensitive or financial information, often by exploiting users' emotional responses. Experts also highlighted that inconsistencies between the source's claimed identity and their linguistic style, particularly when the communication does not resemble how a genuine user would typically write, serve as important indicators of deception. Expert 15 stated:

“... I'm talking not only about spelling and grammar. I'm talking about the message, style, and content, which really no one normal uses. They're very polite. They always say please, I know what I'm asking is a bit difficult, but could you possibly, and then, you know, that's the crunch for the money.”

- Emotional Language

Scammers often employ emotional manipulation to craft messages that appear compelling and credible, prompting users to respond impulsively. Experts 14 and 15 emphasised the central role of linguistic patterns in this process, noting that attackers often use polite and affectionate language to evoke specific psychological reactions. Such language may appeal to users' emotional, relational, religious, or political identities, leading them to lower their guard. Expert 14 warned:

"... Some words matter in our life, like 'mother,' 'father,' 'daughter,' 'son,' and 'beloved.' Avoid being manipulated by someone who uses such words to psychologically influence you through discourse that reveals your affiliations."

Expert 15 offered a similar observation, grounded in personal experience:

"... Hello, my beautiful friend. Hello, gorgeous. I can't wait to be your friend. Your content is so interesting that I need to talk to you. Let's be friends. The times I have received a message like that with lots of hearts, maybe a rose, it's always been a scam."

These reflections illustrate how emotional language can serve as a subtle yet powerful mechanism through which attackers gain users' trust and initiate manipulation.

5.1.3. Situational Emotional and Cognitive Vulnerability

Situational emotional and cognitive vulnerability refers to the temporary emotional states and cognitive conditions that users experience in specific contexts or during interactions on SNSs. These states, including anxiety, fear, loneliness, curiosity, urgency, or low cognitive capacity, can affect users' decision-making processes and increase their susceptibility to SECAs.

- Urgency or Time Pressure

Six experts emphasised urgency as a key mechanism exploited by cyber attackers to manipulate users. They observed that individuals are particularly vulnerable when pressured to make rapid decisions. Expert 9 stated that *"the immediacy and the urgency effect is a huge, huge red flag."* Such tactics disrupt rational thinking by creating a sense of time scarcity, prompting users to react impulsively rather than critically evaluating the message. Expert 15 further emphasised the need for users to remain alert to linguistic markers designed to impose time pressure, phrases such as "you must", "you have to", and "you need to", which can hinder rational thinking. Similarly, Expert 4 underscored the severity of this strategy, stating that:

"... when you put people under a significant amount of time and pressure, that creates a visceral effect, meaning that they become so absorbed into answering the [message] that they will let their guard down."

- Greed

Experts identified greed as another key emotional factor that increases user susceptibility to cyberattacks. From the attacker's perspective, Experts 2, 14, and 15 noted that social engineers strategically exploit users' aspirations for financial gain or personal advancement by crafting deceptive messages that evoke hope, opportunity, and material desires. Such messages often promise tempting monetary rewards or suggest pathways to romantic or economic stability, encouraging users to reveal sensitive information or engage in fraudulent activities. From the user's perspective, vulnerability arises when financial temptation overrides logical cybersecurity considerations. As Expert 7 observed, *"even people just using LinkedIn, they can still get attacked, and it's the same basic kind of thing is this idea of kind of greed."* This insight highlights how attackers may impersonate recruiters or

potential employers to exploit users' ambitions and desire for success, extracting personal or professional information. These insights underscore that greed, expressed through both hope and opportunity, serves as a powerful motivational trigger that attackers can exploit to increase the effectiveness of SECAs.

- Fear

Experts identified fear as a significant emotional factor that social engineers leverage to manipulate users on SNSs. Attackers design their strategies to induce fear and disrupt users' ability to respond rationally, increasing their susceptibility to victimisation. Expert 1, for example, explained that *"many users lack cyber awareness and don't recognise manipulation tactics like fear used by attackers,"* highlighting how limited awareness can amplify the effectiveness of fear-based techniques. In addition to fear-based manipulation, Expert 7 emphasised the role of the fear of missing out (FOMO) as a related emotional driver that heightens vulnerability. As they remarked, *"people will also have something called a fear of missing out. You know, people feel they have to be part of something, they have to be part of an online conversation."* This desire for social inclusion can prompt users to engage impulsively with misleading or malicious content, thus increasing their risk of falling victim to SECAs.

5.2. Theme 2: Individual Dispositions and Social Motivations

Figure 9 illustrates the codes that informed the development of Theme 2. This theme explains how attackers exploit individuals' personal dispositions and social motivations to gain compliance and manipulate user behaviour on SNSs. When personal characteristics, such as agreeableness, impulsivity, self-control, and tendencies toward compliance, are considered alongside socially driven needs such as attractiveness, wealth, attention, and social approval, important patterns of vulnerability emerge. Within social networking environments, these characteristics shape how users interact online, build relationships, and seek validation or intimacy. Such dispositions can make users more receptive to socially manipulative cues, increasing their susceptibility to SECAs.

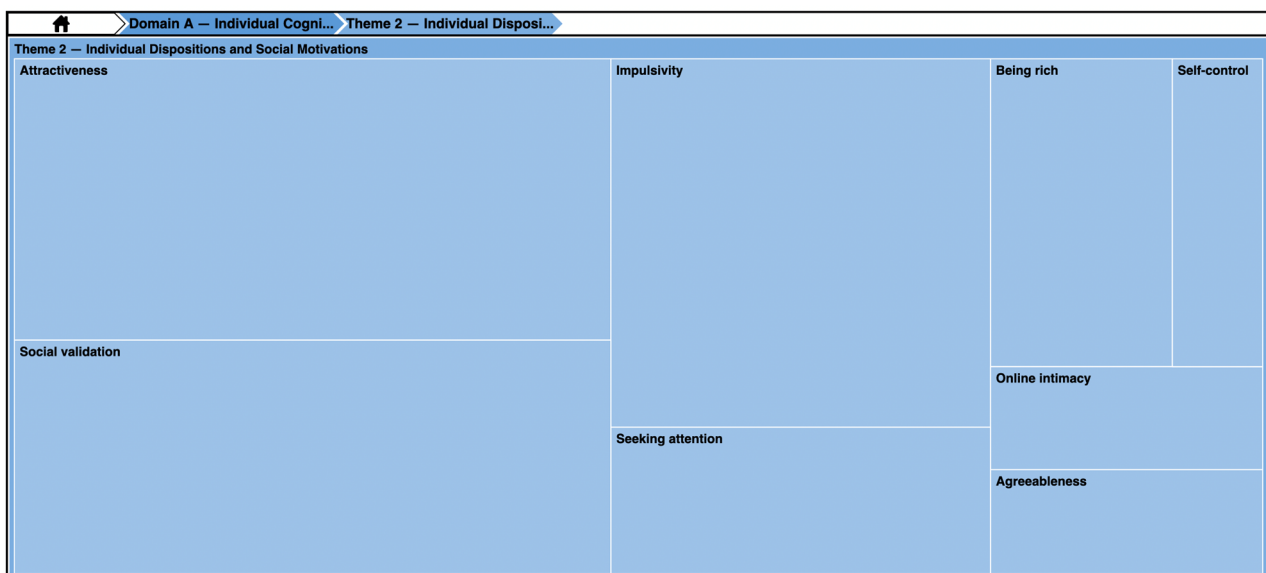


Figure 9. Theme 2 generated codes.

- Attractiveness

Five experts highlighted that user attraction to the opposite sex is a primary factor that social engineers exploit. This form of manipulation operates in two directions. On one side, attackers deliberately target women whom they perceive as less physically attractive,

assuming that they may be more trusting and therefore easier to deceive. As Expert 15 noted:

“... They’re always looking for women... the least attractive, the better. So these people trust and they don’t look for any red flags. So this is the perfect victim.”

On the other side, users themselves become vulnerable when they are drawn to profiles featuring attractive individuals. Images that appeal to relational and emotional desires can reduce scepticism and encourage users to overlook potential warning signs. Expert 10 explained that a strong desire for companionship or romantic connection can impair judgement, stating:

“... some research has probed things like a person’s desire for an ideal partner, like some people are so hell bent on finding love that that’s something that can be exploited.”

These perspectives demonstrate that romantic and sexual attraction can increase user susceptibility to SECAs. By impacting trust, emotional responsiveness, and attentional focus, attractiveness becomes a powerful tool that social engineers exploit to manipulate targets on SNSs.

- Social Validation

Social validation emerged as another factor influencing users’ susceptibility to SECAs. Experts emphasised that the desire for social approval, especially when combined with poor digital hygiene, can significantly amplify users’ exposure to manipulation. Expert 7 emphasised that,

“... people who are looking for social validation might be especially vulnerable to being someone external trying to manipulate them.”

This vulnerability stems from users’ constant efforts to be liked, accepted, or acknowledged within their online networks. In pursuit of such validation, users may engage with unfamiliar individuals, accept random friend requests, or participate in interactions without adequate evaluation. These behaviours, driven by a desire for social connection or affirmation, can increase the likelihood of encountering malicious actors and falling victim to SECAs.

- Impulsivity

Several experts identified impulsivity as a factor that increases users’ vulnerability to SECAs on SNSs. Users who act impulsively are prime targets for manipulation as they often fail to consider the potential consequences of their actions. Experts emphasised that impulsive behaviour reduces users’ ability to exercise critical judgement. To provoke these impulsive responses, social engineers often exploit emotional triggers. Expert 2 explained that:

“... Exploiting religious sentiments or social causes, such as images from conflict zones, can lead users to act impulsively without proper scrutiny.”

Similarly, Expert 7 observed that constant engagement with social media platforms can affect users’ attention spans, making them more prone to react quickly rather than thoughtfully. This tendency toward rapid, unreflective responses can significantly increase susceptibility to deceptive content.

B. Social and Relational Influences

The second high-level domain, *social and relational influences*, comprises two themes and two sub-themes that capture the broader social influences shaping user susceptibility to SECAs. Theme 3: trust, judgement, and source credibility in SNSs includes two sub-themes: Sub-theme 3.1: trust formation and management; and Sub-theme 3.2: source identity and

credibility cues. Theme 4: social context, relationships, and structural positioning focuses on demographic characteristics and social positioning, as well as their roles in susceptibility to SECAs.

5.3. Theme 3: Trust Judgement and Source Credibility in SNS Environments

Figure 10 visualises the codes that contributed to the development of Theme 3. This theme examines how SNS-specific trust heuristics and credibility cues are exploited by attackers to bypass users' scepticism and facilitate deception. It encompasses both the processes through which trust is formed, maintained, and managed (Sub-theme 3.1) and the cues individuals rely upon when assessing the legitimacy of a source (Sub-theme 3.2). These cues, such as profile characteristics, interaction patterns, and shared contacts, play a central role in shaping users' judgements of trustworthiness within SNS environments.

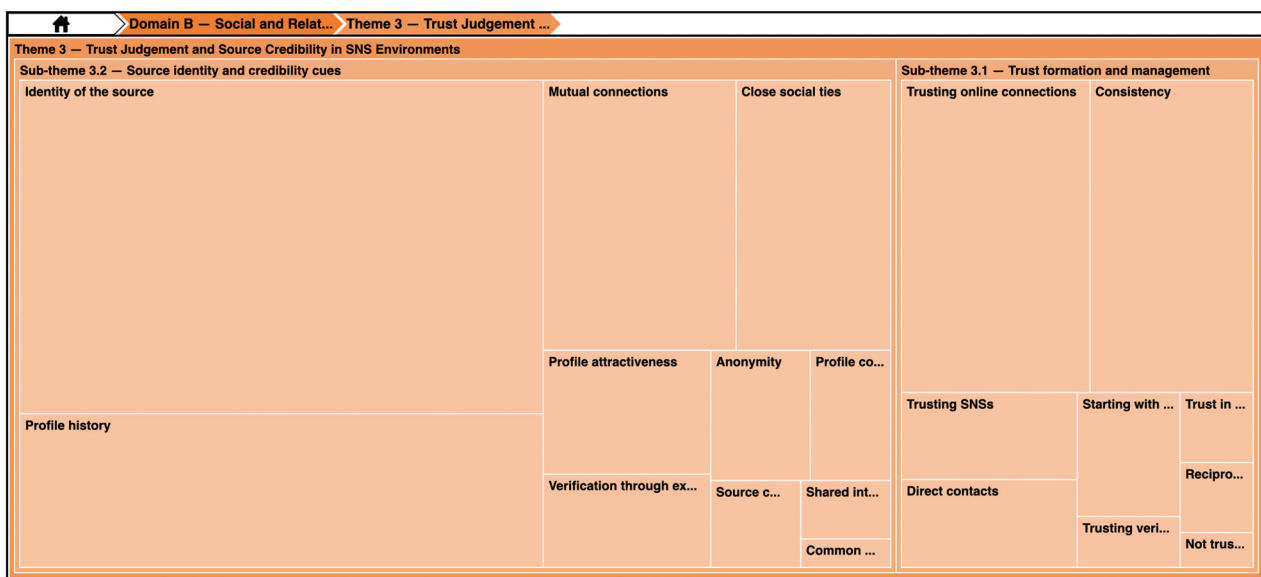


Figure 10. Theme 3 generated codes.

5.3.1. Trust Formation and Management

The sub-theme of *trust formation and management* refers to the ongoing processes through which users develop and sustain trust in other individuals or technologies within SNSs. Trust typically begins at a minimal or neutral level and evolves gradually as users observe behavioural indicators such as consistency, reciprocity, and direct interactions. This sub-theme highlights the cues users rely on, such as consistent behaviour, reciprocal engagement, direct contact, verification markers, and perceptions of technological reliability, to assess and maintain trust.

Trusting Online Connections

Twelve experts emphasised that the trust users place in online connections can increase their likelihood of clicking on malicious links or sharing sensitive information. Expert 10 attributed much of this vulnerability to SNS platform design, stating:

“... So another big issue, and I’m always harping on organisational characteristics, is platforms which constantly push interaction and allow for people to build networks of unvetted individuals. That’s going to be a vulnerability.”

Many users assume that online contacts share their values, intentions, or objectives, and they often interpret such connections as genuine relationships. However, this assumption is frequently misplaced, as cybercriminals systematically exploit these perceptions. Expert 5 highlighted the growing role of artificial intelligence in this context, explaining:

“... Another issue is that users tend to trust online interactions; they are likely to click on links from people they ‘know’. This is further complicated by genAI, making fraudulent schemes more believable, i.e., more difficult to recognise as such.”

Experts 6 & 17 also underscored that users should avoid extending trust to individuals they have not met in person or who have not been verified by a trusted intermediary. This insight reinforces the notion that digital connections are not inherently trustworthy, despite their apparent familiarity and authenticity, and may constitute a significant vulnerability for SECAs.

- Trusting SNSs

Six experts highlighted that the perceived reputation of the SNS can strongly influence the degree of trust users place in the individuals they interact with and the messages they receive. According to these, many users blindly trust SNSs, even when privacy settings are weak or inconsistently applied, compromising both their data security and their online interactions. Expert 14 highlighted an important nuance regarding cross-platform trust signals, stating:

“... If individuals have profiles on LinkedIn, ORCID, ResearchGate, Google Scholar, or Scopus, and if they send messages from Facebook and other SNSs while their profiles do not display details on academic forums, they are usually considered less trustworthy.”

Other experts reinforced the idea that users often overestimate the extent to which SNSs protect their interests. Expert 15 summarised this misplaced trust:

“... They trust social network members and providers. They think that Facebook is going to protect them and which perhaps they should, but they don’t.”

- Consistency

Five experts emphasised consistency as a key indicator of the authenticity and credibility of online communications. They explained that users often judge the genuineness of a profile or message by examining cues such as language, tone, imagery, and personal details. In contrast, inconsistencies, such as variations in writing style, vocabulary, or account details, may signal deception or the presence of a fraudulent actor. Expert 10 stated:

“... I’m looking for consistency across the imagery and the text used details”

Similarly, Expert 16 elaborated on the importance of stylistic coherence when assessing legitimacy, noting that:

“... if it’s one person, then you’d expect, you know, a high level of consistency in the style and words being used from message to message.”

5.3.2. Source Identity and Credibility Cues

This sub-theme concerns the profile-based cues on SNSs that users rely upon when assessing the trustworthiness of a source. Such cues include profile completeness, mutual connections, verification status, and other identity-related indicators. When these cues are falsified or manipulated through impersonation or fake profiles, they become exploitable vulnerabilities that can lower users’ vigilance and facilitate SECAs. Furthermore, users often employ heuristics derived from source attributes, such as identity markers, shared interests, posting history, or account creation date, to influence their trust judgements. While these cues can support more informed decision-making, they can also be easily imitated or fabricated by malicious attackers. Thus, users should take precautions when evaluating unfamiliar profiles, recognising that apparent authenticity on SNSs does not necessarily correspond to genuine identity or credibility.

- Identity of the Source

Nine experts emphasised that the identity of the source is a critical factor influencing user susceptibility to SECAs on SNSs. Users often fail to verify the authenticity of individuals or accounts they interact with, leaving them vulnerable to deception. Expert 10 advised, users should always ask themselves:

“... Is this a person who reasonably credibly is who they claim to be?”

This observation underscores the importance of critically evaluating online identities rather than accepting them at face value. Vigilance requires examining a profile across multiple SNS platforms, scrutinising inconsistencies, and watching for indicators such as unofficial email domains, unfamiliar links, or limited account histories. Attackers are further supported by the ease with which SNSs allow the creation of multiple or fabricated accounts, enabling them to impersonate various identities and target users more effectively. Expert 15 highlighted this issue, stating:

“... It’s very easy to fabricate a false identity on Facebook. So, people, what they have to do is they have to become very sensitive to judging profiles.”

Consequently, these insights indicate that a lack of identity verification remains one of the most significant enablers of successful SECAs, reinforcing the need for users to adopt more rigorous evaluative practices when interacting with unknown or unverified profiles online.

- Profile History

Eleven experts stressed that users should carefully evaluate a profile’s history and related cues when assessing its trustworthiness. They recommended examining how long the profile has existed, how frequently it posts, and whether it includes a reasonable number of photos, connections, and personal details such as educational background, relationships, or employment history. Newly created accounts with limited or generic content were consistently identified as warning signs, as posting frequency and the presence of authentic details often provide insight into a profile’s legitimacy. Experts noted that fake or suspicious profiles tend to exhibit limited activity and sparse content. Expert 5 advised: *“... check history of the profile. Be cautious with new profiles.”* Expert 15 further elaborated:

“... When was the profile created? ... If you look at a profile, they’ve got no friends, no school, no relationships, nothing. Well, obviously, it’s fake.”

Several experts also noted that the quality of a profile’s interactions, the consistency of posting behaviour, and the timing of recent activity serve as additional indicators of credibility. Overall, the experts argued that a thorough evaluation of the profile history is vital in reducing users’ susceptibility to SECAs.

- Mutual Connections

Mutual connections was identified by eleven experts as an important, though imperfect, indicator of a source’s authenticity on SNSs. These shared connections strongly influence users’ perceptions of trust and serve as a common heuristic for assessing the credibility of profiles and messages. Users often evaluate trustworthiness by examining overlapping social networks, shared acquaintances, or social proximity, such as common hometowns or institutional affiliations, which can create an impression of familiarity and reliability. However, several experts cautioned that while mutual connections can be influential, they should not be regarded as definitive evidence of authenticity. Malicious actors can easily exploit this heuristic by infiltrating social networks or connecting with users’ acquaintances to manufacture a false sense of legitimacy. Experts 9 noted:

“... To judge the message credibility, I look ... whether we have mutual connections, although that’s not convincing, even if we have mutual connections, I’m not convinced that the person is not a scammer.”

Similarly, Expert 12 warned:

“... Trust should not be based solely on mutual friends, verification through external means before engaging or sharing personal information”

These insights underscore the necessity of critically evaluating mutual connections, regardless of who they are connected to. Failing to do so may increase users’ vulnerability to SECAs by fostering undue trust in deceptive profiles.

5.4. Theme 4: Social Context, Relationships, and Structural Positioning

Figure 11 visualises the codes that contributed to the development of Theme 4. This theme examines how social relationships and network structures on SNSs create contextual pathways of trust that attackers can exploit to render their scams more credible and far-reaching. This theme also considers how factors such as perceived authority, demographic characteristics (e.g., age, education, gender, and socioeconomic background), access to social support, and context-specific opportunities (e.g., event-driven or seasonal scams) shape users’ trust, decision-making processes, and vulnerability. These factors reveal how social conditions facilitate the occurrence of SECAs.

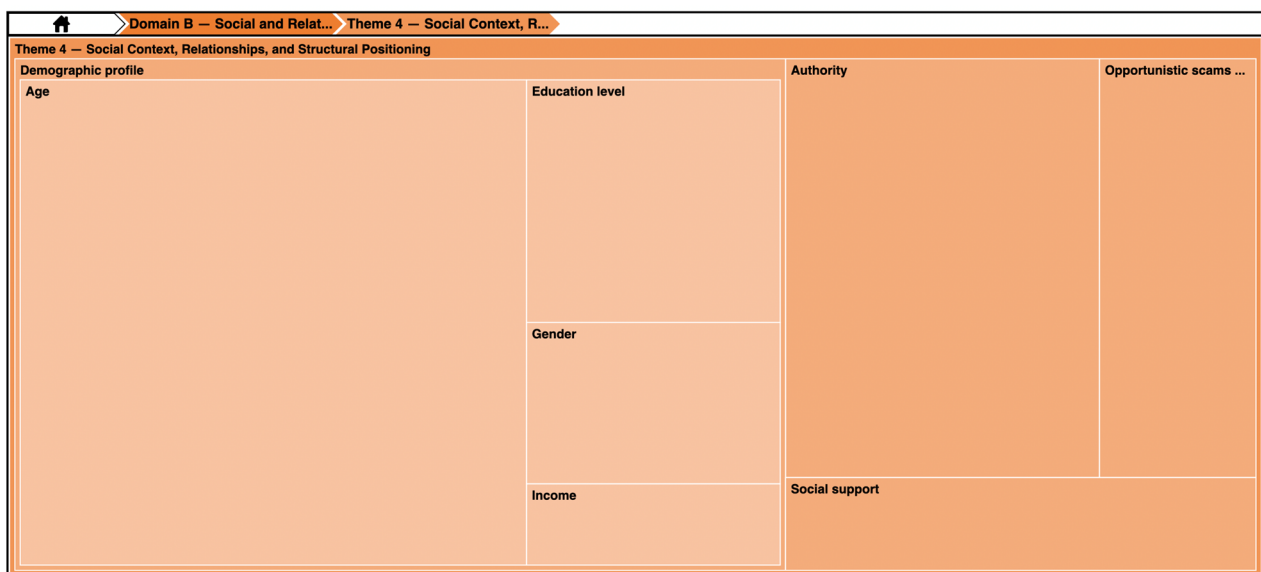


Figure 11. Theme 4 generated codes.

- **Demographic Profile**

Nine experts collectively highlighted how demographic factors such as age, gender, education, and socioeconomic background can influence a user’s susceptibility to SECAs. Several experts agreed that though these factors were generally considered relatively weak predictors when taken in isolation, each nonetheless contributes to vulnerability in distinct ways. Age emerged as the most consistent predictor. Younger users, particularly adolescents, were described as more naïve regarding online risks, while older users, especially those active on platforms such as Facebook, may be less aware of emerging manipulation techniques. As Expert 17 noted:

“... people who are kind of turning 18 now, they’ve had internet their entire lives. It’s going to be interesting to see how do they approach these things as different? I think this is one of the reasons why we look at age as a predictor for susceptibility.”

Education was viewed as another mixed factor. While higher educational attainment may support critical thinking, several experts noted that even well-educated users can fall victim to SECAs if they fail to apply critical evaluation in practice. Expert 6 characterised such individuals as “cognitive misers” prone to accept messages at face value. Gender also appeared relevant. Several experts observed that older women are disproportionately targeted for SECAs. Expert 15 explained this, “They’re always looking for women. . . the older, the better”. Finally, user socioeconomic background may play a role in shaping susceptibility. Users from lower-income groups were described as potentially more trusting of authority figures, making them more vulnerable to manipulation by attackers who strategically adopt authoritative personas.

- Authority

Authority is a commonly exploited element in social engineering, as attackers often craft deceptive messages that invoke or imitate authoritative figures or institutions. Four experts highlighted that user susceptibility to SECAs is strongly influenced by their tendency to comply with perceived authority. Attackers deliberately leverage this inclination by presenting themselves or the content they share as originating from credible, influential, or institutional sources. This strategic use of authority enables social engineers to manipulate user behaviour and gain compliance. Expert 7 observed that this responsiveness to authority may be particularly pronounced within certain cultural contexts, stating:

“... an attacker could use [authority] in some way as part of their social engineering. Authority is really important. It is a very Western culture thing.”

- Opportunistic Scams on Special Occasions

Several experts noted that social engineers often exploit special events or significant occasions to make their scams appear more credible and timely. These opportunistic scams work by aligning deceptive messages with real-world events, personal milestones, or widely relevant societal moments, increasing their perceived legitimacy. Expert 6 provided examples of how such timing is used to increase vulnerability:

“... Also, there are topical scams which occur very soon after a recent government change to tax or benefits (such as the winter fuel allowance). Other scams occur after the end of the tax year to say a tax rebate is approved.”

C. Platform and Technological Affordances

The third high-level domain, *social and relational influences*, comprises two themes and two sub-themes that capture the structural and system-level characteristics of the platforms users engage with. Theme 5: platform design and algorithmic amplification of exposure examines how architectural and algorithmic features shape user experience and influence vulnerability to SECAs. Theme 6: Experience, habituation, and cyber literacy includes two sub-themes: Sub-theme 6.1: Experiential learning and habitual SNS engagement; and Sub-theme 6.2: Technical and cyber literacy, which both consider how users’ accumulated experience, habitual behaviours, and levels of digital competence contribute to their susceptibility or resilience in online environments.

5.5. Theme 5: Platform Design and Algorithmic Amplification of Exposure

Figure 12 visualises the codes that contributed to the development of Theme 5. This theme explains how the structure and algorithms of SNSs influence users’ exposure to SECAs. It considers how elements such as algorithm-driven content sharing, extensive data availability, open or unrestricted messaging systems, and weak privacy or identity verification measures can expand attackers’ reach and impact. These design characteristics

may inadvertently facilitate the spread and effectiveness of SECAs by creating environments in which malicious content is more easily propagated and less readily detected.

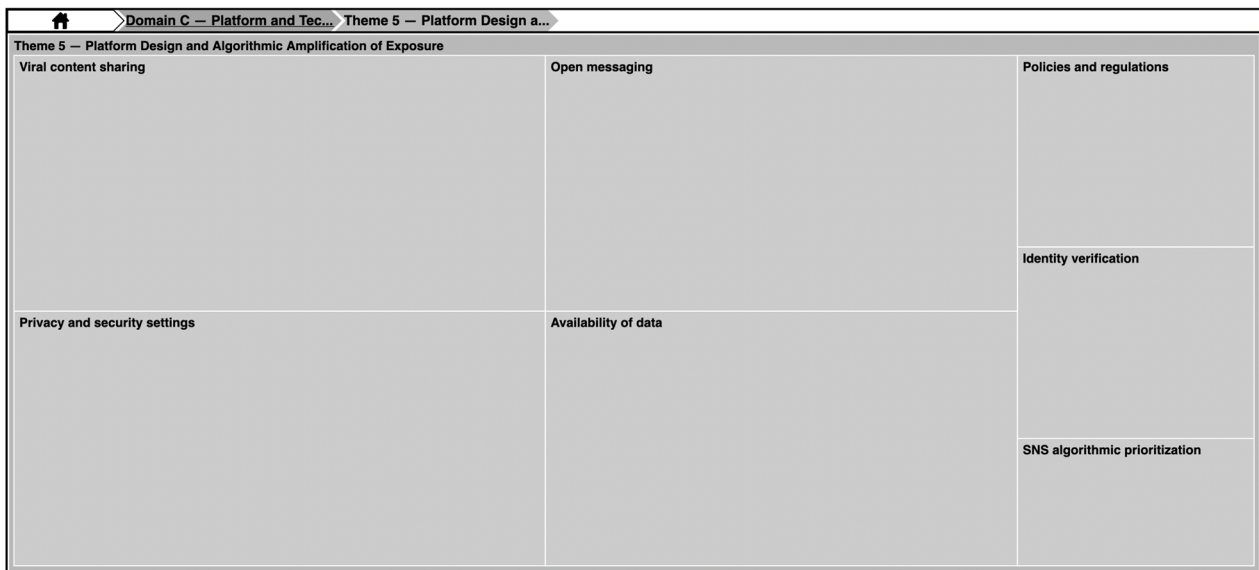


Figure 12. Theme 5 generated codes.

- **Viral Content Sharing**

Eight experts emphasised that cybercriminals target SNSs because of their viral content-sharing features. These features play a central role in users' susceptibility to SECAs by enabling attackers to gather extensive user information and craft highly deceptive, personalised scams. Expert 12 found that platforms such as Facebook and Instagram are particularly vulnerable due to their design and structure, which encourage rapid, often uncritical sharing of personal content. Users on these platforms often disclose detailed personal information and aspects of their daily activities, making it easier for attackers to impersonate them and exploit their social networks. Thus, the viral nature of SNSs, combined with users' tendency to overshare personal information, creates an environment in which attackers harvest personal data and launch targeted attacks. Expert 3 highlighted this point by noting that "... most people don't know about the concept of Footprinting", referring to the process by which social engineers construct detailed profiles of potential victims using publicly available information. Every interaction on SNSs, whether sharing, liking, or reposting, can amplify malicious content. This effect enables deceptive links or fraudulent messages to spread rapidly across user networks. Expert 6 explained:

"... Social media, because it's viral content, so these platforms can promote quick sharing, like likes, shares, retweets, and it can amplify scam links without scrutiny. So, users don't even realise what they do. Oh, this is just an innocent like that I do. But on the other hand, they don't realise that they contribute to the solicitation, to the re-dissemination of scam messages."

- **Privacy and Security Settings**

Privacy and security settings play a crucial role in shaping users' susceptibility to social engineering threats. Several experts emphasised that technical safeguards, such as multi-factor authentication (MFA), two-factor authentication (2FA), and regular password updates, provide essential layers of protection against malicious actors. They also underscored the importance of platform-level mechanisms, including privacy-by-design features, default security settings, and robust identity verification processes, in reducing users' exposure to deceptive tactics. Expert 3 stated: "... the platform security and cross-platform

behaviours are too important.” Furthermore, users can strengthen their resilience by using tools such as browser-based phishing filters and password managers. These perspectives underscore that both platform design and user-driven security practices are important components in mitigating susceptibility to SECAs.

- Availability of Data

Six experts highlighted that the public nature of user profiles on SNSs substantially increases their susceptibility to SECAs. While publicly accessible profiles may offer certain social or professional advantages, they also expose users to heightened privacy and security risks. Expert 8 captured this tension, stating:

“... people exchange ideas and thoughts freely while they are afraid, perhaps to do so for Facebook and Twitter. But that’s what people consider and somehow is true because the data is public, easily available anyway. Easy available.”

5.6. Theme 6: Experience, Habituation, and Cyber Literacy

Figure 13 visualises the codes that contributed to the development of Theme 6. This theme explains how long-term engagement with SNS platforms can produce both protective forms of knowledge and emergent vulnerabilities that attackers may exploit. This theme includes the practices and experiences that shape users’ engagement (Sub-theme 6.1) and how technical competence and cyber literacy can either mitigate or exacerbate susceptibility to SECAs (Sub-theme 6.2).

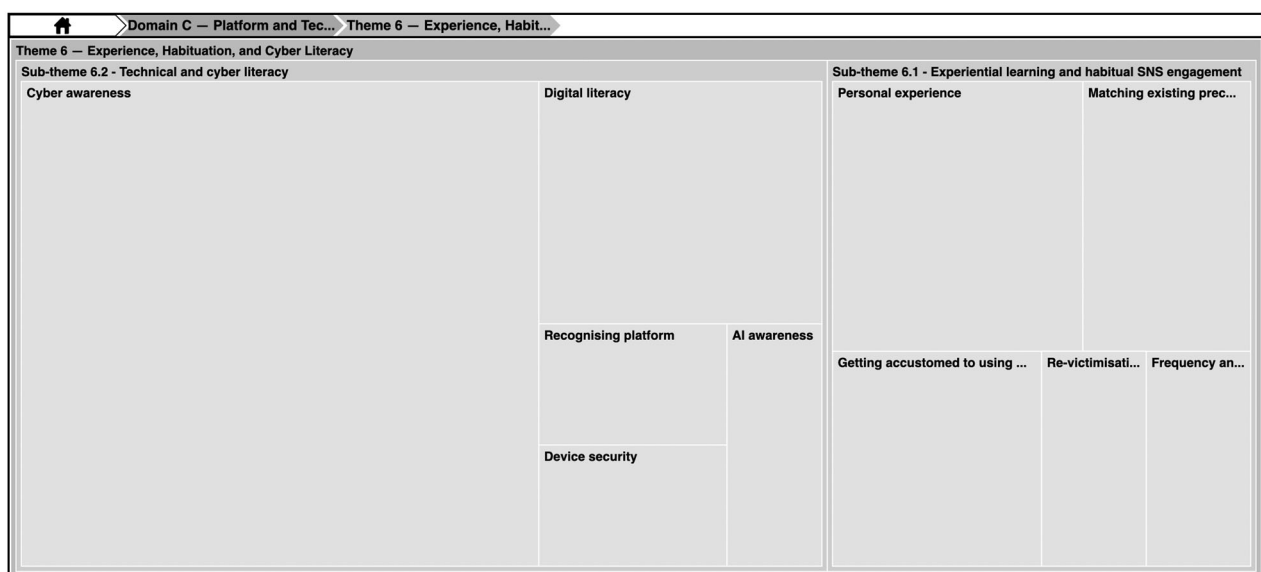


Figure 13. Theme 6 generated codes.

5.6.1. Experiential Learning and Habitual SNS Engagement

The sub-theme explains how users’ routine interactions with SNSs, along with the experiences they accumulate, either directly or indirectly, through their social circles, shape their likelihood of becoming victims or of experiencing re-victimisation. While increased familiarity with SNS platforms can provide users with practical knowledge that supports safer online behaviour, it may also lead to complacency. As users become more accustomed to the rhythms and norms of SNS engagement, they may overlook potential risks or fail to recognise subtle indicators of manipulation. Moreover, habitual patterns of use can reinforce assumptions or pre-existing beliefs that influence how individuals interpret online content. When users rely heavily on these assumptions rather than engaging in critical evaluation, their vulnerability to SECAs increases.

- Personal Experience

Several experts highlighted that limited personal experience and a degree of naivety considerably increase users' susceptibility to SECAs. They observed that social engineers frequently target middle-aged and older individuals who may have financial resources but are less familiar with online threats and digital interaction norms. Expert 6 identified a lack of direct experience with online interactions or prior exposure to scams as a key factor influencing vulnerability. Similarly, Expert 12 noted:

"... The naivety in our interactions (empirically, especially among older and younger persons) leads to increased susceptibility to social engineering-based attacks like romance scams and pig butchering. This issue is also linked to a lack of experience."

- Getting Accustomed to Using SNSs

Experts 4 and 10 emphasised that users' susceptibility to SECAs increases as they become more accustomed to and comfortable with SNSs. With repeated use, familiarity with platform features, interface formats, and interaction norms may reduce users' vigilance, making them less likely to question suspicious requests or messages. Expert 10 explained:

"... If you're talking about SNSs, there are certain things about SNSs in the situations that people find themselves in that can make them vulnerable to social engineering attacks. We're talking about the degree to which a person is comfortable engaging with social media, their familiarity with the format."

- Matching Existing Preconceptions

Experts 2 and 7 highlighted how social engineers exploit users' existing beliefs and expectations. This vulnerability is exacerbated by the design of SNSs, which amplify the risk through targeted tracking and personalised content. By presenting users with information that aligns with their browsing habits or pre-existing viewpoints, SNS algorithms create an environment in which deceptive messages appear familiar, credible, and therefore less likely to be questioned. Social engineers capitalise on this algorithm-driven personalisation by crafting messages that mirror users' preferences or interests, increasing the likelihood of engagement and reducing critical evaluation. Expert 7 explained:

"... You get a thing around confirmation bias, you know, you want to hear things that match your existing preconceptions. So, people are getting those kinds of stories, a social engineer can exploit that."

5.6.2. Technical and Cyber Literacy

Technical and cyber literacy refer to the awareness, knowledge, and practical skills that enable SNS users to navigate platform features effectively and securely. This includes understanding digital technologies, recognising different types of SNSs, identifying cyber threats, including AI-generated manipulation, and managing the security of personal devices. These competencies influence users' vulnerability or resilience to SECAs on SNSs, as higher levels of technical proficiency can enhance protective behaviours, whereas literacy gaps may increase susceptibility.

- Cyber Awareness

Several experts emphasised that a lack of cyber awareness is a major factor contributing to users' susceptibility to SECAs on SNSs. The experts observed that poor digital hygiene and insufficient understanding of common attack tactics, such as deceptive links or fraudulent requests, further increase this vulnerability. One expert explained that users outside computing and cybersecurity fields often lack the foundational knowledge necessary to recognise and appropriately respond to suspicious online behaviours. Expert 3 noted:

"... Based on my research over the past years, I have observed that users outside the computing domain often lack security awareness."

- Digital Literacy

Digital literacy is another important factor influencing users' susceptibility to SECAs on SNSs. Several experts noted that users with limited familiarity with online security practices are less equipped to recognise potential threats, making them prime targets for attackers. Expert 15 highlighted: *"... these people, the perfect victim, are also totally unaware, have a low level of digital literacy..."* Low levels of digital literacy are commonly associated with risky behaviours, such as using weak passwords, neglecting privacy settings, or failing to verify suspicious interactions. These behaviours, in turn, increase vulnerability to manipulation. Expert 1 emphasised the value of educational interventions, noting that digital literacy programs are essential for equipping users with the technical skills and critical awareness needed to recognise and resist social engineering attempts.

- AI Awareness

A lack of user awareness about artificial intelligence (AI) increases vulnerability to social engineering threats. Scammers are increasingly exploiting AI to craft highly convincing scams, from written communications that closely mimic authentic language to sophisticated video interactions that replicate human behaviour. Expert 15 noted that AI-generated content can be remarkably realistic, but it may still display subtle irregularities, such as unnatural eye movements, stating:

"... It even enables them to write better. They can do video chats, believable video chats. To know that they're not real, you have to look at the eyes, the eye movements."

This observation underscores the growing complexity of AI-driven manipulation and highlights the need for greater user awareness to recognise these evolving indicators.

5.7. Practical Implications of the Proposed Framework

The proposed model offers several practical implications. For SNS platform providers, it provides a structured approach to identifying platform features and design elements that may inadvertently facilitate SECAs. For organisations and cybersecurity professionals, the model can support the development of targeted awareness and training initiatives by highlighting the behavioural, social, and platform-related factors that contribute to user susceptibility. The model may also assist policymakers and regulators in evaluating platform governance mechanisms, privacy protections, and user safety measures. Finally, by increasing awareness of the factors that influence user susceptibility, the model can help SNS users make more informed decisions when interacting with content, requests, and recommendations on these platforms.

5.8. Most Vulnerable SNSs

Figure 14 presents experts' perspectives on the SNSs most vulnerable to SECAs. Facebook was identified as the platform with the highest vulnerability ($n = 9$). Experts attributed this vulnerability to several factors, including the platform's encouragement of extensive

personal information sharing, its blend of emotional, social and financial interactions (e.g., marketplaces, business accounts), and its vast user base, which makes it a prime target for impersonation and phishing. And other forms of social engineering. Experts also noted that Facebook facilitates easy user-to-user connections while maintaining relatively weak default privacy controls. Instagram and dating websites emerged as the second most vulnerable SNS platforms ($n = 3$). Like Facebook, Instagram encourages personal disclosure and emotional engagement, creating similar opportunities for manipulation. Conversely, dating platforms place a strong emphasis on emotional and romantic desires, intimacy, and trust-building, thereby increasing users' susceptibility to social engineering by lowering their vigilance. Experts also identified several additional platforms that have become common targets for social engineering, including LinkedIn ($n = 2$), where attackers often exploit professional identity cues and career aspirations. Other potentially vulnerable platforms mentioned by experts include X (formerly Twitter), employment-based websites, the Yahoo search engine, Quora, Gaming sites, WhatsApp, online marketplaces, subscription-based content platforms, and TikTok. Experts' insights highlight that vulnerability is shaped not only by platform design but also by platform purpose, user expectations, and the types of interactions each environment fosters.

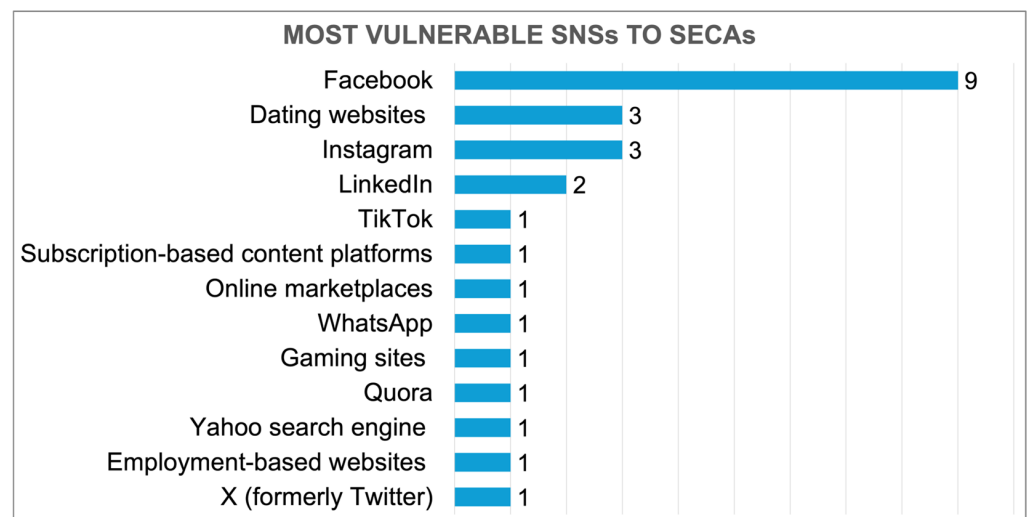


Figure 14. Experts' perspectives on the most vulnerable SNSs.

5.9. Expert Recommendations

Table 6 summarises ten expert-driven recommendations aimed at mitigating the risk of SECAs on SNSs. These recommendations highlight the need for linguistic awareness, enhanced cyber-psychological understanding, stronger security practices, multi-layered defense strategies, and improved policy and technological safeguards.

Table 6. Expert recommendations for mitigating the risk of SECAs on SNSs.

Recommendation	Description
Explore linguistic patterns used in scams	There is a need to work on the linguistic choices and rhetorical patterns that incite or provoke users to access or click on malicious content. Developing linguistic awareness could substantially reduce susceptibility to manipulation.
Investigate the role of cyber psychology in mitigating online threats and vulnerabilities	Experts highlighted a need for greater attention to cyber psychology, particularly regarding platform design and the addictive qualities of SNSs that drive prolonged use. Understanding these behavioural mechanisms can inform more effective preventive strategies.

Table 6. *Cont.*

Recommendation	Description
Ensure device security	Platform-specific design features and device-level security are also missing, yet they play a crucial role in exposure to social engineering. Strengthening baseline device security can reduce overall vulnerability.
Provide users with practical training	There is a need for security awareness training that goes beyond identifying risks and offers concrete, actionable guidance framed positively (i.e., emphasising what users should do rather than only what they should avoid).
Incorporate protective coping mechanisms	There is a need to integrate coping appraisal elements, such as self-efficacy and response efficacy, drawing on Protection Motivation Theory, to enhance users' ability to employ protective measures against social engineering.
Enable real-time profile risk detection	Implementing real-time alerts to notify users when they interact with unfamiliar or potentially risky profiles.
Adopt a multi-layered defense approach	Effective mitigation requires a combination of user education, platform-level safeguards, and robust technical tools, rather than reliance on any single protective measure.
Enhance platform-level security measures	SNS platforms should strengthen their security infrastructures through AI-driven content moderation, automated scam detection, and streamlined reporting mechanisms to identify and block malicious actors more efficiently.
Strengthen policy and regulatory accountability	Experts emphasised the importance of regulatory frameworks that hold SNS platforms accountable for data breaches, misuse, and inadequate security practices.
Advance synthetic identity and deepfake detection research	Experts called for increased research into detecting synthetic identities and deepfakes, given their growing use in sophisticated social engineering schemes.

6. Conclusions

As part of a broader doctoral research project, this study offers valuable insights into user susceptibility to SECAs on SNSs. Semi-structured interviews were conducted with 18 experts from diverse fields, including cybersecurity, psychology, criminology, sociology, and linguistics, to capture perspectives on the factors contributing to user victimisation in online environments.

Using thematic analysis, the study identified six main themes and seven associated sub-themes that explain users' vulnerability to SECAs: (1) cognitive–emotional readiness and vulnerability (comprising risk awareness and psychological readiness, cognitive and emotional processing of content, and situational emotional and cognitive vulnerability); (2) individual dispositions and social motivations; (3) trust judgement and source credibility in SNS environments (covering trust formation and management, and source identity and credibility cues); (4) social context, relationships, and structural positioning; (5) platform design and algorithmic amplification of exposure; and (6) experience, habituation, and cyber literacy (including experiential learning and habitual SNS engagement, and technical and cyber literacy). These themes and sub-themes were integrated into three overarching domains: (a) individual user characteristics, (b) social influences, and (c) platform attributes. The findings provide a robust conceptual framework that encapsulates the key dimensions underlying user susceptibility to SECAs.

This study contributes to the existing body of knowledge on social engineering victimisation by addressing several significant gaps in the literature. While previous studies have primarily focused on specific aspects such as the source characteristics, message characteristics, or user characteristics, they have overlooked the emotional dimensions of user behaviour and the influence of SNS platform-level factors on user susceptibility. Furthermore, inconsistencies across previous findings highlight the need for a unified,

integrated approach to understanding user vulnerability. By developing a holistic, expert-informed framework that integrates individual, social, and technological factors, this study advances a more comprehensive and cohesive understanding of how users become susceptible to SECAs on SNSs. It also contributes an interdisciplinary perspective that bridges technical, psychological, social, criminological, and linguistic insights, which enhances both theoretical development and practical strategies for mitigating social engineering threats in digital environments.

Limitations and Future Work

This study is subject to several limitations that should be acknowledged. First, the framework presented in this study is conceptual, as it draws on expert interview data rather than empirical testing with SNS users. Future research should validate the framework using quantitative methods, such as scenario-based experiments and survey-based analyses, to examine how the identified factors relate to one another and assess their ability to predict users' susceptibility to SECAs on SNSs. For example, researchers could design experimental scenarios that simulate realistic SECAs on SNS platforms and measure how variations in platform features, message characteristics, and user characteristics interact to influence susceptibility.

Second, it primarily focuses on the current determinants of user susceptibility to SECAs within the context of SNSs. While this scope provides valuable insights into patterns of vulnerability on these platforms, it does not extend to other relevant digital environments, such as messaging applications (e.g., WhatsApp, Telegram), online gaming communities (e.g., Discord, Fortnite), or professional networking sites (e.g., LinkedIn), where social engineering techniques are also prevalent. Future research could expand its scope to include these contexts, offering a more comprehensive understanding of how social engineering attempts operate across diverse digital ecosystems. Comparative studies could examine how social engineering techniques differ across platforms and whether the same user susceptibility factors have the same effect.

Third, the use of qualitative methods, particularly semi-structured interviews, introduces a degree of subjectivity. Although this approach yields in-depth, context-rich insights, the findings mainly reflect the perspectives of a specific group of domain experts. Future studies could enhance generalisability and robustness by incorporating a more diverse participant pool and triangulating findings across multiple data sources or methodologies. This could include combining interview data with behavioural observations or experimental data of user interactions with SECAs.

Fourth, despite the researchers' efforts to implement bias mitigation strategies (e.g., triangulation, audit trails), researcher subjectivity may still affect interpretation. Future research could address this limitation by employing mixed-method designs that integrate quantitative validation with qualitative depth. For example, researchers could use survey data to identify broad patterns of user susceptibility and then conduct follow-up interviews to explore the underlying mechanisms.

Fifth, while this study identifies standard demographic variables (e.g., age, gender, education, and socioeconomic background) as factors influencing user susceptibility, it does not capture the deeper influence of diversity factors. Recent literature demonstrates that complex diversity factors significantly shape how individuals process linguistic cues, form trust judgments, and perceive risk in digital environments [56–58]. For example, cultural and linguistic backgrounds can profoundly affect how a user interprets the urgency or authority of a social engineering message. Future studies should examine how such diversity factors influence threat perception and trust dynamics on SNSs.

Finally, the study presents a set of expert-driven recommendations for practice to mitigate user victimisation (see Section 5.9 and Table 6). Future research should apply and empirically test these recommendations to evaluate their effectiveness in reducing users' vulnerability to SECAs on SNSs and other online environments. This includes developing interventions such as linguistic awareness training, cyber psychology-based preventive strategies, platform-level security measures (e.g., real-time risk detection, AI-driven moderation), and multi-layered defence approaches that combine user education with technical safeguards.

Supplementary Materials: The following supporting information can be downloaded at: <https://www.mdpi.com/article/10.3390/fi18070336/s1>, SM1 Codebook: a complete thematic codebook containing code labels, sources, and references.

Author Contributions: Conceptualisation, S.S.A. and B.S.; methodology, S.S.A. and B.S.; software, S.S.A.; validation, S.S.A., B.S. and A.L.; formal analysis, S.S.A. and B.S.; investigation, S.S.A. and B.S.; resources, S.S.A. and B.S.; data curation, S.S.A.; writing—original draft preparation, S.S.A.; writing—review and editing, S.S.A., B.S. and A.L.; visualisation, S.S.A.; Supervision, B.S. and A.L.; project administration, S.S.A., B.S. and A.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: The study was conducted in accordance with the Declaration of Helsinki and approved by the Ethics Committee of La Trobe University (Approval No. HEC25333) on [27 August 2025].

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

SECA Social engineering cyberattacks
SNS Social networking sites

Appendix A. Additional Materials

Table A1. Interview questions used for expert interviews.

Category	Interview Questions
User Vulnerability	Q1: Based on your experience, what makes social media users vulnerable to social engineering cyberattacks (SECAs)?
Discipline-related Perspective	Q2: From the perspective of your discipline or area of expertise, what do you consider the most important factors influencing user susceptibility to SECAs?
Platform-related	Q3: What features or characteristics of SNS platforms do you believe make them more susceptible to SECAs? Are there any specific platforms you consider more vulnerable than others, and if so, why?
Message-related	Q4: How do you assess the credibility of messages received on SNSs?
Source-related	Q5: How do you judge the trustworthiness of people or profiles sending messages on SNSs?

Table A1. Cont.

Category	Interview Questions
Literature Reflection	Q6: I would now like to share with you a list of factors identified in the literature as influencing user vulnerability to SECAs on SNSs. Based on your experience, do any of these factors seem underrepresented, missing, or overemphasised? Are there any you would add or remove, or modify?
Prevention and Mitigation	Q7: What strategies, tools, or interventions do you believe are most effective for preventing or reducing the risk of SECAs on SNSs?
Trends and Future Research	Q8: Have you observed any recent trends in social engineering techniques or user behaviours on SNSs? What areas do you believe deserve more research attention regarding SECAs on SNSs?

Table A2. Themes, sub-themes and key codes derived from the interview data.

Themes	Sub-Themes	Key Codes
Cognitive–emotional readiness and vulnerability	Risk awareness and psychological readiness	Overconfidence Oversharing of personal information Phishing awareness, training and education Potential risks Psychological awareness and resilience Security fatigue
	Cognitive and emotional processing of content	Communication style Content interaction Emotional language Message quality Narrative plausibility Social proof
	Situational emotional and cognitive vulnerability	Anxiety Blackmail Cognitive capacity Curiosity Digital addiction Fear Feeling lonely and isolated Greed Habit Time using SNSs Urgency or time pressure
Individual dispositions and social motivations		Agreeableness Attractiveness Being rich Impulsivity Online intimacy Seeking attention Self-control Social approval Social validation

Table A2. Cont.

Themes	Sub-Themes	Key Codes
Trust judgement and source credibility in SNS environments	Trust formation and management	Consistency Direct contacts Not trusting other users' profiles Reciprocity Starting with zero trust Trust in the technology Trusting online connections Trusting SNSs Trusting verified personal contacts
	Source identity and credibility cues	Anonymity Close social ties Common contacts Creation date Identity of the source Mutual connections Profile attractiveness Profile completeness Profile history Shared interests Source country
Social context, relationships, and structural positioning		Authority Demographic profile (Age, gender, education, socioeconomic background) Opportunistic scams on special occasions Social support
Platform design and algorithmic amplification of exposure		Availability of data Identity verification Open messaging Policies and regulations Privacy and security settings SNS algorithmic prioritisation Viral content sharing
Experience, habituation, and cyber literacy	Experiential learning and habitual SNS engagement	Frequency and duration of social media use Getting accustomed to using SNSs Matching existing preconceptions Personal experience Re-victimisation
	Technical and cyber literacy	AI awareness Cyber awareness Cyber security awareness Device security Digital literacy Password management Recognising platform



Figure A1. Word tree of the term “Social Engineering”.



Figure A2. Word cloud of key terms from the interview data.

References

1. 'The Global Statistics'—The Data Expert. Available online: <https://www.theglobalstatistics.com/> (accessed on 11 January 2026).
2. Boyd, D.M.; Ellison, N.B. Social Network Sites: Definition, History, and Scholarship. *J. Comput.-Mediat. Commun.* **2007**, *13*, 210–230. [\[CrossRef\]](#)
3. Ishaq, M.; Kifayat, K.; Zafar, M. A Survey on Human Factors in Cyberspace: A New Dimension of Privacy Threats. In *2023 International Conference on Communication, Computing and Digital Systems (C-CODE), Islamabad, Pakistan, 17–18 May 2023*; IEEE: New York, NY, USA, 2023; pp. 1–6.
4. Bhattacharya, M.; Roy, S.; Chattopadhyay, S.; Das, A.K.; Shetty, S. A Comprehensive Survey on Online Social Networks Security and Privacy Issues: Threats, Machine Learning-Based Solutions, and Open Challenges. *Secur. Priv.* **2023**, *6*, e275. [\[CrossRef\]](#)
5. Schmitt, M.; Flechais, I. Digital Deception: Generative Artificial Intelligence in Social Engineering and Phishing. *Artif. Intell. Rev.* **2024**, *57*, 324. [\[CrossRef\]](#)
6. Chetioui, K.; Bah, B.; Alami, A.O.; Bahnasse, A. Overview of Social Engineering Attacks on Social Networks. *Procedia Comput. Sci.* **2022**, *198*, 656–661. [\[CrossRef\]](#)
7. Mutluturk, M.; Metin, B. Mapping the Phishing Attacks Research Landscape: A Bibliometric Analysis and Taxonomy. *J. Theor. Appl. Inf. Technol.* **2023**, *101*, 6758–6780.
8. Rege, A.; Williams, K.; Mendlein, A. A Social Engineering Course Project for Undergraduate Students across Multiple Disciplines. In *2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*; IEEE: New York, NY, USA, 2019; pp. 1–8.
9. Wang, Z.; Zhu, H.; Sun, L. Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods. *IEEE Access* **2021**, *9*, 11895–11910. [\[CrossRef\]](#)
10. Mason, M. Sample Size and Saturation in PhD Studies Using Qualitative Interviews. In *Forum: Qualitative Social Research*; Freie Universität Berlin: Berlin, Germany, 2010; Volume 11.
11. Li, T.; Song, C.; Pang, Q. Defending against Social Engineering Attacks: A Security Pattern-based Analysis Framework. *IET Inf. Secur.* **2023**, *17*, 703–726. [\[CrossRef\]](#)
12. Algarni, A. What Message Characteristics Make Social Engineering Successful on Facebook: The Role of Central Route, Peripheral Route, and Perceived Risk. *Information* **2019**, *10*, 211. [\[CrossRef\]](#)
13. Algarni, A.; Xu, Y.; Chan, T. An Empirical Study on the Susceptibility to Social Engineering in Social Networking Sites: The Case of Facebook. *Eur. J. Inf. Syst.* **2017**, *26*, 661–687. [\[CrossRef\]](#)
14. Alturki, A.; Alsanad, A.; Alhathal, S. Source Credibility in Twitter. *Int. J. Comput. Sci. Netw. Secur.* **2022**, *22*, 383–410. [\[CrossRef\]](#)
15. Kano, Y.; Nakajima, T. Trust Factors of Social Engineering Attacks on Social Networking Services. In *2021 IEEE 3rd Global Conference on Life Sciences and Technologies (LifeTech), Kyoto, Japan, 10–12 March 2021*; IEEE: New York, NY, USA, 2021; pp. 25–28.
16. Albladi, S.M.; Weir, G.R.S. User Characteristics That Influence Judgment of Social Engineering Attacks in Social Networks. *Hum.-Centric Comput. Inf. Sci.* **2018**, *8*, 5. [\[CrossRef\]](#)
17. Al-Thani, N.A. Adolescents' and Social Engineering: The Role of Psychometrics Factors in Determining Vulnerability and Designing Interventions. In *2022 9th International Conference on Behavioural and Social Computing (BESC), Matsuyama, Japan, 29–31 October 2022*; IEEE: New York, NY, USA, 2022.
18. Collier, H.; Morton, C.; Alharthi, D.; Kleiner, J. Cultural Influences on Information Security. In *22nd European Conference on Cyber Warfare and Security, Athens, Greece, 22–23 June 2023*; Academic Conferences and Publishing International Limited: Manchester, UK, 2023; Volume 2023-June, pp. 143–150.
19. Wulandari, N.; Adnan, M.S.; Wicaksono, C.B. Are You a Soft Target for Cyber Attack? Drivers of Susceptibility to Social Engineering-Based Cyber Attack (SECA): A Case Study of Mobile Messaging Application. *Hum. Behav. Emerg. Technol.* **2022**, *2022*, 5738969. [\[CrossRef\]](#)
20. Albladi, S.M.; Weir, G.R.S. Personality Traits and Cyber-Attack Victimization: Multiple Mediation Analysis. In *2017 Internet of Things Business Models, Users, and Networks, Copenhagen, Denmark, 23–24 November 2017*; IEEE: New York, NY, USA, 2017; pp. 1–6.
21. Frauenstein, E.D.; Flowerday, S. Susceptibility to Phishing on Social Network Sites: A Personality Information Processing Model. *Comput. Secur.* **2020**, *94*, 101862. [\[CrossRef\]](#) [\[PubMed\]](#)
22. Frauenstein, E.D.; Flowerday, S.; Mishi, S.; Warkentin, M. Unraveling the Behavioral Influence of Social Media on Phishing Susceptibility: A Personality-Habit-Information Processing Model. *Inf. Manag.* **2023**, *60*, 103858. [\[CrossRef\]](#)
23. Kirwan, G.H.; Fullwood, C.; Rooney, B. Risk Factors for Social Networking Site Scam Victimization among Malaysian Students. *Cyberpsychol. Behav. Soc. Netw.* **2018**, *21*, 123–128. [\[CrossRef\]](#) [\[PubMed\]](#)
24. Albladi, S.M.; Weir, G.R.S. Predicting Individuals' Vulnerability to Social Engineering in Social Networks. *Cybersecurity* **2020**, *3*, 7. [\[CrossRef\]](#)
25. Alqarni, Z.; Algarni, A.; Xu, Y. Toward Predicting Susceptibility to Phishing Victimization on Facebook. In *2016 IEEE International Conference on Services Computing (SCC), San Francisco, CA, USA, 27 June–2 July 2016*; IEEE: New York, NY, USA, 2016; pp. 419–426.

26. Collier, H. Including Human Behaviors into IA Training Assessment: A Better Way Forward! In *21st European Conference on Cyber Warfare and Security (ECCWS 2022)*, Chester, UK, 16–17 June 2022; Academic Conferences and Publishing International Limited: Manchester, UK, 2022; Volume 2022-June, pp. 52–59.
27. Vishwanath, A. Diffusion of Deception in Social Media: Social Contagion Effects and Its Antecedents. *Inf. Syst. Front.* **2015**, *17*, 1353–1367. [[CrossRef](#)]
28. Vishwanath, A. Habitual Facebook Use and Its Impact on Getting Deceived on Social Media. *J. Comput.-Mediat. Commun.* **2015**, *20*, 83–98. [[CrossRef](#)]
29. Klütsch, J.; Schwab, J.; Böffel, C.; Zimmermann, V.; Schlittmeier, S.J. Friend or Phisher: How Known Senders and Fear of Missing out Affect Young Adults' Phishing Susceptibility on Social Media. *Humanit. Soc. Sci. Commun.* **2024**, *11*, 1145. [[CrossRef](#)]
30. Kaur, G.; Bonde, U.; Pise, K.L.; Yewale, S.; Agrawal, P.; Shobhane, P.; Maheshwari, S.; Pinjarkar, L.; Gangarde, R. Social Media in the Digital Age: A Comprehensive Review of Impacts, Challenges and Cybercrime. *Eng. Proc.* **2024**, *62*, 6. [[CrossRef](#)]
31. Alotaibi, M.K.N. Employees' Interest in Professional Advancement on LinkedIn Increases Susceptibility to Cyber-Social Engineering: An Empirical Test. In *Human Aspects of Information Security and Assurance*; Clarke, N., Furnell, S., Eds.; IFIP Advances in Information and Communication Technology; Springer International Publishing: Cham, Switzerland, 2020; Volume 593, pp. 85–96, ISBN 978-3-030-57403-1.
32. AlAmeeri, A.A.; AlMourad, M.B. Impact of Social Engineering on Social Media Users. In *2024 International Conference on IT Innovation and Knowledge Discovery (ITIKD)*, Macau, China, 13–15 April 2025; IEEE: New York, NY, USA, 2025; pp. 1–5.
33. Mouncey, E.; Ciobotaru, S. Phishing Scams on Social Media: An Evaluation of Cyber Awareness Education on Impact and Effectiveness. *J. Econ. Criminol.* **2025**, *7*, 100125. [[CrossRef](#)]
34. Blancaflor, E.; Bataller, A.C.; Dulay, J.B.; Leyva, A.M.; Medina, I.J.; Ladera, L.; Abisado, M. Simulating Phishing Attacks via Social Media: Assessing Student Vulnerabilities to Hidden Malicious Links Using Zphisher. In *Proceedings of the 2025 7th World Symposium on Software Engineering, Okayama, Japan, 24–26 October 2025*; ACM: New York, NY, USA, 2025; pp. 189–195.
35. Prasad Panda, S. The Evolution and Defense Against Social Engineering and Phishing Attacks. *IJSR* **2025**, *14*, 397–408. [[CrossRef](#)]
36. Alshammari, S.S.; Soh, B.; Li, A. Understanding Social Engineering Victimization on Social Networking Sites: A Comprehensive Review of Factors Influencing User Susceptibility to Cyber-Attacks. *Information* **2025**, *16*, 153. [[CrossRef](#)]
37. Algarni, A.; Xu, Y.; Chan, T. Measuring Source Credibility of Social Engineering Attackers on Facebook. In *2016 49th Hawaii International Conference on System Sciences (HICSS)*, Koloa, HI, USA, 5–8 January 2016; IEEE: New York, NY, USA, 2016; Volume 2016-March, pp. 3686–3695.
38. Alturki, A.; Alshwihi, N.; Algarni, A. Factors Influencing Players' Susceptibility to Social Engineering in Social Gaming Networks. *IEEE Access* **2020**, *8*, 97383–97391. [[CrossRef](#)]
39. Kvale, S. *InterViews: An Introduction to Qualitative Research Interviewing*; Sage Publications Inc.: Thousand Oaks, CA, USA, 1996; ISBN 978-0-8039-5820-3.
40. Hecker, J.; Kalpokas, N. Recruitment & Sampling for Research Interviews. Available online: <https://atlasti.com/guides/interview-analysis-guide/recruitment-sampling-research-interviews> (accessed on 27 December 2025).
41. Blandford, A.E. Semi-Structured Qualitative Studies. In *The Encyclopedia of Human-Computer Interaction*; Interaction Design Foundation: Aarhus, Denmark, 2013.
42. Guest, G.; Bunce, A.; Johnson, L. How Many Interviews Are Enough? An Experiment with Data Saturation and Variability. *Field Methods* **2006**, *18*, 59–82. [[CrossRef](#)]
43. Hawkins, J. The Practical Utility and Suitability of Email Interviews in Qualitative Research. *Qual. Rep.* **2018**, *23*, 493–501. [[CrossRef](#)]
44. Meho, L.I. E-mail Interviewing in Qualitative Research: A Methodological Discussion. *J. Am. Soc. Inf. Sci.* **2006**, *57*, 1284–1295. [[CrossRef](#)]
45. Braun, V.; Clarke, V. Using Thematic Analysis in Psychology. *Qual. Res. Psychol.* **2006**, *3*, 77–101. [[CrossRef](#)]
46. Zamawe, F.C. The Implication of Using NVivo Software in Qualitative Data Analysis: Evidence-Based Reflections. *Malawi Med. J.* **2015**, *27*, 13–15. [[CrossRef](#)] [[PubMed](#)]
47. Data Storage. Available online: <https://www.latrobe.edu.au/research-infrastructure/digital-research/data/data-storage> (accessed on 17 May 2026).
48. Kyi, L.; Stobert, E. "I Don't Really Give Them Piece of Mind": User Perceptions of Social Engineering Attacks. In *2022 APWG Symposium on Electronic Crime Research (eCrime)*, Boston, MA, USA, 30 November–2 December 2022; IEEE: New York, NY, USA, 2022; pp. 1–13.
49. Parker, H.J.; Flowerday, S.V. Contributing Factors to Increased Susceptibility to Social Media Phishing Attacks. *S. Afr. J. Inf. Manag.* **2020**, *22*, 1–10. [[CrossRef](#)]
50. Muscanell, N.L.; Guadagno, R.E.; Murphy, S. Weapons of Influence Misused: A Social Influence Analysis of Why People Fall Prey to Internet Scams. *Soc. Personal. Psychol. Compass* **2014**, *8*, 388–396. [[CrossRef](#)]

51. Uebelacker, S.; Quiel, S. The Social Engineering Personality Framework. In *2014 Workshop on Socio-Technical Aspects in Security and Trust, Vienna, Austria, 18 June 2014*; IEEE: New York, NY, USA, 2014; pp. 24–30.
52. Fan, W.; Kevin, L.; Rong, R. Social Engineering: IE Based Model of Human Weakness for Attack and Defense Investigations. *Int. J. Comput. Netw. Inf. Secur.* **2017**, *9*, 1–11. [[CrossRef](#)]
53. Algarni, A.; Xu, Y.; Chan, T. Social Engineering in Social Networking Sites: The Art of Impersonation. In *2014 IEEE International Conference on Services Computing, Anchorage, AK, USA, 27 June–2 July 2014*; IEEE: New York, NY, USA, 2014; pp. 797–804.
54. Austin, E.J.; Farrelly, D.; Black, C.; Moore, H. Emotional Intelligence, Machiavellianism and Emotional Manipulation: Does EI Have a Dark Side? *Personal. Individ. Differ.* **2007**, *43*, 179–189. [[CrossRef](#)]
55. Albers, M.J. Cognitive Strain as a Factor in Effective Document Design. In *Proceedings of the 15th Annual International Conference on Computer Documentation, Salt Lake City, UT, USA, 19–22 October 1997*; Association for Computing Machinery: New York, NY, USA, 1997; pp. 1–6.
56. Gibson, S.D. The Case for ‘Risk Awareness’. *Secur. J.* **2003**, *16*, 55–64. [[CrossRef](#)]
57. Thakur, N.; Cui, S.; Khanna, K.; Knieling, V.; Duggal, Y.N.; Shao, M. Investigation of the Gender-Specific Discourse about Online Learning during COVID-19 on Twitter Using Sentiment Analysis, Subjectivity Analysis, and Toxicity Analysis. *Computers* **2023**, *12*, 221. [[CrossRef](#)]
58. Hu, L.; Kearney, M.W. Gendered Tweets: Computational Text Analysis of Gender Differences in Political Discussion on Twitter. *J. Lang. Soc. Psychol.* **2021**, *40*, 482–503.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.