Published by

British Journal of Contemporary Research

BEXFORD PUBLISHING

Human-Centric Factors Influencing Home Users' Susceptibility to Social Engineering Attacks: Synthesising Evidence Through Literature Review and Expert Validation

Original Research Article | Volume 1 | Issue 4 | 2026 | Article Number: 008

Accepted: 17 August 2026 | Published: 10 September 2026 | ISSN: 2979-8582 (Online)

Crossref : 10.67693/BJCR-VUUIQ3YC

Ganiyu Abiodun Salihu[1], Danlami Gabi[2], Hassan Umar Suru[3], Muhammad Garba[4]

[1] Department of Computer Science, Umaru Ali Shinkafi Polytechnic, Sokoto, Nigeria, [2] Department of Computer Science, Faculty of Computing, Univeriti Teknologi Malaysia, Johor Bahru, Malaysia, [3] Department of Computer Science, Abdullahi Fodio University of Science and Technology, Aliero, Nigeria, [4] Department of Computer Science, Abdullahi Fodio University of Science and Technology, Aliero, Nigeria

{{ORCID Line}}

Correspondence: Ganiyu Abiodun Salihu, salihu_ganiyu@yahoo.com

Abstract

Social engineering attacks remain part of the strongest cybersecurity risks facing digital device users because they involve taking advantage of human behavioural weaknesses, as opposed to technical vulnerabilities. While corporate organisations have been benefiting from structured training and well-formulated defence policies, home users are standalone users who navigate digital systems with limited or no guidance, low awareness level and poor security practices. To safeguard digital assets amid the proliferation of dynamically evolving social engineering attack techniques, it is crucial to comprehend home users' susceptible characteristics to cyber-attacks. This study, therefore, explored the human-centric factors that make home users vulnerable to social engineering attacks, using a sequential exploratory research approach. A synthetic literature review of peer-reviewed literature from 2017 to 2025 was conducted, followed by validation by six (6) cybersecurity and human-behaviour experts who formed a focus group. The mixed-method was followed by thematic analysis, which revealed that susceptibility factors are multidimensional and involve interactions among the general domains of broad behavioural factors: "socio-psychological, habitual, perceptual, and socio-emotional". These findings provide a solid foundation that could be employed in developing an enhanced holistic framework to mitigate social engineering attacks among home users.

Keywords: Social Engineering Attacks, Home Users, Human-Centric Cybersecurity, Behavioural Factors, User Susceptibility

1. INTRODUCTION

The deceptive tactics of social engineering, which include manipulation of individuals' behaviours into divulging confidential information, typically via an online platform[1], have continued to evolve as a critical threat to users in cyberspace, exploiting not only technological weaknesses but also human psychology and behaviour to bypass traditional security measures [2]. Apparently, home users are increasingly becoming targets of social engineering attacks [3], and such attacks exploit the propensity of the users to rely on automated security mechanisms that assure a certain level of safety despite the inherent vulnerability associated with their operating environment [4], [5].

Human factors have been identified as the most significant contributors to cyberattacks in the digital ecosystem [6]. Approximately, sixty percent (60%) of all reported breaches were due to human actions or errors, including malicious clicks, errors, social engineering phone calls and the misdelivery of the sensitive data [7].

Notably, scholars have observed that the continual proliferation of cyberattacks and their manifestations have become more sophisticated and are expected to continue in the coming years [7]. Although cyber threats have posed risks to the operation of digital assets across various sectors of society, including business, government, and individuals [8], they are especially pertinent in work-from-home environments, where individuals conduct operations that were initially confined to the corporate environment [2].

Despite the widespread recognition of the problems posed by perceived vulnerabilities, many previous investigations into social engineering have focused primarily on organisational settings, technical defences and staff training programmes with human factors often treated as a secondary factor rather than a primary consideration [9]. However, there is still a significant dearth of knowledge about the specific vulnerabilities and practices to which home users are exposed, as they use less-protected environments with fewer security controls and limited access to professional IT support [10]. The identified gap in knowledge has been hampering the development of tailored interventions for home contexts that address specific risks faced by working remotely from home environments [11]. Therefore, it is desirable to understand the key human behaviours that contribute to users' vulnerabilities in social engineering attacks while attempting to contribute to the enhancement of cybersecurity measures [12].

Therefore, this research aims to identify and validate key human-centric factors that contribute to the susceptibility of home users to social engineering attacks. This helps the research to answer the main question: **"*What are the key human factors that are susceptible to social engineering attacks*?"**

This research article has the following contributions:.

It rigorously extracts and consolidates the critical human-centred susceptibility factors of home-users to social engineering attacks using a synthetic literature review.

It validates the identified factors through the lenses of insights obtained from semi-structured interviews with cybersecurity experts.

It concludes with evidence-based foundation for creation of targeted, human-oriented cybersecurity interventions for home and work-from-home contexts.

Ultimately, the other sections of the paper are organised as follows: Section 2 focuses on the review of related topics on social engineering and human factors, Section 3 discusses the methods employed for conducting the study, Section 4 presents the main results, Section 5 provides discussions on the achieved results while Section 6 deals with identified limitations of the research and the anticipated directions of the research in future and Section 7 provides the concluding part the paper.

2. LITERATURE REVIEW

The techniques of Social Engineering heavily employ the application of deception, manipulation and exploitation of mental biases and emotional appeals to bypass the designed security measures and attack online users [13]. Consequently, a human factor in cybersecurity is the key to the issue since the strongest technical safeguards can be avoided by focusing on human trust and ignorance [14]. It requires being acquainted with human behaviours, motivation and their natural weaknesses that threat agents often use [15].

Consequently, it is encouraged that a proper understanding of the human element is essential in cybersecurity domain, as even the considered robust technical defences can be bypassed by exploiting human trust and ignorance [16]. This calls for adequate understanding of human behaviours, motivations, and inherent vulnerabilities that threat actors frequently exploit in attacking digital users [17].

2.1 Social Engineering Attacks on Home Users

Home-Users make use of different information technologies to connect to cyberspace for different available services on the internet, such as online banking transactions, email services, news, e-commerce, games, surfing the web, voice and video calls, social media, e-learning, file sharing, and other useful services for home users [2]. The wide range of areas in which home digital devices can be used for different platforms in accessing different online services has made cybersecurity in our homes of paramount importance [18].

Social engineering exploits the weakness of human factors [19]. Also, it has been confirmed as a highly result-oriented and successful strategy for cybercriminals because human mistakes and misunderstandings cause 95% of all Cyber Security breaches [20]

However, the current systems significantly protect technology over users, resulting in complex systems that home users struggle with [21], [22], [23]. Indeed, Information Technology (I.T.) is widely used at home and remains a crucial part of modern-day living for home-based users, especially with the increasing proliferation of smart home devices [10].

Moreover, with home devices becoming highly smart and interconnected, online activities are becoming integral parts of human lives (Dawson & Thomson, 2018). The Ordinary users of digital systems are usually not aware of the potential threats associated with the information technology devices they use at home, and do not have adequate knowledge of how to securely manage the smart devices they use without being manipulated through vulnerability factors. They usually encounter difficulties with both network and device security management [25].

2.2 Prevailing Techniques Employed by Attackers in Social Engineering

In the domain of cybersecurity, attacks employing social engineering techniques utilise a range of tactics, with phishing being a prominent example [26]. Social engineering assaults also frequently employ several misleading strategies, such as pretexting, baiting, and tailgating, each manipulating specific facets of human behaviour and cognitive mechanisms [27].

3 METHODOLOGY

This research adopts an exploratory sequential mixed-methods approach to determine human-related issues that affect the vulnerability of home users to social engineering attacks. The integrated method of synthesising literature and interviewing information security experts, followed by thematic analysis, was selected to identify, confirm and narrow down behavioural vulnerability characteristics applicable to non-organisational users.

3.1 Literature Search and Screening Strategy

The first phase of the research technique is conducting a synthetic literature review. The focused search strategy interrogates five databases (Scopus, Web of Science, IEEE Xplore, Google Scholar, and PsycINFO) to locate literature that describes the types of campaigns perpetrated against domestic users and the corresponding knowledge, attitudes, and behaviours that may mitigate risk. Synthetic Literature Review usually assists researchers in interpreting the mass of information collected into an intelligible synthesis and non-conflicting points in the body of research [28]. The Search query: ("social engineering" or "phishing or pretexting") AND ("home users or non- organization users" or "personal devices") AND ("susceptib" or "vulnerab" or "personality traits") AND ("psychology" or "behavio" or "personality traits"), restricted to peer-reviewed articles published between 2017-2024. This is an all-encompassing method that recognises patterns, themes, and gaps in current literature on the vulnerability of home users to social engineering attacks, which delineates such psychological, behavioural, and social characteristics as trust and low awareness. The techniques used to identify recurrent vulnerable factors employed thematic synthesis. The following are the inclusion and exclusion criteria as presented in Table 1.

Table 1: Inclusion and Exclusion Criteria

Category	**Inclusion (Eligible studies)**	**Exclusion (Ineligible studies)**
Publication Type	Peer-reviewed journal articles or conference papers	Non-peer-reviewed (e.g., blogs, theses)
Topical Focus	Human-centric factors (psychological, social, habitual)	Purely technical, no human linkage
Population	Home or general users in non-organizational settings	Organizational-only
Threat Context	Social engineering (e.g., phishing, baiting)	Unrelated security topics

The initial search for relevant articles produced initial studies on cybersecurity threats and human-related vulnerability. After systematically screening and evaluating the adequacy of the studies (using inclusion/exclusion criteria), a group of studies that specifically focuses on home-users and individual factors of susceptibility was selected to be synthesised. After the review, the result produced a consolidated set of vulnerability attributes, which were subsequently refined through the synthesis of overlapping constructs across studies

3.2 Expert Focus Group and Interview

Six (6) cybersecurity experts were purposively sampled to validate and refine the attributes derived from the literature. The selected participants were chosen via professional networks, and referrals from initially contacted participants. Cybersecurity and human behaviour experts offer insights derived from both practical and theoretical expertise, thereby augmenting the acquired dataset. The six (6) participants of the focus group were recruited via professional networks, including LinkedIn and specialised cybersecurity WhatsApp groups, in addition to referrals from initial participants of 30 participants.

The final selection of a focus group of six (6) experts in this study aligns with the recommended 6-8 participants as supported by the research of [29]. The majority of researches indicate that a group of 5 to 10 participants is adequate to achieve a focus group that is as deep in discussion and comprehensive in

thematic coverage [30], [31]. Thus, the relevance and clarity of the identified attributes, their overlapping and completeness were evaluated using semi-structured interview questions. The cybersecurity and human behaviour experts offer insights derived from both practical and theoretical expertise, thereby augmenting the acquired dataset. Table 2 presents the semi-structured questions for the selected experts of the focus group. Table 2 presents questions for the experts while the detailed demographic information is provided in table 3.

Table 2: Questions for the Experts

QUESTIONS	PURPOSE
Are there factors in the selected attributes that should be combined?	To enhance grouping
Is there any factor in the selected attribute that should be split?	To promote the specificity of factors
Do you think any of the factors should be included but omitted?	To have adequate coverage of the factors
Is the grouping under the broad theme adequate?	To check the correctness of the grouping
From your experience, do you think some factors should be removed?	To further refine the identified attributes

Table 3: Demographic Distribution of Focus Group Participants

Expert No	Age	Gender	Education	Years of Experience
Participant 1	45-59	M	Ph.D	13
Participant 2	30-44	M	Ph.D	10
Participant 3	45-59	M	M.Sc	16
Participant 4	15-29	F	M.Sc	4
Participant 5	15-29	F	M.Sc	4
Participant 6	30-49	F	M.Sc	8

3.4 Analysis Method

Data from both the literature review and expert interviews were analysed using thematic analysis following the Braun and Clarke framework [32]. A thematic analysis was employed to analyse and interpret the data due to its recognised flexibility across various epistemological and theoretical perspectives. This approach was chosen for its capacity to uncover emerging themes that can enhance theoretical frameworks and to

strengthen the existing elements of those frameworks [33]. The thematic analysis was also used during the data integration to examine across-study convergence and divergence in the area of social engineering vulnerability of home users. Axial coding (NVivo (social network analysis) and visual mapping of the analysis results were complemented by Atlas.ti to focus on narratives and thematic mapping, display construction, and degree of convergence.

In areas where disparities arose, they were more in regard to the organisation of the attributes as opposed to their significance. Literature tended to introduce more or less similar variables, but the experts were convinced that it would be better to group these features for clarity. Factors conceptually similar were therefore grouped under broad categories. Factors such as privacy awareness, security awareness, and experience with cybercrime were categorized in a perceptual sub-category, and motivation and trust fell under a socio-emotional sub-category.

The insights from both synthetic literature review and the interviews with experts were consolidated to prepare the final emergent themes of the factors of home-user susceptibility,

The procedure employed for the thematic analysis is summarised in Figure 1:

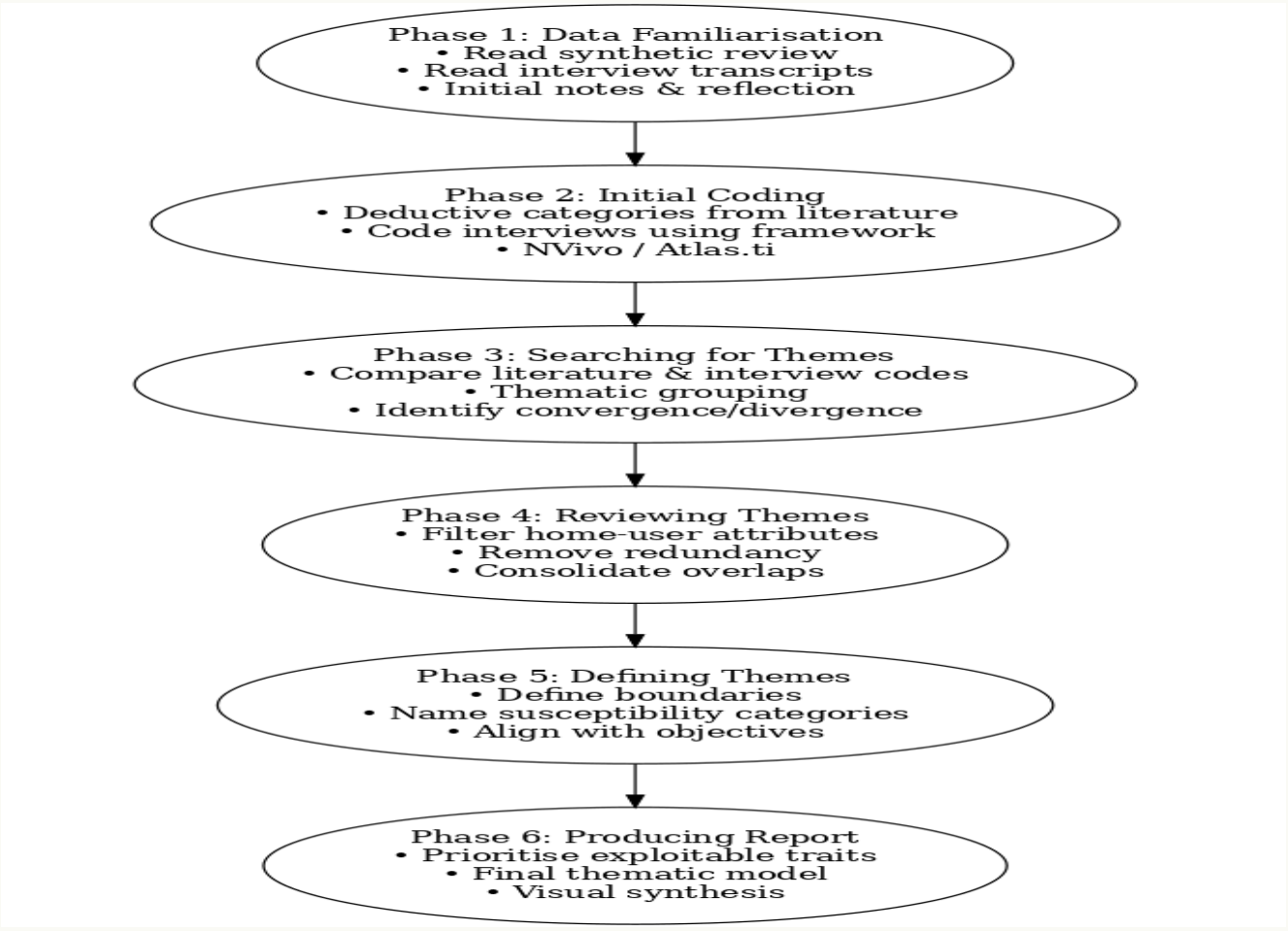

Figure 1: Thematic Analysis Procedure

4. RESULTS

4.1 Synthetic Literature Review Findings

A thematic synthesis of the pertinent factors was carried out on an initially identified set of articles to identify and refine pertinent attributes by synthesising overlapping factors identified (N=94 studies). The thematic synthesis was used in identifying recurring themes and patterns, synthesising overlapping

attributes, refining them for clarity and distinctiveness, and ultimately categorising them into the structured findings to produce normalised attributes presented in Table 4.

Table 4: Identified Attributes from Literature

Attribute (normalised)	**Brief description (indicative)**	**Key supporting source(s)**
Lack of Users Awareness	Users' failure to recognise attacks because of limited security knowledge	Bakhshi (2017); Nahar et al. (2024)
Personality traits	Vulnerability to social engineering is influenced by personality traits.	Albladi & Weir (2018); Albladi & Weir (2017); Nahar (2024)
User demographics	Demographic characteristics relate to susceptibility	Albladi & Weir (2018)
Online habits / online engagement	Online habits and engagement patterns influence exposure/vulnerability	Albladi & Weir (2018)
Communication factors	Socio-technical "risk narrative" factors shape human/organisational risk	McEvoy & Kowalski (2019)
Cognitive factors / thinking ability	Cognitive capacity influences how users process threats	McEvoy & Kowalski (2019); Lee, Gan, & Liew (2023)
Risk perception / threat appraisal	Susceptibility is influenced by psychological evaluation of cyberthreats.	Bada & Nurse (2020); Wulandari, Adnan, & Wicaksono (2022)
Protection motivation / motivation	Motivational drivers shape protective behaviour and susceptibility	Bada & Nurse (2020)
Culture	Cultural background influences perception and response to cyberthreats	Bada & Nurse (2020)
Attacker characteristics	Perceived attacker cues/characteristics affect user judgement and response	Bada & Nurse (2020)
Frequency of attack / exposure	Habitual exposure or repeated attacks relates to susceptibility	Wulandari, Adnan, & Wicaksono (2022)
Experience of attack / victimisation experience	Prior attack experience shapes behaviour and risk response	Wulandari, Adnan, & Wicaksono (2022); Heiman (2022)
Trust tendency	Confidence in other users/providers can increase susceptibility	Albladi & Weir (2017)

Emotional intelligence	Emotional intelligence may protect against cyber-aggression and vulnerability	Rey (2020)
Gratitude	gratitude is associated with emotional intelligence as a protective factor	Rey (2020)
Emotional impact of cyber-victimisation	The outcome of emotional result influence behaviour and vulnerability	Heiman (2022); Nahar et al. (2025)
Online sharing/ disclosure of private information	Personal-information sharing attitudes influence phishing risk	Lee, Gan, & Liew (2023)
Self-efficacy (security-related)	Perceived ability to act securely influences phishing risk and behaviour	Lee, Gan, & Liew (2023)

4.2 Expert Interview Findings

Table 5 shows the agreement and discrepancy between the experts on the initially identified susceptibility factors. The table presents the frequency of validity, refinement, and completeness views of six experts on the susceptibility factors that have been identified based on the synthetic literature review:

Table 5: Responses' Distribution of Experts

Interview Focus Area	Response Option	Number of Experts (n)
Combining related factors	Yes (factors should be simplified/merged)	4
	No	2
Splitting existing factors	Yes (factors should be split further)	1
	No (no splitting required)	5
Inclusion of additional factors	Yes (more factors should be included)	6
	No	0
Adequacy of broad thematic grouping	Adequate	5
	Indifferent	1
Removal of existing factors	Yes (some factors should be removed)	1
	No (all factors are relevant)	5

The relevance of the attributes was largely affirmed by experts (5/6 agreed that groupings were sufficient; 5/6 opposed removal), with minor recommendations to consolidate (4/6) and to add.

The Thematic Analysis showed that thematic factors that were repeatedly highlighted and included as the main causes of home-user vulnerability were the presence of habitual and perceptual factors. A professional, for instance, remarked that "the daily online privacy behaviors of home users, such as sharing or ignoring the pop-ups, expose them to constant exposure, as compared to professional employees" (Participant 3). As another expert says, "A user's general awareness of risks online, through education or even exposure, along with their history of experiences with privacy challenges - whether it's personal victimisation or observing things happening to others - shapes their perceptions about threats in a significant way". These two are interwoven and operate together as a single filtering mechanism for online information.

4.3 Integrated Findings

The literature review revealed a wide range of features associated with the susceptibility of home users, including personality and demographic factors, internet use habits, risk perception, cognitive skills, trust, motivation, self-efficacy, and experience with cybercrime. The relevance of these attributes was substantially validated by the feedback from the experts, and no significant disagreement about including such attributes was expressed. In the literature review and also in the expert interview, habitual factors, i.e. the degree of online presence, frequency of exposure to attacks and sharing of personal information, were found to be determinants of susceptibility. Similarly, perceptual and cognitive variables, such as perceived risk, previous experience with cybercrime, privacy and security awareness, thinking ability, and self-efficacy, were also evident in both sources of data.

After the expert validation and thematic refining, the obtained susceptibility factors were summarised into four general behavioural themes, namely: socio-psychological, habitual, perceptual, and socio-emotional as depicted in Figure 2.

Figure 2: Broad Classification of Susceptible Factors

5. DISCUSSIONS

This research contributes to the existing literature in the domain of social engineering vulnerability of home users by incorporating a synthetic literature review and expert validation into a better thematic framework. Although a significant number of previous studies have tended to consider weakness in the cases of single dimensions, including cognitive impairment, risky behaviour, and absence of awareness, as highlighted in [34]; the results of this paper prove that vulnerability is multi-dimensional. The findings of the research substantiate that vulnerability is multi-dimensional and not an independent attribute.

Consistent with previous research emphasising routine behaviour and exposure as key antecedents of cyber risk, as pointed out in [35], vulnerability has been found to be mostly caused by habitual elements such as online intensive activities, exposure to attacks, and release of personal data, which enhance vulnerability in unchecked home settings where institutional protection is lacking.

The threat detection and response capabilities are moderated by perceptual variables, including risk awareness, cognitive ability, previous experience of cybercrime and self-efficacy, as explained in the previous literature on cyber threats appraisal and critical thinking [36], [37]. The findings of this paper extend the concepts mentioned in the earlier literature by demonstrating how perceptual factors interact with habitual behaviours while amplifying or mitigating susceptibility of home users rather than operating in isolation.

To create conceptual accuracy, factors such as awareness and privacy experience were combined into perceptual factors; trust and motivation were combined into socio-emotional factors; self-efficacy and past victimisation were combined into factors relating to protection.

Substantially, the findings of the paper reinforce consideration of a human-centric perspective that extends beyond purely technical solutions while mitigating social engineering attacks. This is in line with other studies that highlight the importance of addressing social, emotional, and behavioural dimensions of vulnerability to cyber threats [11], [35].

6. LIMITATIONS AND FUTURE DIRECTIONS

Although this study contributes to understanding the home users' vulnerability factors in social engineering attacks through a synthetic literature review and expert validation, it is also imperative to acknowledge some of the following limitations and suggestions for future direction.

The research is mainly theoretical and lacks primary empirical data collected directly from home users. Though the research considers ninety-four (94) studies, the results were validated with interviews of experts in the field of cybersecurity to enrich the theoretical background, the findings still require validation with quantitative techniques. Further research is expected to be carried out to test the empirical validity of the identified attributes, and surveys, experiments, or longitudinal studies may be used to measure the predictive validity of the model.

Another noticeable limitation of the research is the small number of selected participants in the expert review. Although only six (6) individuals who participated are adequate to conduct an exploratory analysis, a higher number of experts would be more beneficial in improving the generalisability and give more contextual and behavioural information about the home-user environment.

Finally, this work provides slightly generalised opinions regarding home users without separating the demographic, cultural, and digital literacy characteristics. The differences between habitual, perceptual, socio-psychological, and socio-emotional domains across different groups of the population should be studied further to help in formulating more effective mitigation strategies.

7. CONCLUSION

The research combines a synthetic literature review with interviews of experts to contribute to the understanding of human-centric factors that make home users susceptible to social engineering attacks. The findings have successfully shown that vulnerability to social engineering attacks is a function of multiple factors, because of the interactions among the various susceptibility factors of habitual, perceptual, socio-psychological, and socio-emotional, rather than a single attribute.

More specifically, factors such as habitual online habits and exposure, along with risk perception, risk awareness, self-efficacy, and trust tendencies of users, are significant determinants of susceptibility to social engineering threats in home environments where formal security protection policies are not well known. However, the study provides a synthetic approach that promotes proper understanding of susceptibility factors, focusing on home users while integrating previously disjointed human-centric attributes into holistic behavioural themes. Therefore, the research emphasises the need to implement cybersecurity interventions, which are not limited to technical protection but consider behavioural, educational, and emotional risk aspects.

Finally, the research has provided a sound base geared towards realising human-oriented countermeasure initiatives that aim at improving resiliency to social engineering attacks in the rapidly changing digital ecosystem in the home environments.

References

R. Almatarneh, M. Aljaidi, A. Alsarhan, S. A. Alshammari, and N. H. Alshammari, "The Rising Tide of Social Engineering: Trends, Impacts, and Multi-Layered Mitigation Strategies," *International Journal of Innovative Research and Scientific Studies*, vol. 8, no. 3, pp. 115–129, 2025, doi: 10.53894/ijirss.v8i3.6443.

M. S. Kamarulzaman, A. J. Toha, and S. Mohamed Shuhidan, "Factors That Influence Information Security Behaviour of Home User," *EDUCATUM Journal of Science, Mathematics and Technology*, vol. 9, no. 2, pp. 129–135, Oct. 2022, doi: 10.37134/ejsmt.vol9.2.14.2022.

S. M. Albladi and G. R. S. Weir, "Predicting individuals' vulnerability to social engineering in social networks," *Cybersecurity*, vol. 3, no. 1, 2020, doi: 10.1186/s42400-020-00047-5.

H. Asker and A. Tamtam, "Knowledge of Information Security Awareness and Practices for Home Users: Case Study in Libya," *European Scientific Journal, ESJ*, vol. 19, no. 15, p. 238, 2023, doi: 10.19044/esj.2023.v19n15p238.

[5]S. Thomson and M. Bewong, "Social Engineering Attacks : A Systemisation of Knowledge on People Against Humans," 2024.

M. Hakimi, A. Fazil, and M. Quchi, "Human factors in cybersecurity: an in depth analysis of user centric studies," *Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)*, vol. 3, no. 01, pp. 20–33, Oct. 2024, doi: 10.58471/esaprom.v3i01.3832.

[7]Verizon, "2025 Data Breach Investigations Report," 2025. doi: https://www.verizon.com/business/resources/T25.

P. Stastny and A.-M. Stoica, "Protecting aviation safety against cybersecurity threats," in *IOP Conference Series: Materials Science and Engineering*, IOP Publishing, 2022, p. 012025. doi: 10.1088/1757-899x/1226/1/012025.

M. R. Arabia-Obedoza, G. Rodriguez, A. Johnston, F. Salahdine, and N. Kaabouch, "Social Engineering Attacks A Reconnaissance Synthesis Analysis," *2020 11th IEEE Annual Ubiquitous Computing, Electronics and Mobile Communication Conference, UEMCON 2020*, pp. 0843–0848, 2020, doi: 10.1109/UEMCON51285.2020.9298100.

S. Piasecki, L. Urquhart, and P. D. McAuley, “Defence against the dark artefacts: Smart home cybercrimes and cybersecurity standards,” *Computer Law and Security Review*, vol. 42, pp. 1–15, 2021, doi: 10.1016/j.clsr.2021.105542.

K. Khadka and A. Barkat, “Human factors in cybersecurity : an interdisciplinary review and framework proposal,” *Int. J. Inf. Secur.*, vol. 24, no. 3, pp. 1–13, 2025, doi: 10.1007/s10207-025-01032-0.

A. A. Moustafa, A. Bello, and A. Maurushat, “The Role of User Behaviour in Improving Cyber Security Management,” *Front. Psychol.*, vol. 12, no. June, pp. 1–9, 2021, doi: 10.3389/fpsyg.2021.561011.

N. Klimburg-Witjes and A. Wentland, “Hacking Humans? Social Engineering and the Construction of the ‘Deficient User’ in Cybersecurity Discourses,” *Sci. Technol. Human Values*, vol. 46, no. 6, pp. 1316–1339, 2021, doi: 10.1177/0162243921992844.

A. Hamoud and E. Aïmeur, “Handling User-Oriented Cyber-Attacks: STRIM, a User-Based Security Training Model,” *Front. Comput. Sci.*, vol. 2, no. September, pp. 1–17, 2020, doi: 10.3389/fcomp.2020.00025.

M. A. Siddiqi, W. Pak, and M. A. Siddiqi, “A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures,” *Applied Sciences (Switzerland)*, vol. 12, no. 12, 2022, doi: 10.3390/app12126042.

A. Hamoud and E. Aïmeur, “Handling User-Oriented Cyber-Attacks: STRIM, a User-Based Security Training Model,” *Front. Comput. Sci.*, vol. 2, no. September, pp. 1–17, 2020, doi: 10.3389/fcomp.2020.00025.

M. A. Siddiqi, W. Pak, and M. A. Siddiqi, “A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures,” *Applied Sciences (Switzerland)*, vol. 12, no. 12, 2022, doi: 10.3390/app12126042.

[18]NSA, “Cybersecurity Information Sheet: Best Practices for Securing Your Home Network,” National Security Agency. Accessed: Mar. 03, 2023. [Online]. Available: https://media.defense.gov/2023/Feb/22/2003165170/-1/-1/0/CSI_BEST_PRACTICS_FOR_SECURING_YOUR_HOME_NETWORK.PDF

S. Parkin and Y. T. Chua, “A cyber-risk framework for coordination of the prevention and preservation of behaviours,” *J. Comput. Secur.*, vol. 30, no. 3, pp. 327–356, 2022, doi: 10.3233/JCS-210047.

A. A. Moustafa, A. Bello, and A. Maurushat, “The Role of User Behaviour in Improving Cyber Security Management,” *Front. Psychol.*, vol. 12, no. June, pp. 1–9, 2021, doi: 10.3389/fpsyg.2021.561011.

Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, “A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions,” *Electronics (Switzerland)*, vol. 12, no. 6, 2023, doi: 10.3390/electronics12061333.

P. Mwiinga, “Investigating the Far-Reaching Consequences of Cybercrime A Case Study on the Impact in Lusaka,” *ResearchGate*, no. July, 2023.

H. Taherdoost, “Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview,” *Electronics (Switzerland)*, vol. 11, no. 14, 2022, doi: 10.3390/electronics11142181.

J. Dawson and R. Thomson, “The future cybersecurity workforce: Going beyond technical skills for successful cyber performance,” *Front. Psychol.*, vol. 9, no. JUN, pp. 1–12, 2018, doi: 10.3389/fpsyg.2018.00744.

S. Heister and K. Yuthas, “How Blockchain and AI Enable Personal Data Privacy and Support Cybersecurity,” *Blockchain Potential in AI*, 2022. doi: 10.5772/intechopen.96999.

R. O. Ogundokun, R. Damaševičius, M. O. Arowolo, and S. Misra, “Phishing Detection in Blockchain Transaction Networks Using Ensemble Learning,” *Telecom*, vol. 4, no. 2, pp. 279–297, 2023, doi: 10.3390/telecom4020017.

U. Maqsood, T. Alsaedi, K. Mahmood, M. Kundi, T. Ali, and S. Ur Rehman, “An Intelligent Framework Based on Deep Learning for SMS and e-mail Spam Detection,” *Applied Computational Intelligence and Soft Computing*, vol. 2023, pp. 1–16, 2023, doi: 10.1155/2023/6648970.

B. R. Schirmer, “Framework for Conducting and Writing a Synthetic Literature Review,” *International Journal of Education*, vol. 10, no. 1, p. 94, 2018, doi: 10.5296/ije.v10i1.12799.

W. Webster and K. Goldstein, “The definitive guide to focus groups,” *qualtrics*, 2023.

W. Burke, A. Stranieri, T. Oseni, and I. Gondal, “The need for cybersecurity self-evaluation in healthcare,” *BMC Med. Inform. Decis. Mak.*, vol. 24, no. 1, pp. 1–15, 2024, doi: 10.1186/s12911-024-02551-x.

A. R. Dikito, M. S. Kaiser, and J. P. Vincent, “Factors Influencing Cybersecurity: A Focus Group Approach,” *International Journal of Academic Research in Progressive Education and Development*, vol. 13, no. 4, pp. 754–767, 2024, doi: 10.6007/ijarped/v13-i4/23539.

V. Braun and V. Clarke, “Thematic Analysis Thematic Analysis , p . 2,” *APA handbook of research methods in psychology*, vol. 2, pp. 57–71, 2012.

M. Naeem, W. Ozuem, K. Howell, and S. Ranfagni, “A Step-by-Step Process of Thematic Analysis to Develop a Conceptual Model in Qualitative Research,” *Int. J. Qual. Methods*, vol. 22, no. October, pp. 1–18, 2023, doi: 10.1177/16094069231205789.

N. Klimburg-Witjes and A. Wentland, “Hacking Humans? Social Engineering and the Construction of the ‘Deficient User’ in Cybersecurity Discourses,” *Sci. Technol. Human Values*, vol. 46, no. 6, pp. 1316–1339, 2021, doi: 10.1177/0162243921992844.

S. S. Alshammari, B. Soh, and A. Li, “Understanding Social Engineering Victimisation on Social Networking Sites: A Comprehensive Review of Factors Influencing User Susceptibility to Cyber-Attacks,” *Information (Switzerland)*, vol. 16, no. 2, 2025, doi: 10.3390/info16020153.

P. van Schaik, D. Jeske, J. Onibokun, L. Coventry, J. Jansen, and P. Kusev, “Risk perceptions of cyber-security and precautionary behaviour,” *Comput. Human Behav.*, vol. 75, pp. 547–559, 2017, doi: 10.1016/j.chb.2017.05.038.

[37]J. Ebuzor, “Understanding Customer Perception of Cyber Attacks,” igi global, 2024, pp. 83–111.