Improved Human-Centric Cyber security Framework for Protecting Home users from Social Engineering Attacks

Ganiyu Abiodun Salihu, Hassan Umar Suru, Danlami Gabi and Muhammad Garba

Department of Computer Science, Abdullahi Fodio University of Science and Technology, Aliero, Kebbi State, Nigeria.
*Corresponding author email: Email: gashaf3@gmail.com, hassansuru@gmail.com, gabsonley@gmail.com, garbamga@gmail.com

Direct Research Journal of Engineering and Information Technology

Vol. 14(1), Pp. 38-49, February 2026,

https://journals.directresearchpublisher.org/index.php/drjeit; https://www.ajol.info/index.php/drjeit

Research Article
ISSN: 2354-4155

Received 5 December 2025, Accepted 10 January 2026, Published 14 February 2026

ABSTRACT

Social engineering attacks remain a major cybersecurity threat, especially among home users who do not have the well-developed security policies typically found in organizations. Despite the fact that current countermeasures are primarily focused on technical defences, there is increasing evidence that the strategies are no longer adequate in the light of attacks that rely on human cognition, emotion, and behaviour. The problem addressed in this study is the inefficiency of existing cybersecurity measures in preventing social engineering attacks against home users, necessitating the development of an improved cybersecurity approach to address gaps identified in the literature. The qualitative research design was chosen and semi-structured interviews with cybersecurity professionals were carried out using the purposive sampling method. Thematic analysis was used to identify existing threats, anticipated future risks, and mitigation strategies. Results indicate that phishing, vishing, and smishing are the most prevalent attack vectors affecting home users, and their sophistication has been increasing due to personalisation, artificial intelligence, and impersonation techniques. Experts argued that technical solutions alone are insufficient; continuous user awareness, behavioural adaptation, and contextual understanding are therefore imperative to improve resilience. The research develops a more human-centred cybersecurity framework that integrates cognitive, behavioural, psychological, and contextual variables with applicable technological controls. The framework does this by positioning home users as stakeholders in the fight against cybersecurity offences and by establishing a culture of adaptive cybersecurity, which provides a less inherently unsustainable means of addressing evolving social engineering challenges. Although the framework remains conceptual and has not yet been empirically validated in a home setting, it provides a systematic basis for further research and for the practice of home-user cybersecurity. It is suggested that future research be conducted to empirically validate the framework in large populations and in new threat situations.

Keywords: *Social engineering; Human-centric Cybersecurity; Home Users; Phishing; Vishing; Smishing; User awareness; Cybersecurity framework; Behavioral Security*

Citation: Salihu, G. A., Suru, H. U., Gabi, D. & Garba, M. (2026). Improved Human-Centric Cyber security Framework for Protecting Home users from Social Engineering Attacks. *Direct Research Journal of Engineering and Information Technology*, 14(1), Pp. 38-49 https://doi.org/10.26765/DRJEIT0633518613

INTRODUCTION

Social engineering attacks are a growing concern across the world (Siddiqi et al., 2022). It engages a series of tactics to manipulate an individual into divulging confidential or restricted information (Zheng et al., 2022). Usually, the attackers exploit people's natural tendency to fear, trust, and a lackadaisical attitude towards information sharing protocols (Moustafa et al., 2021). Most attacks employing social engineering tactics often select their targets based on ease of perceived manipulation to reveal sensitive data (Aslan et al., 2023; Li & Liu, 2021).

As the global trend shifts towards remote work and home connectivity has increased, home users are particularly vulnerable to social engineering attacks because they often lack the knowledge and resources to implement security measures comparable to those of organizations (Michaelides, 2021). With the increasing reliance on computing devices and online services, personal, financial, and confidential information stored on devices without adequate protection becomes an attractive target (Malik et al., 2022). Cybercriminals find individuals easier to manipulate than corporations, and social engineering attacks extend beyond technology to services like telecommunication, banking, and utilities. The present study investigates how social engineering threats targeting home users can be mitigated more effectively (Michaelides, 2021).

Despite the increasing relevance of home-based cybersecurity, there are few studies that focus on exploring the efficacy of a human-centric approach in mitigating attacks on home users (Kolodziej, 2024). However, organizations do invest heavily in securing their assets and educating employees to reduce their attack surface, but the cybersecurity level for home users is not as mature as organizational environments (Singh et al., 2022). Therefore, home users are the most vulnerable to social engineering attacks, which endanger not only home users but also all devices connected to the internet (Asker & Tamtam, 2023).

Therefore, as the complexity and prevalence of social engineering attacks increase, there is a critical need for an improved human-centric cybersecurity approach. However, research indicates that existing cybersecurity methods, which primarily focus on technical defences, are insufficient to counter the strategies employed by social engineers who exploit human psychology to achieve their aims (Hakimi et al., 2024). This necessity is underscored by studies showing that approximately 95% of successful cyber incidents involve human error or manipulation, highlighting the essential role of human factors in cybersecurity (Taherdoost, 2022).

To ensure that the new framework addresses existing gaps and delivers tangible improvements, it is critical to first assess the effectiveness of current cybersecurity frameworks and to develop an improved countermeasures approach informed by the identified gaps. It has been asserted that a human-centric approach is the first line of defence for users against social engineering attacks (Holland, 2020). Consequently, the research questions guiding this investigation are as follows:

i) What strategies have been used or can be employed to mitigate social engineering threats against home users?
ii) How can the social engineering threats against home users be mitigated?

The objective of the study is not only to highlight where the existing frameworks fall short but also to provide valuable insights that inform the design of a more robust solution. The improved framework is designed specifically for home users by integrating reviews of prior frameworks, expert insights, and practical security principles to propose an improved cybersecurity approach in response to the growing threat of social engineering attacks.

LITERATURE REVIEW

The human role in cybersecurity is to create a secure Information Technology (I.T) ecosystem aligned with the values and lifestyles of end users (Hamoud & Aïmeur, 2020). Social engineering actions are implemented to compromise the "weak link" in the chain, which is a secured IT ecosystem where it is possible to implement a variety of security controls to minimize risks faced by the I.T infrastructure (Ambore et al., 2021). In mitigating the effects of cyberattacks, research conducted by (Ofcom, 2014) observes that most internet users are taking one measure or the other to improve cybersecurity. 94% of internet users employed at least one security measure to protect themselves online. The only security measure undertaken by most internet users was the use of strong passwords (68%). The next most common measures were downloading the latest software updates onto devices when prompted (50%), and using security software such as anti-virus or anti-spyware (47%). In view of these, concepts on social engineering attacks and human-centric cybersecurity were reviewed in the following subsections.

Social Engineering Attacks

Social engineering attacks represent cybersecurity threats that exploit of human psychology and behaviour to obtain unauthorized access to confidential information or systems. These attacks focus on manipulating people rather than exploiting technical weaknesses (Al-Otaibi & S Alsuwat, 2020). Interestingly, while technological solutions like anti-phishing software and computational methods have proven effective, hackers continually develop new methods to circumvent these countermeasures. This evolving nature of social engineering attacks highlights the importance of combining technical solutions with human awareness and education. For instance, Albladi & Weir (2018) emphasizes the role of socio-psychological factors

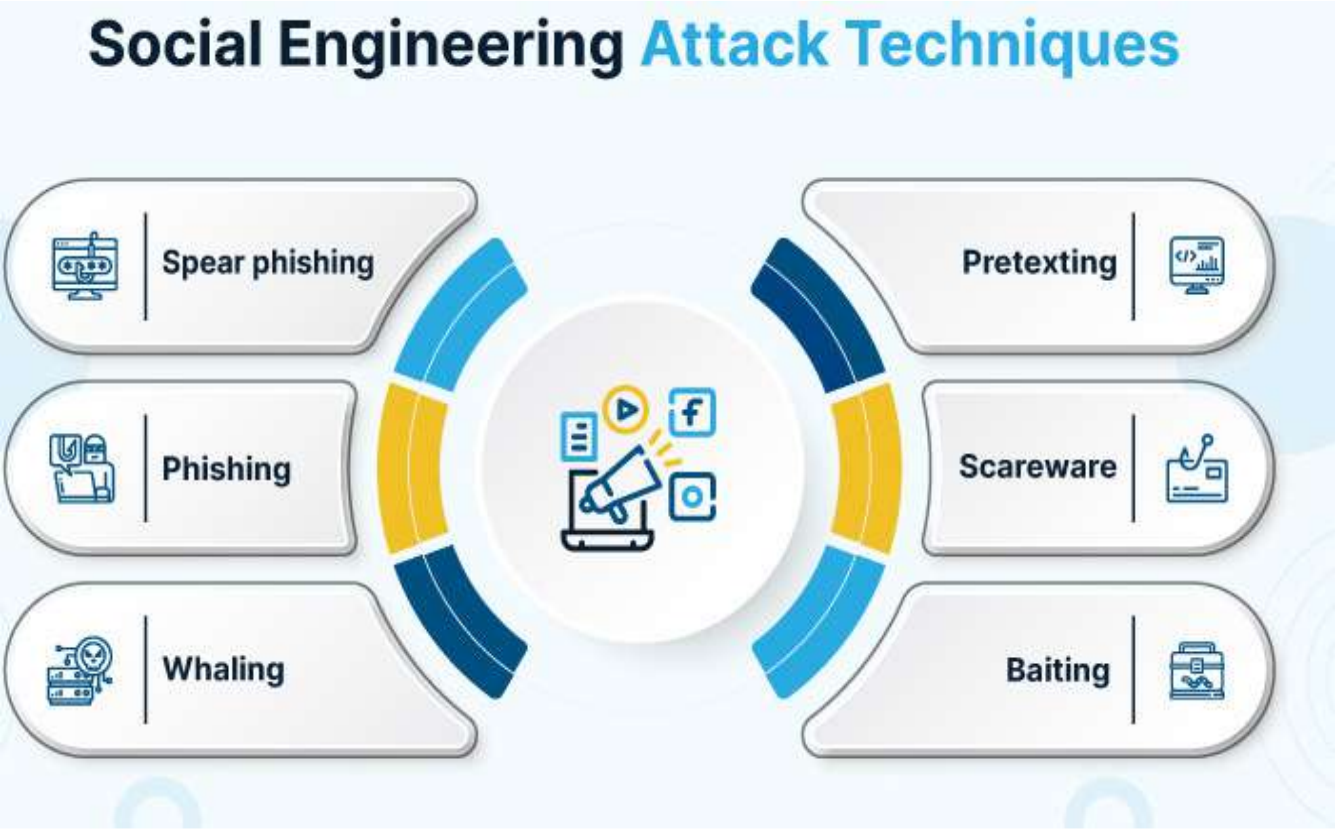

Figure 1: Social Engineering Attack Techniques

in influencing users' cybersecurity behaviours, suggesting that age, gender, and educational level mediate factors affecting their cybersecurity practices. Cyberattacks constitute major concerns in the evolving field of cybersecurity because they make securities of individuals and businesses to be compromised (INTERPOL, 2023). With evolving digital systems and development experienced in the internet ecosystem, the rate of cyberattacks, the nature of attacks, and the range of threats and consequential damages or threats are also on the increase (Aslan et al., 2023). Cybercriminals employ a range of attacks that target individuals, companies, and government institutions, causing severe harm. Cyberattacks are becoming an everyday occurrence for individual users and businesses of all sizes and operations, but little is known about cybercrime on the internet (Bendovschi, 2015). Cybercriminals employ various tactics to undermine the core principles of cybersecurity: confidentiality, integrity, and availability. Cybercrime includes the abilities and techniques utilized by cyberattackers to perpetrate crimes within the internet ecosystem. Cybercrimes serve as the generic category, encompassing various illicit activities, while cyberattacks refer to a specific category of targeted actions and offences against cybersecurity (Brar & Kumar, 2018). Figure 1 presents different techniques of social engineering attacks.

Human-Centric Cybersecurity

This is a technique of cybersecurity that considers the elements of human behaviour and human factors to securely operate a digital system in cyberspace (Young et al., 2018). It entails an understanding of users' preferences, capabilities and weaknesses that dictate the users' behaviour as well as how the factors influence their interaction with the digital system and their associated data. The consideration of human factors provides users better opportunity to discover likely threats before they transform into serious problems (Grobler et al., 2021).

Human centric cyber security as a domain is still evolving and not fully understood (Ystgaard et al., 2023). Recently, the domain is established as an integration of traditional principles of cyber security and those of human-computer interaction, with improved attention on collaborative intelligence, considering humans and technology working together (Grobler et al., 2021). The area of Human-Centric Cybersecurity is showing a socio-cognitive-technical approach to cybersecurity, focusing not only on the roles that human factors play in cybersecurity, but also on developing improved approaches that could lead to an enhanced cybersecurity perspective, with

minimal failure (Young et al., 2018). This contrasts with the common adage that “humans are the weakest link in a technical system” Human-Centric Cybersecurity is a symbiotic relationship where technology and human awareness unite to fortify the digital frontier (Grobler et al. 2021; van Schaik et al., 2017; Zheng et al., 2022). However, the human element possesses unmatched perception, behaviour, and response to problems. Human-Centric Cybersecurity emphasizes the creation of intuitive and user-friendly security interfaces. Complex security measures, if not presented in an understandable manner, can lead to errors and, in some cases, even circumvention by users. By designing interfaces that align with human cognition, cybersecurity measures can emphasize to be seamlessly integrated into daily digital interaction (Sarawagi & Srivastava, 2017).

METHODOLOGY

Building on a review of existing human-centric cybersecurity frameworks, themes were identified in current countermeasures and related factors. Additionally, a qualitative study was conducted to understand experts' perspectives on the use of a human-centric approach to secure home users. This approach allowed for a multifaceted understanding of the evolving threat landscape, particularly concerning the heightened susceptibility of users to psychologically manipulative tactics (Burke et al., 2024). The following subsections provide a detailed process of the methodology.

Research Design

A qualitative study was conducted to understand experts' perspectives on the use of a human-centric approach to secure home users. Data were collected through semi-structured interviews, using a combination of predefined and follow-up questions to explore participants' viewpoints in greater depth. The qualitative method was selected to facilitate a comprehensive examination of subjective insights, experiences, and expert assessments that are not readily quantified, as pointed out in (Pollini et al., 2022). Figure 2 presents the research process.

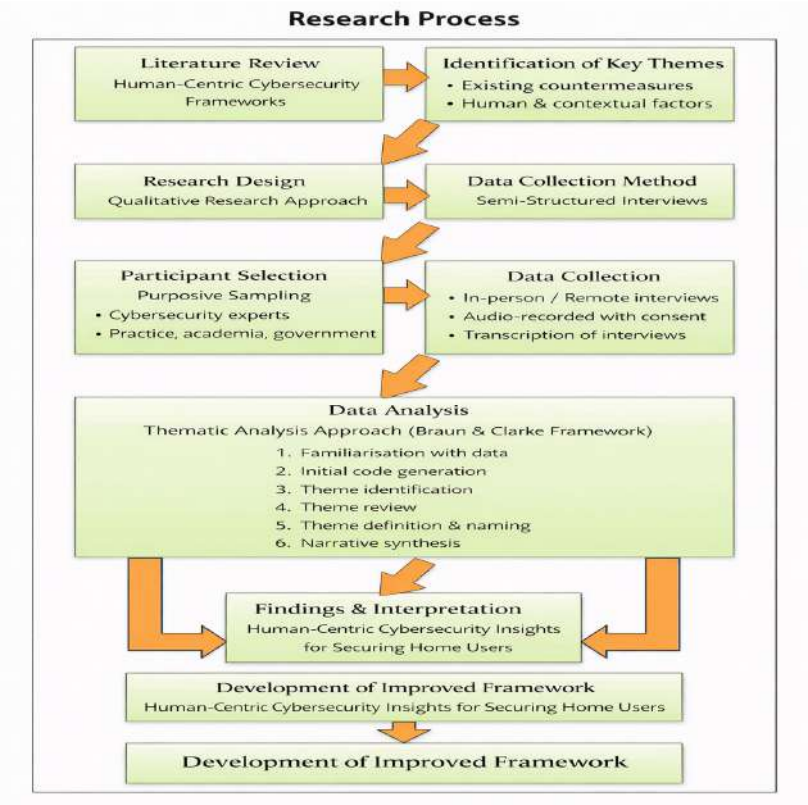

Figure 2: Research Process

Participants Selection

A purposive sampling strategy was employed to ensure the reliability and relevance of the data obtained. The selection criteria sought to identify cybersecurity experts with a distinguished record, including those with recognized experience, certifications, or contributions to cybersecurity practice, education, or policy. A total of 30 specialists were initially solicited in accordance with rigorous selection criteria. Out of the 30 experts approached, 20 agreed to participate fully in the study. This group established a strong and trustworthy basis for

Table 1: Participants' Characteristics.

Expert No	Age	Gender	Education
Expert 1	30-44	M	B.Sc
Expert 2	45-59	M	Ph.D
Expert 3	30-44	F	M.Sc
Expert 4	30-44	F	M.Sc
Expert 5	15-29	M	B. Sc
Expert 6	45-59	M	Ph.D
Expert 7	30-44	M	M. Sc
Expert 8	30-44	M	M.Sc
Expert 9	45-59	M	M.Sc
Expert 10	30-44	F	H.N.D
Expert 11	15-29	F	M.Sc
Expert 12	30-44	M	Ph.D
Expert 13	30-44	M	M.Sc
Expert 14	45-59	M	M.Sc
Expert 15	30-44	M	M. Sc
Expert 16	30-44	M	Ph.D
Expert 17	45-59	F	Ph.D
Expert 18	45-59	M	Ph.D
Expert 19	45-59	M	Ph.D
Expert 20	30-49	F	M.Sc

Table 2: Interview Questions for Experts.

QUESTIONS	PURPOSE
What cybersecurity threats have been prevalent in the last few years, particularly for home users? What impact does social engineering currently have?	To identify the prevailing social engineering impacts on home users
What impact is social engineering expected to have on home users in the near future?	To identify anticipated social engineering impacts on home users
What is the impact of social engineering on home users?	To identify the prevailing social engineering impacts on home users
Can technical solutions alone fully address the social engineering problem for home users? If not, what other approaches are necessary to effectively combat these threats?	To determine the need for a human-centric approach
How crucial is it for home users to be knowledgeable in order to prevent social engineering attacks?	To determine the Importance of user sensitization in mitigating social engineering threats
What role does awareness among home users play in reducing the risk of social engineering attacks?	To ascertain the effectiveness of home users' awareness in mitigating social engineering threats to home users
What user awareness strategies are most effective for home users in defending against cyber threats?	Determination of Strategies
Do you think cybersecurity and social engineering awareness training should be deemed compulsory for home device users? If so, how often should this training be conducted	To determine the Importance of user sensitization in mitigating social engineering threats
Do you have any other specific concerns or suggestions that are related to social engineering and online security awareness that you believe would benefit home users?	To explore conclusion on mitigating the effectsa of social engineering through human-centric approach

qualitative analysis, encompassing a varied array of professional backgrounds, including cybersecurity consultancy, academic research, business security operations, and government cybersecurity positions. The demographic details of the research participants are displayed in (Table 1). Twenty experts, representing diverse ages, genders, levels of education, and years of work experience, comprised the participants. The distribution of participants by educational attainment is shown in Figure 3, and by age in (Figure 4).

Data Collection

Data were collected through semi-structured interviews, enabling participants to articulate their perspectives while addressing essential research themes. Interviews were conducted with a few participants in person and with 17 participants remotely, contingent on participants' availability and location, and were audio recorded with consent for subsequent transcription and analysis. The following questions in (Table 2) were administered to a set of cybersecurity experts to elicit their opinions on the impact of prevailing cyber threats, the perceived roles of social engineering, and the expected solutions. This set of questions is designed to determine whether the current cybersecurity measures are adequate, given prevailing impacts, anticipated threats, and the need to develop an improved framework.

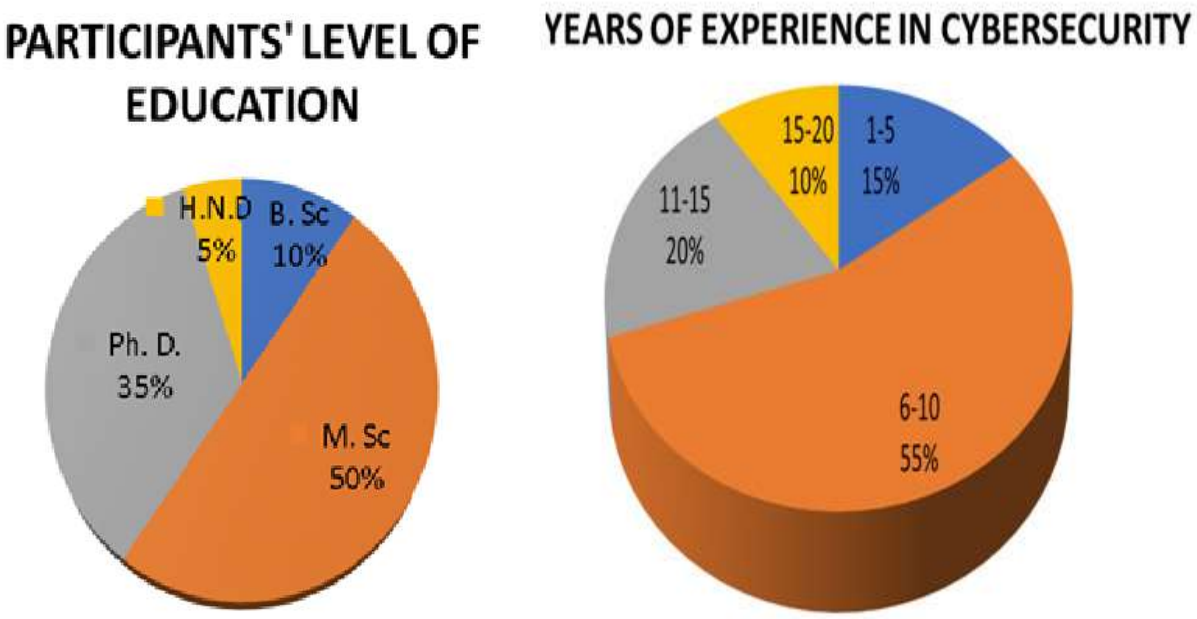

Figure 4: Distribution of participants by Cybersecurity Years of Experience. **Figure 3:** Distribution of participants by Education Level

Analysis Method

The gathered data were analyzed using thematic analysis, a qualitative approach designed to identify, analyze, and interpret patterns of meaning within the data. The analysis adhered to Braun and Clarke's six-phase methodology.

i. Acquaintance with the Data: Transcripts were perused multiple times to guarantee thorough engagement with the information.
ii. Preliminary Code Generation: Principal assertions and concepts were manually coded to represent emergent ideas.
iii. Theme Identification: Associated codes were consolidated to establish first themes.
iv Theme Evaluation: Themes were enhanced by comparative analysis with the dataset to ensure coherence and consistency.
V Themes were distinctly defined and aptly labelled to encapsulate their essence.
Themes were synthesized into a narrative that responds to the study questions.

Development of Improved Framework

The improved human-centric cybersecurity framework was designed by synthesizing the literature review results and themes based on the interviews with experts. An in-depth analysis of current technology-oriented and existing human-centred frameworks was conducted to identify gaps in concepts and practice, particularly in safeguarding home users. The framework was structured around key themes from the thematic analysis, including the most common threats, future risks, constraints on technical controls, and the significance of user awareness. A multidisciplinary strategy has been used, incorporating cognitive, behavioural, psychological, and contextual aspects, as well as practical technological protection, which aligns with the work of (AL-Otaibi & Alsuwat, 2020; Nasir, 2023; Oni et al., 2023). The framework places home users at the centre of cybersecurity defence, thereby facilitating awareness, flexibility, and the longevity of protection.

Ethical Consideration

Ethical permission was secured prior to the commencement of data collection. Participants were informed of the study's objectives, their entitlement to withdraw at any time, and the use of their data. Anonymity and confidentiality were rigorously upheld during the research process. To ensure that the participants were aware of the problem domain and the nature of their expertise, respondents were recruited based on research literature. Home users were selected as the target group to explore the application of a human-centric approach because they constitute the largest and most diverse user group. The data were sufficiently rich and informed the construction of a conceptual framework in the literature. The research question of the proposed study was addressed by professionals who could provide insights into the effectiveness of a human-centric approach in

addressing home users from physical, psychological, and social perspectives.

RESULTS

Thematic and Descriptive methods of analysis were employed in analyzing the qualitative data obtained. Researchers can gain a comprehensive understanding of social engineering vulnerabilities and the effectiveness of defensive measures by integrating thematic and descriptive analytical methods.

Themes Identification

The theme identification focuses on identifying terms in existing social engineering threats, anticipated future threats, and solutions to social engineering attacks. The purpose for the themes identification is to isolate actionable themes that can inform the creation of an improved framework designed not only to prevent attacks but also to empower users with the knowledge and tools needed to mitigate the risks associated with social engineering. Figure 5 categorizes the range of current threats that home users face due to social engineering tactics. The information in the table highlights the theme of several terms associated with the consequences of social engineering attacks specifically targeting individuals in their homes. Table 4 outlines potential threats and evolving risks associated with social engineering tactics that could affect individuals at home. Table 5 identifies terms on proposed solutions to social engineering,

Terms Exploration for Theme Recognition of Past, Present and Solution of Social Engineering Threats

From responses from respondents, the following themes in (Figure 5) were identified:

Findings from Expert Interviews on Social Engineering Threats and Mitigation

Prevalent Social Engineering Threats Affecting Home Users

The findings indicate that phishing, vishing (voice phishing), and smishing (SMS phishing) are the most prevalent social engineering threats currently affecting home users. A majority of the participants (85%) identified these attack vectors as the dominant forms of social engineering encountered in recent years. These attacks were reported to result in financial loss, identity theft, and unauthorized access to personal devices. Participants further noted that social engineering attacks exploit human perceptual and emotional weaknesses, particularly trust, fear, and urgency. The findings also reveal that increased remote work and home-based digital activities have heightened users' exposure to these attacks. Insecurity-related factors, including banditry and kidnapping, were reported to intensify susceptibility, as attackers increasingly leverage fear-based manipulation techniques.

Anticipated Future Social Engineering Threats

The findings show that a significant proportion of experts (75%) anticipate that social engineering attacks will become more difficult to detect in the future due to advances in artificial intelligence and deepfake technologies. Participants reported that impersonation-based attacks are expected to increase, with attackers replicating trusted individuals or institutions to deceive home users. Experts further indicated that future social engineering tactics are likely to be more personalized and adaptive, increasing the likelihood of successful manipulation and further eroding user trust in digital communications.

Role of User Awareness in Mitigating Social Engineering Attacks

The findings demonstrate strong agreement among participants (95%) that user awareness plays a critical role in reducing susceptibility to social engineering attacks. Experts reported that informed users are significantly less likely to fall victim to manipulation-based threats. Participants highlighted the importance of continuous training and reinforcement, noting that one-time awareness initiatives are insufficient due to the evolving nature of social engineering tactics. The findings also indicate that restricting user privileges can reduce exposure to social engineering risks; however, this practice is not widely adopted by non-technical home users.

Effective Awareness Strategies for Home Users

The findings show that a substantial proportion of experts (75%) support the use of targeted awareness strategies, including interactive training programs, gamification, and real-time threat warnings. Participants emphasized the use of simple, non-technical language and relatable examples to improve engagement among home users.
Experts also identified social media platforms as effective channels for disseminating cybersecurity awareness due to their widespread use among home users. Customized training packages were reported to enhance engagement and information retention.

Mandatory Cybersecurity Awareness Training

Most participants (85%) supported making cybersecurity and social engineering awareness training mandatory for home users, particularly for individuals accessing sensitive information through personal devices. Annual refresher training combined with on-demand learning resources was

Theme	Terms
Present Social Engineering Impact on Home Users	Identity Theft, Unauthorized Access, Fraud, Scams, Malicious Software Attack, Data Breach & Manipulation, Privacy Violations, Direction to Fake Login Pages, Credential Theft, Spyware attack, Ransom ware Attack, Financial Loss, Character Assassination
Theme	**Terms**
Future Role of Social Engineering on Home Users	Data Harvesting Exploiting Further Vulnerabilities Cryptocurrency Theft AI-Driven Attacks Smart Device Exploits Emerging Threats Targeted Phishing Social Engineering Metamorphosis Cloud Storage Vulnerability Exploits Compromised Authentication Systems Social Media Deception
Theme	**Terms**
Effective Solution to Social Engineering	Strengthening Cybersecurity Awareness Security Awareness Training for Home Users Implementing Least Privilege Access Deploying Custom Anti-Phishing Tools Ongoing Cybersecurity Education Human-Centric Security Strategies Risk Mitigation Strategies

Figure 5: Figure 5: Identification of Terms on Present, Future and Solutions of Social Engineering

recommended to maintain sustained awareness. Participants further suggested that such training could establish baseline cybersecurity hygiene and reduce overall risk exposure.

Stakeholder Collaboration and Additional Mitigation Measures

Over half of the experts (55%) recommended collaborative efforts among governments, cybersecurity organizations, and educational institutions to promote a culture of cybersecurity awareness. Participants also suggested incentive-based approaches, such as rewards or insurance benefits linked to cybersecurity compliance, to encourage adoption of best practices

DISCUSSION

The findings showed that while technical controls such as firewalls, antivirus programs, and spam filters are necessary, they are not enough to mitigate the threats of social engineering which mainly exploit human cognition, emotion, and behavior. This supports existing evidence that technology-focused defenses cannot effectively address manipulation-based cyberattacks (Aldawood & Skinner, 2019; Siddiqi et al., 2022). Phishing, vishing, and smishing continue to be major attack vectors because home users remain vulnerable in poorly informed environments with lax security practices. The discovery that the increased use of personal digital devices for remote work has widen the attack surface further confirmed earlier researches that discovered home settings to be less secure than organizational infrastructures (Michaelides, 2021; Singh et al., 2022). Experts highlighted the increasing threat of AI-facilitated social engineering, encompassing deepfakes and meticulously targeted impersonation assaults. These recent advancements significantly diminish the efficacy of traditional detection approaches and necessitate adaptable, behavior-conscious security strategies. This aligns with literature indicating that advances in artificial intelligence are increasing the complexity and threat posed by social engineering attacks (Aslan et al., 2023; Guembe et al., 2022). One main result from this study is confirming that user awareness and education are very important factors for resilience against social engineering. Continuous awareness in context was found to be more effective than static training approaches. Nonetheless, the inadequate protection measures among home users indicates the persistence of usability and engagement obstacles. This corresponds with earlier appeals for security solutions that emphasize human-centered design and accessibility (Bullee & Junger, 2020; Grobler et al., 2021). In summary, these findings support call for an improved human-centric cybersecurity framework that incorporates cognitive, behavioral, psychological, and contextual elements alongside effective technology controls.

Development of Improved Human-Centric Framework

Based on the findings discussed in Section 5, an improved human-centric cybersecurity framework was developed to address the identified gap in the current cybersecurity strategies. The framework combined the identified gap, information from experts, and well-known principles of usable security that are human-centric to improve the existing counter-measure strategies. The aim is to fix the problems with technology-based models by adding human, behavioural, and contextual factors, as well as supportive technological measures, that are specifically made for home users. This framework uses an interdisciplinary approach because it recognises that social engineering attacks mostly target people's thoughts, feelings, and habits instead of technical weaknesses. The proposed model, therefore, places the user at the centre of cybersecurity defence, with awareness, behaviour, and decision-making as the most important protective layers, supported by technologies that are easy to use. Therefore, the proposed framework places the home users at the core of cybersecurity and focus on the need for an interdisciplinary approach that integrates human, behavioral, and technological factors to reduce vulnerabilities to social engineering attacks. The proposed framework integrates components that culminated into an improved cybersecurity culture in which home users are enabled to prevent, detect, and respond effectively to social engineering attacks. The integration of human-centric principles with usable technological support offers a dynamic and sustainable framework to mitigate social engineering threats in home settings (Figure 6).

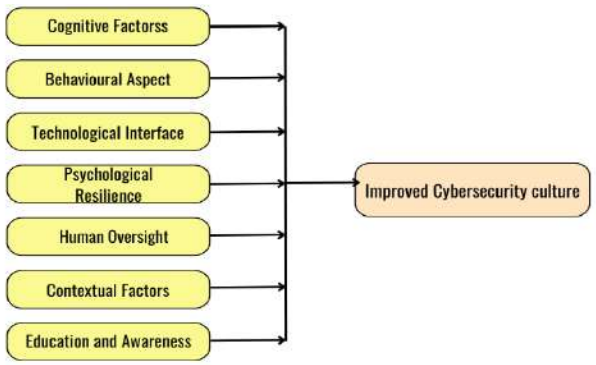

Figure 6: Improved Human-Centric Cybersecurity Culture

CONCLUSION

This research determined the sufficiency of the current cybersecurity countermeasures to counter the social engineering attacker against home users and found that there are major weaknesses in existing technology-focused systems. The results show that even though technical defenses are still needed, they are not adequate

in dealing with social engineering threats which mostly appeal to human cognition, emotions and behavior. Phishing, vishing, and smishing remain the order of the day, and their sophistication is growing due to trends of personalization, artificial intelligence, and impersonation.

The findings also underscore the fact that user consciousness, poor security habits, and amplified home-based digital behavior make one more vulnerable to such attacks. To this, this paper suggests a better human-based cyber security model, which incorporates cognitive, behavioral, psychological, and contextual elements with practical technological controls. The framework is better placed to reduce the changing social engineering threats by placing the home users as an active member in helping with cybersecurity defense and focus on constant awareness and flexibility. The work of the future needs to be based on the empirical validation of the framework in various home-user settings and even in a new threat environment. The paper evaluated the effectiveness of the existing cybersecurity countermeasures in mitigating social engineering-related attacks against home users. It has been identified that significant gaps exist in the current technology-based and human-centric approaches approaches. These results showed that technical defences were vital, but not sufficient to curb social engineering attacks that greatly use human cognition, emotions and behaviour. Phishing, vishing and smishing threats have been increasing in sophistication with personalization, artificial intelligence and impersonation tactics. The results highlight lack of awareness among users, inadequate security measures and more time taken at home which enhances susceptibility to such attacks. The proposed framework emphasize a more human-centric cyberspace security approach, which would use cognitive, behavioural, psychological as well as contextual factors with efficient technological controls. The framework also emphasizes home users as the frontline in cybersecurity defence, with suggestion on continuous awareness and flexibility as a priority, which makes the framework more sustainable in terms of dealing with the changing social engineering threats.

Limitations and future directions

A limitation of this research is the use of qualitative data with a purposive sample of cybersecurity experts. It might not completely reflect the experiences of all home users. The suggested human-centered cybersecurity framework remains conceptual and has not been empirically tested and applied in real home settings. Further studies should focus on supporting the framework through empirical research with a diverse range of home-user populations. To test its effectiveness, usefulness, and flexibility across different situations and evolving threat scenarios in social engineering, longitudinal and experimental measurements are recommended.

REFERENCES

Albladi, S. M., & Weir, G. R. S. (2018). User characteristics that influence judgment of social engineering attacks in social networks. *Human-Centric Computing and Information Sciences*, *8*(1), 1–24. https://doi.org/10.1186/s13673-018-0128-7

Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs-pitfalls and ongoing issues. *Future Internet*, *11*(3). https://doi.org/10.3390/fi11030073

AL-Otaibi, A., & S Alsuwat, E. (2020). A Study on Social Engineering Attacks: Phishing Attack. *International Journal of Recent Advances in Multidisciplinary Research*, *07*(11), 6374–6380.

Ambore, S., Dogan, H., & Apeh, E. (2021). Development of Usable Security Heuristics for Fintech. *34th British Human Computer Interaction Conference Interaction Conference, BCS HCI 2021*, 121–132. https://doi.org/10.14236/ewic/HCI2021.12

Asker, H., & Tamtam, A. (2023). Knowledge of Information Security Awareness and Practices for Home Users: Case Study in Libya. *European Scientific Journal, ESJ*, *19*(15), 238.

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. *Electronics (Switzerland)*, *12*(6). https://doi.org/10.3390/electronics12061333

Bendovschi, A. (2015). Cyber-Attacks – Trends, Patterns and Security Countermeasures. *Procedia Economics and Finance*, *28*(0), 24–31. https://doi.org/10.1016/s2212-5671(15)01077-1

Brar, H. S., & Kumar, G. (2018). Cybercrimes: A proposed taxonomy and challenges. *Journal of Computer Networks and Communications*, *2018*(1). https://doi.org/10.1155/2018/1798659

Bullee, J. W., & Junger, M. (2020). How effective are social engineering interventions? A meta-analysis. *Information and Computer Security*, *28*(5), 801–830. https://doi.org/10.1108/ICS-07-2019-0078

Burke, W., Stranieri, A., Oseni, T., & Gondal, I. (2024). The need for cybersecurity self-evaluation in healthcare. *BMC Medical Informatics and Decision Making*, *24*(1), 1–15. https://doi.org/10.1186/s12911-024-02551-x

Grobler, M., Gaire, R., & Nepal, S. (2021). User, Usage and Usability: Redefining Human Centric Cyber Security. *Frontiers in Big Data*, *4*(March), 1–18. https://doi.org/10.3389/fdata.2021.583723

Guembe, B., Azeta, A., Misra, S., Osamor, V., Fernandez-Sanz, L., & Pospelova, V. (2022). The Emerging Threat of Ai-driven Cyber Attacks: A Review. *Applied Artificial Intelligence*, *36*(1). https://doi.org/10.1080/08839514.2022.2037254

Hakimi, M., Fazil, A., & Quchi, M. (2024). Human factors in cybersecurity: an in depth analysis of user centric studies. *Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)*, *3*(01), 20–33. https://doi.org/10.58471/esaprom.v3i01.3832

Hamoud, A., & Aïmeur, E. (2020). Handling User-Oriented Cyber-Attacks: STRIM, a User-Based Security Training Model. *Frontiers in Computer Science*, *2*(September), 1–17. https://doi.org/10.3389/fcomp.2020.00025

Holland, N. (2020). *The human-centric cybersecurity stance*. https://doi.org/10.19044/esj.2023.v19n15p238

INTERPOL. (2023). *AFRICAN CYBERTHREAT ASSESSMENT REPORT 2023 AFRICAN CYBERTHREAT ASSESSMENT REPORT CYBERTHREAT TRENDS* (Issue March). https://www.interpol.int/content/download/19174/file/2023_03 CYBER_African Cyberthreat Assessment Report 2022_EN.pdf

Kolodziej, J. (2024). *Human-centric cybersecurity: trends - secmos invited talk*. 567–568. https://doi.org/10.7148/2024-0567

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

Malik, A., Abid, A., Farooq, S., Abid, I., Nawaz, N. A., & Ishaq, K. (2022). Cyber Threats: Taxonomy, Impact, Policies, and Way Forward. *Ksii Transactions on Internet and Information Systems*, *16*(7). https://doi.org/10.3837/tiis.2022.07.017

Michaelides, N. (2021). *Remote Working and Cyber Security Literature Review*. *February*. https://www.researchgate.net/publication/349396561_Remote_Working_and_Cyber_Security_Literature_Review

Moustafa, A. A., Bello, A., & Maurushat, A. (2021). The Role of User Behaviour in Improving Cyber Security Management. *Frontiers in Psychology*, *12*(June), 1–9. https://doi.org/10.3389/fpsyg.2021.561011.

Nasir, S. N. S. (2023). Exploring the Effectiveness of Cybersecurity Training Programs: Factors, Best Practices, and Future Directions. *Advances in Multidisciplinary & Scientific Research Journal Publication*, *2*(1), 151–160. https://doi.org/10.22624/aims/csean-smart2023p18

Ofcom. (2014). Adults' Media Use and Attitudes Report 2014.

Oni, D., Arshad, E., & Pham, B. N. (2023). Cybercrime on Social Media In Nigeria: Trends, Scams, Vulnerabilities and Prevention. *Advances in Multidisciplinary and Scientific Research Journal Publication*, *2*(1), 143–150. https://doi.org/10.22624/aims/csean-smart2023p17.

Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2022). Leveraging human factors in cybersecurity: an integrated methodological approach. *Cognition, Technology and Work*, *24*(2), 371–390. https://doi.org/10.1007/s10111-021-00683-y

Sarawagi, K., & Srivastava, A. (2017). Examination of Cyber Crime in Special Reference of Non- Technical Attacks. *International Journal of Forensic Sciences*, *2*(1), 0–4. https://doi.org/10.23880/ijfsc-16000117

Siddiqi, M. A., Pak, W., & Siddiqi, M. A. (2022). A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures. *Applied Sciences (Switzerland)*, *12*(12). https://doi.org/10.3390/app12126042

Singh, H., Grundy, J., Graetsch, U. M., Khalajzadeh, H., & Paktinat, S. (2022). Modelling human-centric aspects of end-users with iStar. *Journal of Computer Languages*, *68*, 101091. https://doi.org/10.1016/j.cola.2022.101091

Taherdoost, H. (2022). Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview. *Electronics (Switzerland)*, *11*(14). https://doi.org/10.3390/electronics11142181

van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior*, *75*, 547–559. https://doi.org/10.1016/j.chb.2017.05.038
Website, *April*, 182. http://stakeholders.ofcom.org.uk/market-data-research/other/research-publications/adults/media-lit-10years/%5Cnhttp://stakeholders.ofcom.org.uk/market-data-research/other/research-publications/adults/adults-media-lit-14/

Young, H., van Vliet, T., van de Ven, J., Jol, S., & Broekman, C. (2018). Understanding human factors in cyber security as a dynamic system. *Advances in Intelligent Systems and Computing*, *593*(March 2022), 244–254. https://doi.org/10.1007/978-3-319-60585-2_23

Ystgaard, K. F., Atzori, L., Palma, D., Heegaard, P. E., Bertheussen, L. E., Jensen, M. R., & De Moor, K. (2023). Review of the theory, principles, and design requirements of human-centric Internet of Things (IoT). In *Journal of Ambient Intelligence and Humanized Computing* (Vol. 14, Issue 3). Springer Berlin Heidelberg. https://doi.org/10.1007/s12652-023-04539-3

Zheng, Y., Li, Z., Xu, X., & Zhao, Q. (2022). Dynamic defenses in cyber security: Techniques, methods and challenges. *Digital Communications and Networks*, *8*(4), 422–435. https://doi.org/10.1016/j.dcan.2021.07.006.