SEMARAK ILMU
PUBLISHING
202103268166(003316878-P)

Journal of Advanced Research in Applied Sciences and Engineering Technology

Journal homepage:
https://semarakilmu.com.my/journals/index.php/applied_sciences_eng_tech/index
ISSN: 2462-1943

Unveiling the Dynamics of Cybersecurity Awareness and Exploring Influential Factors for Enhanced Vigilance: A Systematic Literature Review

Noor Haslindawati Abd Rahman[1,2,*], Md Zawawi Abu Bakar[1], Zalmizy Husin[1]

[1] School of Applied Psychology, Social Work and Policy, Universiti Utara Malaysia, Sintok, Kedah, Malaysia
[2] Commercial Crime Investigation Department, Royal Malaysian Police Bukit Aman Headquarters, Kuala Lumpur, Malaysia

ABSTRACT

Cybersecurity threats are spreading worldwide, targeting unsuspecting individuals and leading to substantial financial and emotional hardships. While general cybersecurity awareness has been studied extensively, there is a discernible gap in the literature focusing on the dynamics of cybersecurity awareness. Therefore, this systematic literature review aims to elucidate influential factors that can boost vigilance against cybersecurity threats. Adhering to the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines, 29 articles had been meticulously reviewed. The findings were categorised under four primary themes: (i) Regional and demographic concerns in cybersecurity awareness highlighted the susceptibility of specific groups to cybersecurity threats and stressed targeted awareness campaigns. (ii) Educational approaches and assessment tools for cybersecurity emphasised the significance of comprehensive education models to combat these threats. (iii) Technological Advancements, Models and Cybersecurity Implications underscored the double-edged sword of technology, indicating both pitfalls and safeguards against cybersecurity threats. (iv) Behavioral, attitudinal, and perceptional aspects of cybercrime and security revealed how attitudes and behaviours can function as both a susceptibility and a safeguard against cybersecurity dangers. Expert opinions solidified the findings, endorsing the importance of multifaceted awareness strategies. Improving cybersecurity awareness by integrating regional insights, education, technological tools, and a comprehensive understanding of behavioural dynamics is crucial. By comprehending and addressing these factors, societies can foster an environment of heightened vigilance against cybersecurity threats.

Keywords:
Cybersecurity; phone; digital; telecommunication; awareness; vigilance

1. Introduction

In the evolving communication technology landscape, cybersecurity has emerged as a pervasive threat, taking advantage of the prevalence of mobile devices and the personal nature of phone communications. As these fraudulent schemes become increasingly sophisticated, understanding the dynamics of cybersecurity awareness is paramount in developing robust strategies to enhance public vigilance and resilience. This systematic literature review endeavours to consolidate existing

[*] *Corresponding author.*
E-mail address: sab5485h2@gmail.com

https://doi.org/10.37934/araset.XX.X.255270

knowledge, analyse the influential factors and chart a comprehensive overview of cybersecurity awareness. In their various manifestations, cybersecurity threats exploit human vulnerabilities and leverage technological advancements to deceive and manipulate individuals, resulting in financial losses and the leaking of personal information. Despite the growing incidence of these threats, public awareness and understanding remain inconsistent. This phenomenon underscores the necessity of investigating the influential factors that shape cybersecurity awareness and determining effective avenues for promoting enhanced vigilance.

The body of literature on cybersecurity is broad and includes research from psychology, communication, criminology, and information technology. This review systematically synthesises these studies to unravel the complex interplay of factors influencing cybersecurity awareness. In doing so, it aims to identify gaps in the current knowledge, highlight effective educational and preventative strategies, and propose directions for future research. However, the role of cognitive biases, psychological traits, and social influences in shaping awareness cannot be understated. Technological advancements and the rapid adoption of smartphones have also played a pivotal role in the evolution of these threats. Moreover, it underscores the importance of fostering a cybersecurity and digital hygiene culture to mitigate the risk.

This systematic literature review delves into the multifaceted nature of cybersecurity awareness, aiming to uncover influential factors for enhanced vigilance. Despite a wealth of existing literature, knowledge deficiencies remain in cybersecurity awareness, underscoring the importance of conducting longitudinal studies to observe how public awareness and scam tactics evolve. Further investigation into the effectiveness of educational and preventative strategies is essential to optimise interventions for diverse demographic and cultural contexts. This review, which involves multidisciplinary literature, comprehensively explores the factors shaping cybersecurity awareness, emphasising the crucial roles of academia, policymakers, and the general public in safeguarding against cybersecurity threats. By identifying effective strategies and highlighting the pressing nature of this issue, the review sets the stage for future research and interventions, emphasising the collective effort required to build resilience against these evolving threats.

1.1 Demographic Influences on Cybersecurity Awareness

Cybersecurity threats represent a significant challenge in today’s digital age, leveraging the pervasive use of mobile devices to exploit individuals. Numerous studies highlighted demographic variables as one of the key factors in susceptibility to cybersecurity threats. A survey conducted among staff and students in tertiary institutions in the State of Imo, Nigeria, reveals a high level of cybercrime awareness (89%), with understanding primarily focused on computer-related cybercrimes, indicating a disparity in awareness between genders and a positive correlation with education level and age [1]. Awareness of cybercrime among secondary students in Lucknow, India, was not significantly affected by gender or type of school management [2]. Demographic variables such as age, education, and socioeconomic status have been identified as critical factors in determining an individual’s susceptibility to cybersecurity threats [3]. Moreover, the elderly demographic is especially prone to cybercrimes due to their difficulty grasping modern cybersecurity measures’ intricacies [4].

1.2 Educational Initiatives and Tools for Cybersecurity Awareness

The psychological and cognitive dimensions of scam awareness have garnered emphasis on the role of education in enhancing awareness, suggesting targeted educational initiatives as substantial attention in recent literature. Since older adults are vulnerable to online scams, there is a need to customise their cybersecurity awareness education and grassroots educational strategies to enhance their prevention skills effectively [5]. The critical success factors for the Security Education, Training, and Awareness (SETA) program effectiveness have been studied by Al-Nuaimi [6], and regular communication is vital to highlight the program's role in safeguarding information assets, boosting cybersecurity awareness, and mitigating security risks within organisations. It also underscores the necessity for customised educational initiatives to bridge gaps in cybersecurity awareness and preventive measures across diverse contexts and demographics. Besides, the South African Police Service (SAPS) struggles to raise awareness among Gauteng's youth about cybercrime due to limited resources, highlighting the need for specialised education initiatives for vulnerable populations [7].

1.3 Technological Landscape and Cybersecurity Threats

The technological landscape is a critical factor in the evolution of cybersecurity threats. In the context of Iraqi Academia, it investigates the impact of various cybersecurity initiatives on digital awareness, demonstrating a crucial need for enhanced education and understanding in dealing with cybersecurity threats [8]. Meanwhile, a study of Welsh Small and Medium Enterprises (SMEs) by [40] reveals a significant gap in adopting intelligent software for cybersecurity prevention, with only 30% demonstrating adequate cybersecurity understanding. The factors influencing cybersecurity awareness among Nigerian youths were comprehensively examined by Olofinbiyi [9], which comprise urbanisation, unemployment, poverty, and weak law enforcement, emphasising the urgent need for enhanced cybersecurity practices and stringent law enforcement. The study by Hadlington and Sally [10] uncovers the essential correlation between susceptibility to cybersecurity threats, understanding of information security, and personal traits, showing that 60% of subjects are classified in higher-risk segments, underscoring the significance of demographic aspects in creating focused awareness and intervention tactics.

1.4 Social and Cultural Factors in Cybersecurity Awareness

Social networks and cultural contexts also play pivotal roles in shaping cybersecurity awareness. A study in Saudi Arabia reveals cybersecurity practices among 1,230 participants, including widespread use of public Wi-Fi, personal data in passwords, and low awareness of phishing attacks, emphasising the urgent need for improved cybersecurity education and practices in the region [11]. A comprehensive study by Arpaci and Ersin [12] introduced the Cybersecurity Awareness Scale (CAS) to assess individual awareness and responses to cybersecurity threats, validating its reliability and validity through two extensive parts with 994 participants. Additionally, [10] introduced the Cybersecurity Awareness on Social Media Scale (CASM-S), a validated and reliable tool for assessing awareness of cybersecurity threats like phone scams on social media platforms. An analysis performed by Adebayo *et al.,* [4] evaluated and recognises the Synergistic Cybersecurity Awareness Model for the Elderly (SCSAM-Elderly) as the optimal choice for enhancing cybersecurity awareness in older individuals, promoting education to boost their understanding and safety.

2. Methodology

The Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) protocol was utilised in a qualitative research approach for analysing documents via a systematic literature review. The PRISMA guidelines have been designed to ensure that systematic reviews are valuable to users.

Additionally, authors need to present a transparent, comprehensive, and precise rationale for conducting the review and detailing their research (like how studies were identified and selected) and what has been discovered (including the characteristics of the contributing studies and meta-analysis results). The systematic literature review started based on this review procedure by formulating excellent research questions for the review. Moreover, the authors then discussed the systematic search strategy, comprising four stages: identification, screening, eligibility and inclusion. Finally, how the data were retrieved, processed, and analysed will be explained before they are utilised in the study.

2.1 Identification

The identification phase involves searching for synonyms, related concepts, and variations of crucial keywords for the research. The aim is to obtain more pertinent articles for subsequent analysis. The research query, derived from a reference [13], facilitated the generation of the keywords list. The identification technique was based on a blend of a web-based thesaurus, keywords from past studies, and keywords sourced from Scopus. In two prominent databases, Scopus and Web of Science (WOS), the authors successfully expanded upon existing keywords and devised an exhaustive search string (utilising Boolean operators, truncation, wild card, phrase searching, as well as field code functions (refer to Table 1).

Table 1
The search string

Database	Search string
SCOPUS	TITLE-ABS-KEY ((cybersecurity OR “cyber security”) AND (phone* OR digital* OR telecommunication*) AND (awareness OR vigilance)) AND PUBYEAR > 2019 AND PUBYEAR < 2024 AND (LIMIT-TO (DOCTYPE , “ar”)) AND (LIMIT-TO (LANGUAGE , “English”))
Web of Science	TS=((cybersecurity OR “cyber security”) AND (phone* OR digital* OR telecommunication*) AND (awareness OR vigilance)) and Preprint Citation Index (Exclude-Database) and 2020 or 2021 or 2022 or 2023 (Publication Years) and Article (Document Types) and English (Languages)

Due to their advanced search capabilities, strict quality control of articles, thorough indexing, and broad focus across multiple disciplines, these databases are well-positioned for systematic literature reviews [14]. Science Direct and Google Scholar were selected as additional databases [15], with Google Scholar complementing traditional scientific databases, ensuring a thorough and optimal retrieval of relevant references. The keywords were combined using phrase searching functions and Boolean operators (OR, AND), as appropriate, and detailed in Table 1. The academic search system satisfied all performance standards, suggesting Science Direct and Google Scholar as complementary databases, leading to 1,550 articles. Figure 1 depicts the search outcomes from these two databases, Scopus as well as Web of Sciences (WOS).

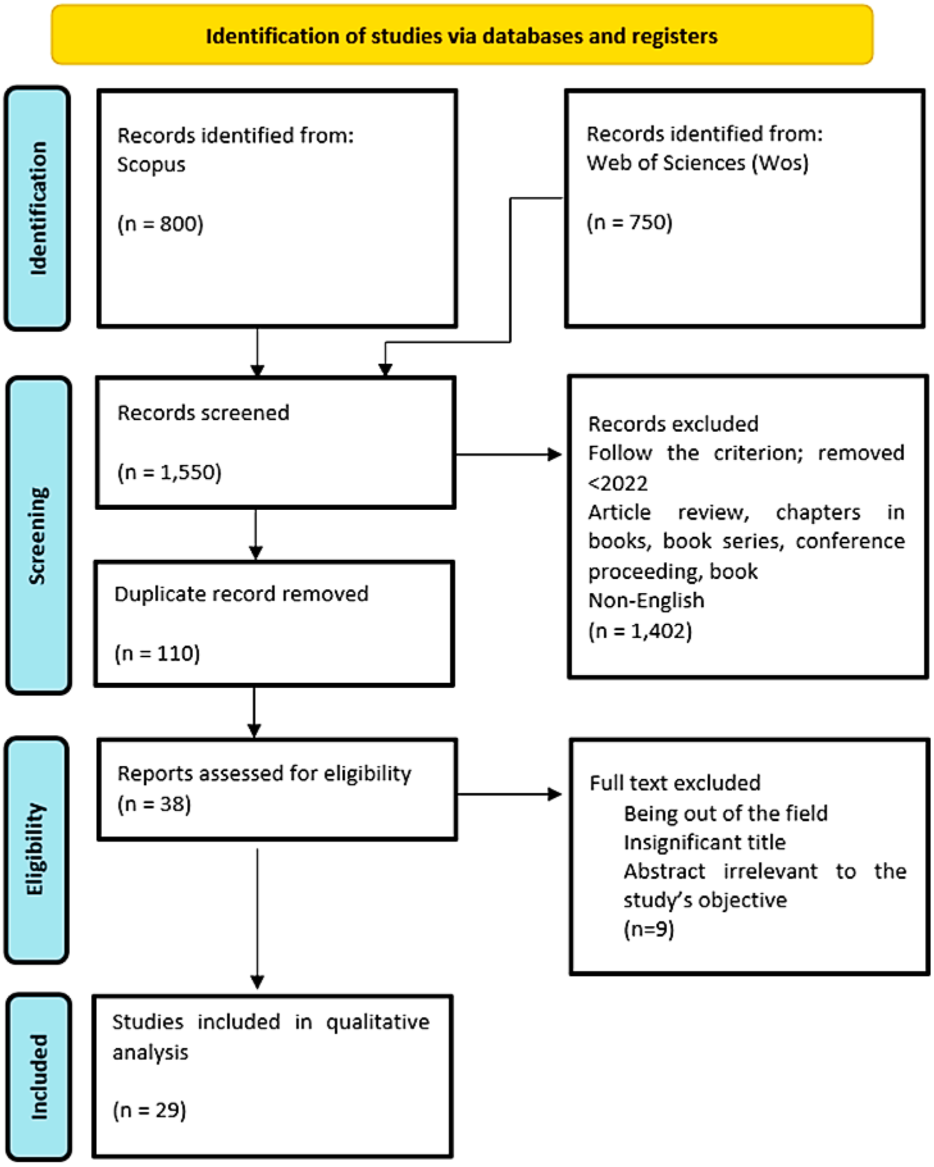
Identification of studies via databases and registers
Identification
Screening
Eligibility
Included
Records identified from: Scopus (n = 800)
Records identified from: Web of Sciences (Wos) (n = 750)
Records screened (n = 1,550)
Records excluded
Follow the criterion; removed <2022
Article review, chapters in books, book series, conference proceeding, book
Non-English
(n = 1,402)
Duplicate record removed (n = 110)
Reports assessed for eligibility (n = 38)
Full text excluded
Being out of the field
Insignificant title
Abstract irrelevant to the study's objective
(n=9)
Studies included in qualitative analysis (n = 29)

Fig. 1. Flow diagram of the suggested searching study [16]

2.2 Screening

The article selection criteria were applied in screening all 1,550 chosen studies, aided by the database's sorting feature. The selection criteria must be relevant to the research question [17]. Given the vast literature, it advised researchers to set manageable review periods [13]. Suggested using time-based limitations only when it's apparent that pertinent studies fall within a particular timeframe [18]. The database search revealed a surge of research from 2020 to 2023 focusing on the factors influencing phone scam awareness. Only studies written in English with verified data and published in journals have been considered to ensure that the information is universally comprehensible. From the initial pool of 1,550 articles, 1,402 were disqualified for not meeting the criteria, leaving only 148. After removing 110 duplicates, the final assessment focused on the remaining 38 articles.

2.3 Eligibility

After screening, the authors carefully examined the remaining 34 articles to confirm they met the necessary criteria (Table 2). The eligibility assessment involved examining the articles' titles and abstracts. Given the emphasis on exploring influential factors for enhanced cybersecurity vigilance, 9 articles were excluded, leaving 29 articles.

Table 2
The inclusion and exclusion criteria

Criteria	Inclusion	Exclusion
Timeline	2020-2023	<2020
Document Type	Article journal (empirical data)	Article review, chapters in the book, book series, conference proceeding, book
Language	English	Non-English

2.4 Data Abstraction and Analysis

This research employed an integrative analysis to evaluate various research methods, including quantitative, qualitative, and mixed designs. The primary objective was to identify pertinent subjects and their subcategories. The first step in theme formation was data collection. The authors meticulously examined the 29 articles whose content aligns with the focus of this study, as depicted in Figure 1. The authors then examined the elements that prompt society to be conscious of cybersecurity. Four main subjects had been identified: (i) regional and demographic, (ii) educational approaches and assessment tools, (iii) technological advancements, models and cybersecurity implications, and (iv) behavioural, attitudinal and perceptual aspects. The authors broadened the discussion of these topics by encompassing related themes, concepts, or perspectives. A detailed log captured insights, conundrums, and viewpoints throughout the study. The researchers scrutinised results for thematic uniformity, debating and reconciling discrepancies before finalising the themes. A cybercrime expert and a psychologist were involved to validate the themes. This expert review aimed to ensure each subtheme's clarity, relevance, and appropriateness by verifying its scope. The lead author adjusted their conclusions based on expert feedback and professional insights.

3. Results

Delving into the dynamics of cybersecurity awareness and analysing influential factors for improved vigilance delivers a comprehensive systematic literature review, bringing attention to essential aspects of cybersecurity. The study delves into the intricacies of cybersecurity awareness, highlighting how susceptibility and readiness differ among various regions and demographics. It meticulously assesses the efficacy of educational strategies and tools to bolster cybersecurity. The research underscores their intertwined relationship with cybersecurity implications by examining technological advancements. This analysis examines the behavioural, attitudinal, and perceptual dimensions of cybercrime and security, providing a comprehensive understanding of the current landscape.

3.1 Regional and Demographic Concerns in Cybersecurity Awareness

The theme explores regional and demographic-focused research to gauge cybersecurity awareness and identify unique challenges encountered (Table 3).

Table 3
Regional and demographic concerns in cybersecurity awareness

Authors	Title	Source title	Methodology	Result and advantage
Balabantaray *et al.,* [19]	A sociological study of cybercrimes against women in India: Deciphering the causes and evaluating the impact on the victims	International Journal of Asia-Pacific Studies	Purposive sampling	In India, the incidence of cybercrimes is on the rise, particularly affecting women who have lower computer literacy and are more emotionally vulnerable.
Garba [20]	An approach to cybercrime issues in Dandume local government area of Katsina State, Nigeria	Nigerian Journal of Technology	Structured questionnaire for 115 Dandume residents; analysed statistically.	Dandume faces high cybercrime rates. Many are unaware of protections. Emphasises community education and enhanced security.
Karagiannopoulos *et al.,* [5]	Cybercrime awareness and victimisation in individuals over 60 years: A Portsmouth case study	Computer Law and Security Review	Focus groups and semi-structured interviews with fifteen older adults over 60.	Older adults need tailored cyberawareness. Co-designed education is crucial for effective cyber-risk education.
Olofinbiyi [9]	Exploring youth awareness of cybercrime and factors engendering its proliferation in Nigeria	African Renaissance	one-on-one semi-structured, in-depth interviews	Factors identified for youth's cybercrime in Nigeria. Recommends Information Technology (IT) security, strict laws, and individual protections.
Khalid *et al.,* [8]	Cybercrime challenges in Iraqi academia: Creating digital awareness for preventing cybercrimes	International Journal of Cyber Criminology	The study sampled 140 academicians, conducted an online questionnaire, and analysed them using the Statistical Package for Social Sciences (SPSS).	Digital awareness boosts examined variables. Comprehensive methods enhance awareness. Institutions: prioritise cybersecurity in curriculums for safety.
Verma and Shyam [2]	Awareness towards cybercrime among secondary school students: The role of gender and school management	Safer Communities	100 students; Likert scale; "t" test analysis.	Gender and school management do not expect cybercrime awareness. Policy curriculum changes are suggested to promote a safer environment.

3.2 Educational Approaches and Assessment Tools for Cybersecurity

This theme focuses on the role of emerging technologies, including the modelling techniques applied to predict and analyse cyber threats. The broader implications of these advancements were also discussed (Table 4).

Table 4
Educational approaches and assessment tools for cybersecurity

Authors	Title	Source title	Methodology	Result and advantage
Alharbi and Asifa [21]	Assessment of cybersecurity awareness among students of Majmaah University	Big Data and Cognitive Computing	Majmaah University questionnaire; quantitative; Analysis of variance (ANOVA); Kaiser–Meyer–Olkin (KMO) tests.	Majmaah University students show cybersecurity gaps. They emphasised education needs. Recommendations are given for safety and compliance.
Shah and Anuja [22]	Cyber Suraksha: A card game for smartphone security awareness	Information and Computer Security	Used learning theory, Fogg model, between-subjects design; Pearson's Chi-Square.	Cyber Suraksha champions the adoption of security measures, revealing that the intervention group is 2.65 times more inclined to take action. It underscores the potency of hope and fear in raising cybersecurity awareness.
Arpaci and Omer [23]	Development of a scale to measure cybercrime awareness on social media	Journal of Computer Information Systems	1,045 users; Exploratory, principal components, Confirmatory analysis; tested Cybercrime-Awareness on social media (CASM-S) properties.	The CASM-S is a one-dimensional, robustly reliable instrument with a validated structure, effectively gauging cybercrime awareness on social media.
Arpaci and Ersin [12]	Development of the Cybercrime Awareness Scale (CAS): A validity and reliability study in a Turkish sample	Online Information Review	Developed CAS, two exploratory and confirmatory studies, with 994 respondents.	The three-factor structure confirms the validity of CAS, offering a reliable assessment of cybercrime awareness and significantly enriching cybersecurity literature.
Conway and Lee [24]	How do undergraduate students construct their view of cybercrime? Exploring definitions of cybercrime, perceptions of online risk and victimisation	Policing-A Journal of Policy and Practice	Three focus groups, 16 undergraduates; inductive thematic analysis.	Misconceptions about cybercrime can leave students vulnerable. Targeted education empowers them to mitigate risks and decrease the likelihood of becoming victims.
Maran and Bamasoud [25]	The impact of enhancing awareness of cybersecurity on universities students: A survey paper	Journal of Theoretical and Applied Information Technology	Survey on cybersecurity awareness; Saudi university students.	Inadequate cybersecurity knowledge among Saudi students elevates risk levels. Boosting awareness aligns with Saudi Vision 2030 objectives and fortifies security.

3.3 Technological Advancements, Models and Cybersecurity Implications

This theme explores the emerging technologies and the predictive models used to forecast and scrutinise cyber threats. The wider consequences of these technological progressions are also reviewed (Table 5).

Table 5
Technological advancements, models and cybersecurity implications

Authors	Title	Source title	Methodology	Result and advantage
Razaque *et al.,* [26]	Avoidance of cybersecurity threats with the deployment of a web-based blockchain-enabled cybersecurity awareness system	Applied Sciences (Switzerland)	Web-based Blockchain (WBCA) program; trained users; expert validation.	WBCA bolsters cybersecurity proficiency through Blockchain technology, efficiently authenticates skills, and surpasses competing online programs while elevating awareness.
Rawindaran *et al.,* [27]	Exploration of the impact of cybersecurity awareness on Small and Medium Enterprises (SMEs) in Wales using intelligent software to combat cybercrime	Computers	Welsh SMEs' cybercrime survey; 122 respondents; analysed influencing factors.	Welsh SMEs exhibit a modest understanding of cybercrime software, with only 30% familiar with the relevant terminology. The scale of educational resources influences their decision-making processes. It is advisable to formulate strategic recommendations to address this knowledge gap.
Sagheer *et al.,* [28]	Factors affecting adaptability of cryptocurrency: An application of technology acceptance model	Frontiers in Psychology	Surveyed 333 Z generation	The impact of adopting cryptocurrency is influenced by perceived usefulness, ease of use, and risk, which are mediated by technology awareness and further bolstered by government support.
Tin *et al.,* [29]	Machine learning based predictive modelling of cybersecurity threats utilising behavioural data cybersecurity threat predictive modelling	International Journal of Advanced Computer Science and Applications	Used behavioral data, 207 undergraduates;	The K-Nearest Neighbor (KNN) model adeptly forecasts cybercrime risks, enhancing user vigilance and proactive measures through timely alerts.
Ridho [30]	Unmasking online fake job group financial scams: A thematic examination of victim exploitation from perspective of financial behavior	Journal of Financial Crime	Blended case study, thematic analysis; explored online scam dynamics.	Online scams exploit behavioural finance principles. Public awareness, corporate responsibility, and robust regulations are necessary.

3.4 Behavioural, Attitudinal and Perceptual Aspects of Cybercrime and Security

The theme explores public perception, response, and conduct on cybercrimes, considering their attitudes, awareness, and actions (Table 6).

Table 6
Behavioural, attitudinal and perceptual aspects of cybercrime and security

Authors	Title	Source title	Methodology	Result and advantage
Datt and Tewari [31]	A Study of Computer users' attitude and awareness towards cyber security A study of computer	International Journal of Computer Information Systems and Industrial Management Applications	Survey-based questionnaire collected primary data.	Females are more unaware of online risks than males. Protection measures against cyber-attacks are recommended.
Ayyoub [32]	Awareness of electronic crimes related to e-learning among students at the university of Jordan	Heliyon	Quantitative research methods were used. Questionnaires were distributed to students in online courses.	Students at Jordan University exhibit a strong understanding of cybercrime risks, yet their grasp of e-learning legalities remains moderate. It is advisable to bolster this awareness for comprehensive online safety.
Mai and Andrea [33]	Cyber security awareness and behavior of youth in smartphone usage: a comparative study between university students in Hungary and Vietnam	Acta Polytechnica Hungarica	Questionnaires for 313 university students in Hungary as well as Vietnam. Quantitative analysis with SPSS	Cybersecurity awareness is globally deficient, with subtle behavioural variations. Studies highlight cultural subtleties in system design.
Lee and Ji [34]	How victims perceive fear of cybercrime: importance of informed risk	Criminal Justice Studies	Used 2019 Eurobarometer; analysed 10 cybercrimes; multilevel regression.	Victims of cybercrime live in fear; experts recommend targeted policies, education, and global collaboration to mitigate these informed risks.
Althibyani and Abdulrahman [35]	Investigating the effect of students' knowledge, beliefs, and digital citizenship skills on the prevention of cybercrime	Sustainability (Switzerland)	Mixed-method; surveys, interviews; 652 Saudi students.	Digital citizenship is crucial in decreasing cybercrimes; understanding laws, etiquette, and effective communication are essential for online education.
Abdul Wahab *et al.,* [36]	Knowledge, attitude and practice society in Kuala Lumpur against online fraud crime prevention campaign	Malaysian Journal of Communication	Qualitative; focus groups; 21 informants; Kuala Lumpur districts	The community exhibits a high level of knowledge regarding fraud prevention, with campaigns efficiently highlighting the advantages and motivating constructive actions.

Table 6
Behavioural, attitudinal and perceptual aspects of cybercrime and security

Authors	Title	Source title	Methodology	Result and advantage
Pitchan *et al.,* [37]	Knowledge, attitudes, practices towards information privacy & security of online purchase by youth	Malaysian Journal of Communication	Quantitative: 400 respondents; Klang, Selangor; online purchasing questionnaire.	Knowledge empowers young individuals to effectively shield themselves from cybercrime and mitigate the risks of online transactions. Education is instrumental in ensuring safety.
Alzubaidi [11]	Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia	Heliyon	Online questionnaire; 1230 participants; Saudi Arabia; cyber-security awareness.	A recent survey in Saudi Arabia revealed that 31.7% access public Wi-Fi, 51% secure their accounts with personal passwords, and 32.5% are uninformed about phishing. Underscores the critical need for enhanced cybersecurity awareness.
Kimpe *et al.,* [38]	Research note: an investigation of cybercrime victims' reporting behavior	European Journal of Crime Criminal Law and Criminal Justice	Survey; 334 cybercrime victims; analysed reporting behaviours/patterns.	73.4% of victims choose not to report; older individuals tend to report more frequently. Advocates emphasise the importance of educating youth and implementing a centralised reporting system.
Hadlington and Sally [10]	Segmentation analysis of susceptibility to cybercrime: exploring individual differences in information security awareness and personality factors	Policing (Oxford)	Online survey; 1,054 participants; cybercrime susceptibility, demographics.	Lack of awareness leads to a 60% increase in vulnerability to cybercrime. Supports the identification of at-risk groups and the development of targeted interventions.
Fissel and Jin [39]	The cybercrime illusion: Examining the impact of cybercrime misbeliefs on perceptions of cybercrime seriousness	Journal of Criminology	Mechanical Turk survey; 504 adults; perceptions, terminology, demographics.	Varied opinions on the gravity of cybercrime; older adults tend to take it more seriously. There is a need for educational programs.
Lee and Yi [40]	The role of cybersecurity knowledge and awareness in cybersecurity intention and behavior in the United States	Crime and Delinquency	U.S. study; cybersecurity knowledge; various predictors analysed.	Predictions of cybersecurity knowledge can be made based on variables such as Information and Communications Technology (ICT), education, income, and gender; it is crucial to comprehend both technical and human factors.

4. Discussions

The findings of this systematic literature review highlight the substantial differences in cybersecurity awareness among various regions, primarily shaped by demographic factors. For instance, in India, there's a concerning rise in cybercrimes targeting women, attributed to a disparity in computer literacy, with many female victims experiencing mental health issues such as depression and anxiety [19]. Similarly, in the Dandume community, despite frequent cybercrime occurrences, there is a general lack of awareness about protective measures, highlighting the urgent need for community education [20]. Furthermore, specialised cybersecurity awareness campaigns are necessary for the elderly, underscoring the importance of individualised prevention and education efforts. Additionally, the study reveals a growing youth involvement in cybercrimes in Nigeria, highlighting the necessity for enhanced IT security and robust cybercrime laws. Notably, gender and school management do not play a significant role in shaping cybercrime awareness, emphasising the essential need for cybersecurity education across diverse populations.

Digital applications positively impact student learning, especially among youth, by making teaching engaging, interactive, and flexible. However, overuse can lead to antisocial behavior and neglect of studies. The study emphasizes the importance of digital applications in education, highlighting their effectiveness in promoting self-directed learning, critical thinking, and improved academic achievements in the industry 4.0 era [41]. These skills are crucial in addressing cybercrime threats, as critical and logical thinking help individuals recognize and mitigate cyber risks more effectively. An interdisciplinary, problem-based approach is needed to develop critical, logical, and systematic thinking. STEM education impacts other fields like social and economics, with graduates often employed in non-technology sectors due to their critical thinking skills [42]. This insight aligns with the need for improved cybersecurity education. By integrating STEM education principles, students can develop the necessary skills to understand and combat cyber threats effectively. Critical and logical thinking, fostered through STEM, are essential in addressing complex cybersecurity issues, making individuals more adept at recognizing and mitigating cyber risks.

Educational interventions and assessment tools are crucial in enhancing cybersecurity awareness, addressing significant knowledge gaps among students and fostering secure behaviours. Innovative methods such as the "Cyber Suraksha" game have been proven effective in promoting cybercrime awareness among participants. Furthermore, assessment tools like CASM-S and CAS have been developed with high reliability to gauge users' cybercrime awareness, particularly on social media platforms. Addressing misconceptions about cybercrimes, including phone scams, is vital to equip at-risk groups with protective strategies to reduce potential victimisation. Strengthened cybersecurity instruction promotes individual safety and aligns with broader national objectives, such as Saudi Arabia's Vision 2030, which underscores the development of a secure digital society.

The influence of novel technologies on cybersecurity awareness is also explored, highlighting the effectiveness of tools like Blockchain technology in educating users and enhancing their cybersecurity knowledge. However, Welsh SMEs have a notable awareness gap regarding intelligent software and machine learning in cybercrime prevention. Predictive modelling, such as the KNN, has demonstrated high accuracy in anticipating cybercrime threats, aiding users in recognising and mitigating risks. Additionally, online scams, particularly phone scams, exploit behavioural finance principles, emphasising the urgency for increased public awareness and stronger regulations to ensure online safety.

Furthermore, cybersecurity awareness levels show significant variation due to behavioural, attitudinal, and perceptual factors, leading to a lack of understanding regarding online sharing and phishing risks, especially among females. Cultural differences across nations underscore the necessity of global cyber-awareness solutions. At the same time, victims' fears are shaped by the trauma of cybercrimes they have faced, highlighting the importance of policies informed by experience. Digital citizenship skills are instrumental in safeguarding against cybercrimes in e-learning environments, and successful fraud prevention campaigns demonstrate effective awareness strategies. Nevertheless, numerous cybercrime victims refrain from reporting incidents, emphasising the requirement for specific intervention to deal with the public's limited security awareness and impulsiveness. Ultimately, knowledge about Information and Communications Technology (ICT) and demographic factors is pivotal in cybersecurity education and awareness efforts.

This study aimed to determine whether cybersecurity awareness varies globally, influenced by demographics, regions, and educational interventions. Knowledge gaps persist, notably among women, highlighting the importance of focused education. Awareness and protective measures remain insufficient in the face of frequent cybercrimes. Advanced assessment tools and games enhance cybersecurity knowledge, yet misconceptions about phone scams persist. The research underscores the importance of tailoring educational strategies, leveraging innovative platforms, and promoting safe online behaviours. Future research should prioritise individualised educational approaches, address misconceptions, and focus on at-risk demographics. Additionally, global cyber-awareness solutions and experience-based policies are vital for a comprehensive approach.

5. Conclusions

This systematic literature review has highlighted the significant regional variations in cybersecurity awareness, which are heavily influenced by demographic factors. Older adults and individuals with limited digital literacy are particularly vulnerable, underscoring the need for targeted interventions and education programs to enhance their independence and connectivity [43]. Tailored educational initiatives are crucial for addressing limited digital skills in specific demographic groups, especially rural areas [44-46] The review also underscores the evolving nature of cybersecurity threats, such as caller ID spoofing, robocalls, and SMS phishing, which require continuous updates in public education and awareness campaigns [47]. Cybercriminals' use of these advanced tactics emphasises the importance of vigilance and informed public awareness. Effective education campaigns empower individuals to recognise and respond to these sophisticated threats.

Moreover, trust, risk perception, and social networks significantly influence an individual's ability to recognise and respond to cybersecurity threats. User susceptibility and behavior risk assessment are crucial for evaluating the effectiveness of cybersecurity awareness programs and policies. Urgent action is needed to implement awareness campaigns aimed at vulnerable groups like women and children, while policymakers and educators should factor in various elements to enhance cybersecurity education. Descriptive and statistical analyses show that participants' awareness of cybersecurity threats and risks increased after completing educational programs [48]. Despite technological progress, numerous users still do not possess essential cybersecurity knowledge, rendering them susceptible to cyberattacks [49]. Implementing gamification in cybersecurity education offers an engaging and effective tool to enhance users' knowledge and awareness [49].

Additionally, the intricacies of cyber risks necessitate the use of advanced algorithms. Fuzzy, Q-Learning and autonomous computing are proposed to ensure proactive policies can manage uncertainty and adapt to volatile situations [50]. This approach aims to address and mitigate cybersecurity threats effectively. The review highlights the importance of education, awareness, and robust cybersecurity measures in mitigating risks. Future efforts should include prioritising tailored educational strategies, leveraging innovative platforms and promoting safe online behaviours.

Comprehensive, global cyber-awareness solutions and experience-based policies are vital for building a resilient digital culture.

Acknowledgement

This research was not funded by any grant.

References

[1] Nzeakor, Ogochukwu Favour, Bonaventure N. Nwokeoma, and Peter-Jazzy Ezeh. "Pattern of cybercrime awareness in Imo state, Nigeria: An empirical assessment." *International Journal of Cyber Criminology* 14, no. 1 (2020): 283-299.

[2] Verma, Mudit Kumar, and Shyam Sundar Kushwaha. "Awareness towards cybercrime among secondary school students: The role of gender and school management." *Safer Communities* 20, no. 3 (2021): 150-158. https://doi.org/10.1108/SC-07-2020-0026

[3] Khan, Naurin Farooq, Naveed Ikram, and Sumera Saleem. "Effects of socioeconomic and digital inequalities on cybersecurity in a developing country." *Security Journal* (2023): 1-31. https://doi.org/10.1057/s41284-023-00375-4

[4] Adebayo, David Obafemi, Mohd Tajudin Ninggal, and Foluke Nike Bolu-Steve. "Relationship between demographic factors and undergraduates' cyberbullying experiences in public Universities in Malaysia." *International Journal of Instruction* 13, no. 1 (2020): 901-914. https://doi.org/10.29333/iji.2020.13158a

[5] Karagiannopoulos, Vasileios, Annie Kirby, Shakiba Oftadeh-Moghadam Ms, and Lisa Sugiura. "Cybercrime awareness and victimisation in individuals over 60 years: A Portsmouth case study." *Computer Law & Security Review* 43 (2021): 105615. https://doi.org/10.1016/j.clsr.2021.105615

[6] AL-Nuaimi, Maryam Nasser. "Human and contextual factors influencing cyber-security in organizations, and implications for higher education institutions: A systematic review." *Global Knowledge, Memory and Communication* 73, no. 1/2 (2024): 1-23. https://doi.org/10.1108/GKMC-12-2021-0209

[7] Aphane, Mmabatho P., and Jacob T. Mofokeng. "Critical Analysis of Strategies Towards Creating an Adequate Level of Awareness on Cybercrime among the Youth in Gauteng Province." *International Journal of Criminology and Sociology* 9 (2020): 1385-1396. https://doi.org/10.6000/1929-4409.2020.09.159

[8] Tarrad, Khalid Mukhlif, Hanen Al-Hareeri, Tawfeeq Alghazali, Mohammed Ahmed, Mohammed Kadhim Abbas Al-Maeeni, Ghadban Abdullah Kalaf, Refad E. Alsaddon, and Yaqeen S. Mezaal. "Cybercrime challenges in Iraqi Academia: creating digital awareness for preventing cybercrimes." *International Journal of Cyber Criminology* 16, no. 2 (2022): 15-31.

[9] Olofinbiyi, Sogo Angel. "Exploring youth awareness of cybercrime and factors engendering its proliferation in Nigeria." *African Renaissance* 18, no. 4 (2021): 319.

[10] Hadlington, Lee, and Sally Chivers. "Segmentation analysis of susceptibility to cybercrime: Exploring individual differences in information security awareness and personality factors." *Policing: A Journal of Policy and Practice* 14, no. 2 (2020): 479-492. https://doi.org/10.1093/police/pay027

[11] Alzubaidi, Abdulaziz. "Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia." *Heliyon* 7, no. 1 (2021). https://doi.org/10.1016/j.heliyon.2021.e06016

[12] Arpaci, Ibrahim, and Ersin Ateş. "Development of the cybercrime awareness scale (CAS): a validity and reliability study in a Turkish sample." *Online Information Review* 47, no. 4 (2023): 633-643. https://doi.org/10.1108/OIR-01-2022-0023

[13] Okoli, Chitu, and Kira Schabram. "A guide to conducting a systematic literature review of information systems research." *Sprouts: Working Papers on Information Systems* 10, no. 26 (2015). 1-49.

[14] Gusenbauer, Michael, and Neal R. Haddaway. "Which academic search systems are suitable for systematic reviews or meta-analyses? Evaluating retrieval qualities of Google Scholar, PubMed, and 26 other resources." *Research Synthesis Methods* 11, no. 2 (2020): 181-217. https://doi.org/10.1002/jrsm.1378

[15] Gusenbauer, Michael. "Google Scholar to overshadow them all? Comparing the sizes of 12 academic search engines and bibliographic databases." *Scientometrics* 118, no. 1 (2019): 177-214. https://doi.org/10.1007/s11192-018-2958-5

[16] Page, Matthew J., Joanne E. McKenzie, Patrick M. Bossuyt, Isabelle Boutron, Tammy C. Hoffmann, Cynthia D. Mulrow, Larissa Shamseer. "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews." *BMJ* (2021): 372. https://doi.org/10.1136/bmj.n71

[17] Keele, Staffs. *Guidelines for performing systematic literature reviews in software engineering*. 5. Technical Report, ver. 2.3 EBSE Technical Report. EBSE, 2007.

[18] Higgins, Julian PT, and Sally Green. "Cochrane handbook for systematic reviews of interventions. The Cochrane Collaboration." *London, UK* (2011).

[19] Balabantaray, Subhra Rajat, Mausumi Mishra, and Upananda Pani. "A sociological study of cybercrimes against women in india: Deciphering the causes and evaluating the impact on the victims." *International Journal of Asia-Pacific Studies* 19, no. 1 (2023). https://doi.org/10.21315/ijaps2023.19.1.2

[20] Garba, Jamilu. "An approach to cybercrime issues in Dandume Local Government area of Katsina State, Nigeria." *Nigerian Journal of Technology* 42, no. 2 (2023): 249-256. https://doi.org/10.4314/njt.v42i2.13

[21] Alharbi, Talal, and Asifa Tassaddiq. "Assessment of cybersecurity awareness among students of Majmaah University." *Big Data and Cognitive Computing* 5, no. 2 (2021): 23. https://doi.org/10.3390/bdcc5020023

[22] Shah, Pintu, and Anuja Agarwal. "Cyber Suraksha: A card game for smartphone security awareness." *Information & Computer Security* 31, no. 5 (2023): 576-600. https://doi.org/10.1108/ICS-05-2022-0087

[23] Arpaci, Ibrahim, and Omer Aslan. "Development of a scale to measure cybercrime-awareness on social media." *Journal of Computer Information Systems* 63, no. 3 (2023): 695-705. https://doi.org/10.1080/08874417.2022.2101160

[24] Conway, Georgia, and Lee Hadlington. "How do undergraduate students construct their view of cybercrime? Exploring definitions of cybercrime, perceptions of online risk and victimization." *Policing: A Journal of Policy and Practice* 15, no. 1 (2021): 119-129. https://doi.org/10.1093/police/pay098

[25] Mohammed, Maram., and Doaa M. Bamasoud. "The impact of enhancing awareness of cybersecurity on universities students: A survey paper." *Journal of Theoretical and Applied Information Technology* 100, no. 15 (2022): 4756-4766.

[26] Razaque, Abdul, Abrar Al Ajlan, Noussaiba Melaoune, Munif Alotaibi, Bandar Alotaibi, Issabekov Dias, Ammar Oad, Salim Hariri, and Chenglin Zhao. "Avoidance of cybersecurity threats with the deployment of a web-based blockchain-enabled cybersecurity awareness system." *Applied Sciences* 11, no. 17 (2021): 7880. https://doi.org/10.3390/app11177880

[27] Rawindaran, Nisha, Ambikesh Jayal, and Edmond Prakash. "Exploration of the impact of cybersecurity awareness on small and medium enterprises (SMEs) in Wales using intelligent software to combat cybercrime." *Computers* 11, no. 12 (2022): 174. https://doi.org/10.3390/computers11120174

[28] Sagheer, Nadia, Kanwal Iqbal Khan, Samar Fahd, Shahid Mahmood, Tayyiba Rashid, and Hassan Jamil. "Factors affecting adaptability of cryptocurrency: An application of technology acceptance model." *Frontiers in Psychology* 13 (2022): 903473. https://doi.org/10.3389/fpsyg.2022.903473

[29] Tin, Ting Tin, Khiew Jie Xin, Ali Aitizaz, Lee Kuok Tiung, Teoh Chong Keat, and Hasan Sarwar. "Machine learning based predictive modelling of cybersecurity threats utilising behavioural data." *International Journal of Advanced Computer Science and Applications* 14, no. 9 (2023). https://doi.org/10.14569/IJACSA.2023.0140987

[30] Ridho, Wahyu Fahrul. "Unmasking online fake job group financial scams: a thematic examination of victim exploitation from perspective of financial behavior." *Journal of Financial Crime* 31, no. 3 (2024): 748-758. https://doi.org/10.1108/JFC-05-2023-0124

[31] Datt, Gopal, and Naveen Tewari. "A Study of Computer Users' Attitude and Awareness towards Cyber Security." *International Journal of Computer Information Systems and Industrial Management Applications* 13 (2021): 8-8.

[32] Ayyoub, Hani Y., Ahmad A. AlAhmad, Amani Al-Serhan, Mohammad F. Al-Abdallat, Hadeel Boshmaf, Yasmeen A. Abu-Taleb, Yarob O. Alqudah, and Yazan Alshamaileh. "Awareness of electronic crimes related to E-learning among students at the University of Jordan." *Heliyon* 8, no. 10 (2022). https://doi.org/10.1016/j.heliyon.2022.e10897

[33] Mai, Phuong Thao, and Andrea Tick. "Cyber Security Awareness and behavior of youth in smartphone usage: A comparative study between university students in Hungary and Vietnam." *Acta Polytechnica Hungarica* 18, no. 8 (2021): 67-89. https://doi.org/10.12700/APH.18.8.2021.8.4

[34] Lee, Claire Seungeun, and Ji Hye Kim. "How victims perceive fear of cybercrime: Importance of informed risk." *Criminal Justice Studies* 36, no. 3 (2023): 206-227. https://doi.org/10.1080/1478601X.2023.2254099

[35] Althibyani, Hosam A., and Abdulrahman M. Al-Zahrani. "Investigating the effect of students' knowledge, beliefs, and digital citizenship skills on the prevention of cybercrime." *Sustainability* 15, no. 15 (2023): 11512. https://doi.org/10.3390/su151511512

[36] Wahab, Ernawati Abdul, Muhammad Adnan Pitchan, and A. Salman. "Knowledge, attitude and practice society in Kuala Lumpur against online fraud crime prevention campaign [Pengetahuan, sikap dan amalan masyarakat di Kuala Lumpur terhadap kempen pencegahan jenayah penipuan dalam talian]." *Jurnal Komunikasi: Malaysian Journal of Communication* (2023). https://doi.org/10.17576/JKMJC-2023-3901-14

[37] Pitchan, Muhammad Adnan, Mohamad Adli Baco, Fauziah Hassan, and Akmar Hayati Ahmad Ghazali. "Pengetahuan, sikap, amalan terhadap privasi maklumat & keselamatan pembelian barangan dalam talian oleh

golongan belia." *Jurnal Komunikasi: Malaysian Journal of Communication* 38, no. 4 (2022): 250-267 https://doi.org/10.17576/JKMJC-2022-3804-14.

[38] De Kimpe, Lies, Michel Walrave, Thom Snaphaan, Lieven Pauwels, Wim Hardyns, and Koen Ponnet. "Research note: An investigation of cybercrime victims' reporting behavior." *European Journal of Crime, Criminal Law and Criminal Justice* 29, no. 1 (2021): 66-78. https://doi.org/10.1163/15718174-bja10019

[39] Fissel, Erica R., and Jin R. Lee. "The cybercrime illusion: Examining the impact of cybercrime misbeliefs on perceptions of cybercrime seriousness." *Journal of Criminology* 56, no. 2-3 (2023): 150-169. https://doi.org/10.1177/26338076231174639

[40] Lee, Claire Seungeun, and Yi Ting Chua. "The role of cybersecurity knowledge and awareness in cybersecurity intention and behavior in the United States." *Crime & Delinquency* 70, no. 9 (2024): 2250-2277. https://doi.org/10.1177/00111287231180093

[41] Ismail, Safinah, Aemy Elyani Mat Zain, Haslina Ibrahim, Nazneen Ismail, Nur Aisyah Abu Hassan, and Fatin Farzana Dass Meral. "Kepentingan aplikasi digital dalam pembelajaran anak muda era industri 4.0: the importance of digital applications in young children's learning industry era 4.0." *Semarak International Journal of STEM Education* 1, no. 1 (2024): 28-38. https://doi.org/10.37934/sijste.1.1.2838

[42] Veza, Ibham, Mohd Farid Muhamad Said, Tri Widodo Besar Riyadi, Mohd Azman Abas, and Zulkarnain Abdul Latiff. "Issues in the Science and Engineering Education in Indonesia: How to improve competitiveness through STEM mastery." *International Journal of Advanced Research in Future Ready Learning and Education* 24, no. 1 (2021): 1-6. https://doi.org/10.37934/frle.24.1.16

[43] Xu, Wei, and Shujie Zheng. "Childhood emotional abuse and cyberbullying perpetration among Chinese university students: The chain mediating effects of self-esteem and problematic social media use." *Frontiers in psychology* 13 (2022): 1036128. https://doi.org/10.3389/fpsyg.2022.1036128

[44] Ang, Amberyce. "Help through digital platforms in a time of distanced connectivity-application for older adults, people with intellectual disabilities and individuals with depression." *Psychiatry* 1 (2021): 18-24. https://doi.org/10.46619/psy.2021.1.1004

[45] Cheng, Hao, Keyi Lyu, Jiacheng Li, and Hoiyan Shiu. "Bridging the digital divide for rural older adults by family intergenerational learning: A classroom case in a rural primary school in china." *International Journal of Environmental Research And Public Health* 19, no. 1 (2021): 371. https://doi.org/10.3390/ijerph19010371

[46] Liu, Siqi, Hongyan Zhao, Jingjing Fu, Dehui Kong, Zhu Zhong, Yan Hong, Jing Tan, and Yu Luo. "Current status and influencing factors of digital health literacy among community-dwelling older adults in Southwest China: A cross-sectional study." *BMC Public Health* 22, no. 1 (2022): 996. https://doi.org/10.1186/s12889-022-13378-4

[47] Gupta, Payas, Bharat Srinivasan, Vijay Balasubramaniyan, and Mustaque Ahamad. "Phoneypot: Data-driven understanding of telephony threats." In *NDSS*, 107, p. 108. 2015. https://doi.org/10.14722/ndss.2015.23176

[48] Jalil, Masita, Noraida Hj Ali, Farizah Yunus, Fakhrul Adli Mohd Zaki, Lee Hwee Hsiung, and Mohammed Amin Almaayah. "Cybersecurity Awareness among Secondary School Students Post Covid-19 Pandemic." *Journal of Advanced Research in Applied Sciences and Engineering Technology* 37, no. 1 (2024): 115-127. https://doi.org/10.37934/araset.37.1.115127

[49] Rose, Nurul Naimah, Aida Shakila Ishak, Nor Fazira Zakaria, and Mohd Yusri Mustafa. "Case study of cyberbully among effeminate male students in public university." In *Journal of Physics: Conference Series*, 1529, no. 3, p. 032016. IOP Publishing, 2020. https://doi.org/10.1088/1742-6596/1529/3/032016

[50] Ramli, Ahmad Kamal. "An active cyber insurance policy against cybersecurity risks using fuzzy Q-learning." *Journal of Advanced Research in Applied Sciences and Engineering Technology* 30, no. 3 (2023): 212-221. https://doi.org/10.37934/araset.30.3.212221