International Journal of Multidisciplinary Research and Publications
ISSN (Online): 2581-6187

Social Environmental Factors Influencing Cybersecurity Awareness and Behaviour: A Study of Higher Education Institutions in Nantong City, Jiangsu Province, China

Zhaopeng Hu[1,2,*], Md Gapar Md Johar[3,*], Jacquline Tham[2]
[1]School of Information Engineering, Nantong Institute of Technology, Nantong, China
[2]School of Graduate Studies, Postgraduate Centre, Management and Science University, Shah Alam, Selangor, Malaysia
[3]Software Engineering and Digital Innovation Center, Management and Science University, Shah Alam, Selangor, Malaysia
Email address: huzhaopeng88@sina.com

***Abstract*—*With the continuous development of computer and network technology, an increasing number of cybersecurity issues have become increasingly prominent. As the primary user group of the internet, students in higher education institutions often lack strong cybersecurity awareness due to the influence of the social environment. The majority of students exhibit unsafe cybersecurity behaviours in their daily lives, making them vulnerable to various cyber threats. As one of the major educational cities in Jiangsu Province, China, Nantong City is home to nine higher education institutions. Studying the social environmental factors influencing the cybersecurity awareness and behaviours of students in Nantong's higher education institutions holds significant representativeness and practical significance. This study aims to explore the social environment factors influencing students' cybersecurity awareness in Higher Education Institutions, as these factors indirectly impact their cybersecurity behaviour. We will collect data through a questionnaire survey and discuss the expected contributions and impacts*.

***Keywords*—** *Cybersecurity, Cybersecurity Awareness, Cybersecurity Behaviour, Higher Education Institution*.

I. INTRODUCTION

In the 1990s, the internet entered people's lives (Ergen et al., 2021). Due to the ease of accessing information through globally interconnected networks, the internet has enabled anyone, regardless of their location, to launch attacks on information systems and personal information. As the number of internet users continues to grow, cybersecurity has become a critical issue for many countries (Tosun et al., 2020), with various cyber threats increasing in frequency (Admass et al., 2024). China, which accounts for one-fifth of the world's internet users, faces significant cybersecurity challenges (Zwilling et al., 2022). In higher education institutions, students are active internet users (Garba et al., 2020). Therefore, students in higher education institutions are an important group that requires special attention regarding cybersecurity awareness and behaviour (Alzahrani, 2021). Prolonged internet use may expose university students to cyber risks and threats, making them vulnerable (Garba et al., 2020) . Due to a lack of cybersecurity awareness and knowledge of how to protect themselves online (Yildirim & Erendor, 2024), students in higher education institutions are more susceptible to these threats (Taha & Dahabiyeh, 2021). Strengthening cybersecurity awareness and behaviour is of utmost importance (Hu, 2024).

Although numerous researchers have investigated the factors influencing cybersecurity awareness and behaviour in higher education institutions (Mohammed et al., 2022; Alqahtani, 2022; Eltahir & Ahmed, 2023; Ahamed et al., 2024). However, there has been limited in-depth research on the social environment factors influencing students' cybersecurity awareness and behaviour in higher education institutions, particularly in Nantong City, Jiangsu Province, China. As one of Jiangsu Province's leading education cities, Nantong boasts a well-developed education system and rapid growth in higher education scale. According to official statistics from Nantong City, as of the end of 2024, there were nine general higher education institutions in Nantong City (Nantong Municipal Government, 2024). Selecting Nantong as the research location allows for the inclusion of students from various types of higher education institutions, such as undergraduate, vocational, and private institutions, facilitating the analysis of the differences in cybersecurity awareness and behaviour among students from different types of higher education institutions. Currently, higher education in Nantong is still in a phase of rapid expansion, with growing demand for cybersecurity education. Therefore, studying the cybersecurity awareness and behaviour of students in higher education institutions in Nantong City, Jiangsu Province, holds significant representativeness and practical significance. To explore the social environmental factors influencing the cybersecurity awareness and behaviour of students in higher education institutions, this study proposes a more comprehensive framework for a more thorough analysis of social environmental factors.

This thesis is a study of higher education institutions in Nantong City, Jiangsu Province, China. The study is organised as follows: the first section provides an introduction; the second section reviews relevant literature; the third section proposes hypotheses and presents a conceptual framework; the fourth section describes the research methods and data

Zhaopeng Hu, Md Gapar Md Johar, and Jacquline Tham, "Social Environmental Factors influencing Cybersecurity Awareness and Behaviour: A study of Higher Education Institutions in Nantong City, Jiangsu Province, China," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 8, Issue 3, pp. 62-67, 2025.

collection; and the final section discusses the expected contributions and implications of this study, which will fill a gap in the field of cybersecurity awareness and behaviour among students in higher education institutions in Nantong City, Jiangsu Province, China.

II. Problem Statements

Existing research indicates that the lack of cybersecurity awareness and behaviour is largely attributable to the absence of social environment factors (Simonet & Teufel, 2019). Social media enhances cybersecurity awareness and behaviour through social influence and other means. This social influence may originate from peer influence (Boyd & Ellison, 2007; Elrayah & Jamil, 2023). When faced with cybersecurity threats, people often develop negative emotions toward others, including peers. Currently, there is limited literature on how peer behaviour influences cybersecurity awareness and behaviour (Almansoori et al., 2023). Therefore, this study aims to conduct further research to enhance cybersecurity awareness and behaviour among students at Higher Education Institutions in Nantong, thereby addressing gaps in this field.

Users are more likely to take action when there is a lack of training and media coverage, but this is not always the case (Toukabri, 2024). A lack of understanding of the cue to action in cybersecurity may lead end-users to engage in inappropriate cybersecurity behaviours (Cain et al., 2018). Existing research has limited exploration of action cue factors in cybersecurity awareness and behaviour among students in Higher Education Institutions, and this study can further address this gap.

Various cyber threats and attacks exist on social media, such as social phishing and identity theft (Zhang & Gupta, 2018). Most people use social media to share their thoughts, emotions, and experiences, but a lack of cybersecurity awareness may prevent them from considering related cybersecurity issues (Herath et al., 2022). Therefore, this thesis will conduct further research on social media usage to enhance cybersecurity awareness and behaviour among students at Higher Education Institutions in Nantong.

III. Literature Review

The International Telecommunication Union (ITU) defines Cybersecurity as a set of security concepts, policies, tools, guidelines, security assurances, and best practices that can be used to protect an organization's assets, users, and network environment (Quayyum et al., 2021). Cybersecurity awareness, also known as information security awareness, refers to the extent to which users perceive and understand cyber risks (such as phishing, malware, etc.) and pay attention to security protection behaviors (such as security settings, etc.) (Drogkaris & Bourka, 2019; Nurse, 2021). The majority of students (98%) believe that setting security features on social media has positive significance. Emphasizing the setup of security features can enhance protection against cyberattacks and make them feel safer.

As early as 1975, concerns about information system security in university environments began to emerge (Kerievsky, 1976). Among various groups, students in Higher Education Institutions constitute a particularly important demographic, and their Cybersecurity awareness warrants special attention (Alzahrani, 2021). Therefore, enhancing Cybersecurity awareness among university students to regulate their Cybersecurity behavior is of utmost importance (Garba et al., 2022). Some studies have systematically explored social media from the perspective of cybersecurity awareness and behaviour (Alsharida et al., 2023). According to existing research, the lack of cybersecurity awareness and behaviour is largely due to social environmental factors (Simonet & Teufel, 2019).Most students (98%) believe that setting up security features on social media has positive significance. Emphasizing the design of security features can enhance protection against cyberattacks and make them feel secure. However, 6% of students believe that setting up security features on social media has some drawbacks (Sales et al., 2024).

Alqahtani (2022) conducted a study on university students in Saudi Arabia to explore the factors influencing college students' cybersecurity awareness. The study found that students avoid excessive dissemination of personal information on social media and know how to report suspicious threats on social media. Social media usage significantly influences cybersecurity awareness. Other researchers have also reached similar conclusions, such as Mburaimoh et al. (2025) surveyed 1,000 social media users, indicating that social media use is a useful tool for enhancing Cybersecurity awareness and promoting safe online behavior. However, social media use also poses certain security risks. Herath et al. (2022) explicitly highlighted the severity of cyberattacks targeting social media users and the inadequacy of existing technical solutions. The study also emphasized that Cybersecurity behavior and awareness are critical for safeguarding information security. Almansoori et al. (2023) conducted a further in-depth analysis of 39 studies published between 2012 and 2021, with the main finding that Cybersecurity behavior depends on social factors. Appropriate Cybersecurity behavior by social media users is crucial for protecting privacy. Additionally, the study pointed out that peer behavior and cue to action are also major factors influencing Cybersecurity behavior. It suggested that future research should place greater emphasis on social factors.

Simonet & Teufel (2019) found that family members or friends (i.e., peer behavior) can enhance the social learning process of cybersecurity issues through storytelling, thereby influencing their cybersecurity awareness. Information provided by public administrative departments or reports published by mass media (i.e., cue to action) can emphasize the importance of Cybersecurity and promote individual Cybersecurity awareness. Hadee (2022) conducted a quantitative survey and provided a suitable conceptual framework for studying Cybersecurity behavior. The results indicated that cue to action influences Cybersecurity awareness and behavior. Toukabri (2024) investigated students' awareness of information-related threats. It was found that cue to action is a factor that encourages individuals to take action. For example, news reports, etc. In the context of information security, this variable is considered a trigger or promoter of Cybersecurity behavior.

Zhaopeng Hu, Md Gapar Md Johar, and Jacquline Tham, "Social Environmental Factors influencing Cybersecurity Awareness and Behaviour: A study of Higher Education Institutions in Nantong City, Jiangsu Province, China," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 8, Issue 3, pp. 62-67, 2025.

In summary, it is necessary to study the impact of social environment factors (social media use, peer behavior, and cue to action) on cybersecurity awareness and behavior among students in Higher Education Institutions. However, current research has not yet integrated these variables. This paper aims to build upon previous research by developing a comprehensive conceptual framework that takes into account the influence of social environment factors on cybersecurity awareness and behavior among students in Higher Education Institution. The paper seeks to assist other researchers in understanding the anticipated outcomes and the underlying causes within the Higher Education Institution context.

IV. Conceptual Framework and Hypotheses

The connection between the study question and more general theoretical ideas must be shown in any research. The relevance of the study is highlighted when the links between the variables are clarified, which improves our comprehension of the research issue. The goal of this research is to examine how social environmental variables affect students' knowledge and behavior related to cybersecurity in higher education institutions in Nantong City, Jiangsu Province, China. Among these, social environmental factors are divided into three parts: social media use, peer behaviour, and cue to action. Social media use refers to the platforms used by internet users to create electronic networks, primarily for communication, sharing daily life experiences, and mutual interaction (Bhatnagar & Pry, 2020). Peer behaviour is used to measure users' beliefs about their friends' safety behaviours (Herath & Rao, 2009). Cue to action refers to users being aware of certain triggers or cue to action that prompt them to take normative actions (Ng et al., 2009). Furthermore, cybersecurity behavior serves as the dependent variable, with cybersecurity awareness acting as the intervening variable. By integrating these variables, a novel conceptual framework is presented that addresses gaps in the current literature on the social environment variables that affect cybersecurity knowledge and conduct.

Some researchers have studied social media use (Alqahtani, 2022; Mburaimoh et al., 2025). Due to a lack of Cybersecurity awareness, posting less sensitive data on social media may lead to privacy breaches (Herath et al., 2022). Social media use is widespread among university students, with both benefits and drawbacks (Singh et al., 2020). Excessive social media use can impair cybersecurity awareness, thereby exposing users to cyber threats (Alsmadi et al., 2024). Based on existing literature evidence, the hypothesis holds.

H_1: There is a correlation between Social Media Use and Cybersecurity Awareness.

Cue to action (Kamarulzaman et al., 2022) influences information security awareness through external environmental factors, which in turn affect security behaviour. Information provided by public administrative departments or reports published by mass media (i.e., cue to action) can emphasise the importance of Cybersecurity and promote individual Cybersecurity awareness (Simonet & Teufel, 2019). Additionally, schools can enhance students' Cybersecurity awareness by sending security notifications and implementing measures (Du et al., 2024). Based on existing literature evidence, the hypothesis is established.

H_2: There is a correlation between Cues to Action and Cybersecurity Awareness.

Some researchers have shown that peer behaviour, as a variable measuring the level of trust in the safety of one's friends, influences Cybersecurity awareness (Fait et al., 2020; Snyma & Kruger, 2020). If peers encourage the adoption of Cybersecurity behaviours to ensure their own Cybersecurity, this can have a positive impact on the willingness to engage in Cybersecurity behaviours (Alanazi et al., 2022). However, some literature also suggests that peer pressure may lead individuals to participate in cyberattacks (Bleize et al., 2021). Therefore, peer behaviour influences Cybersecurity awareness. Based on existing literature evidence, the hypothesis holds.

H_3: There is a correlation between Peer Behaviour and Cybersecurity Awareness.

Several studies have identified the relationship between cybersecurity awareness and behaviour (Nilupú-Moreno, 2024; Bognár & Bottyán, 2024). Numerous studies support the notion that cybersecurity awareness influences cybersecurity behaviour. Research findings indicate that the stronger the cybersecurity awareness, the fewer the number of cyber threats (Schilder et al., 2016; Herath et al., 2022). A lack of understanding of cybersecurity actions may lead to the adoption of inappropriate cybersecurity behaviours. On the other hand, cybersecurity awareness campaigns have failed to successfully change people's behaviours (Chang & Coppel, 2020). Sharma et al. (2022) observed that cybersecurity awareness promotes people to take proactive cybersecurity actions and impacts their cybersecurity behavior.

H_4: There is a correlation between Cybersecurity Awareness and Cybersecurity Behaviour.

Based on the above assumptions, we propose a comprehensive conceptual framework of the influence of social environment factors on cybersecurity awareness and behaviour, as shown in Figure 1.

V. Research Methodology

To test the aforementioned conceptual framework and related hypotheses, we will conduct a study at higher education institutions in Nantong City, Jiangsu Province, China. This study employs quantitative research methods, collecting data through questionnaires. These data can be measured, processed, and analysed using statistical tools to determine the correlations between variables, with the statistical results serving as the final conclusions of this study. The independent variables in this study are social media usage, cue to action, and peer behaviour, the dependent variable is Cybersecurity behaviour, and the mediating variable is Cybersecurity awareness. We will address the following research questions in this study:

To what extent does investigating the social media use of students in higher education institutions in Nantong influence cybersecurity awareness and behaviours?

Zhaopeng Hu, Md Gapar Md Johar, and Jacquline Tham, "Social Environmental Factors influencing Cybersecurity Awareness and Behaviour: A study of Higher Education Institutions in Nantong City, Jiangsu Province, China," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 8, Issue 3, pp. 62-67, 2025.

To what extent does investigating the cues to action of students in higher education institutions in Nantong influence cybersecurity awareness and behaviours?

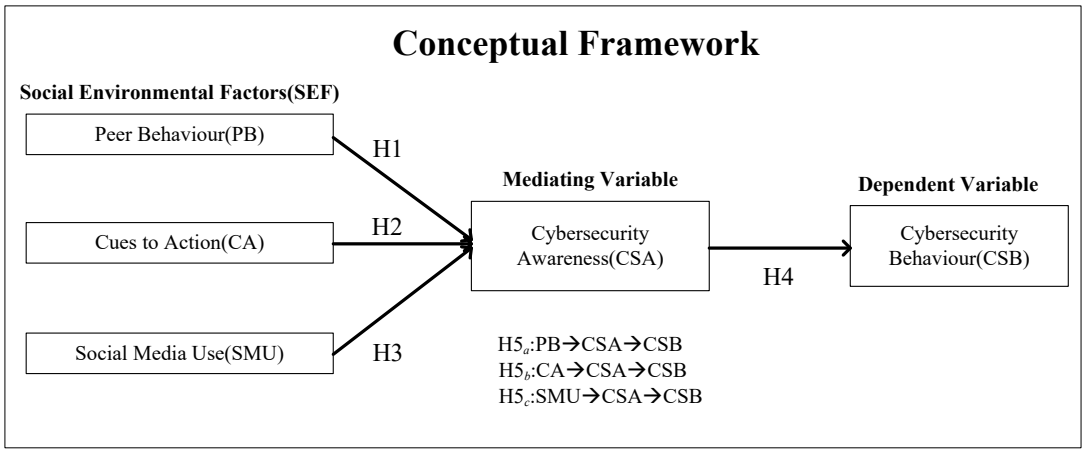

Figure 1. Conceptual Framework

To what extent does investigating the peer behaviours of students in higher education institutions in Nantong g influence cybersecurity awareness and behaviours?

The Likert scale is widely used in social science research (Robinson, 2024). This study employed a five-point Likert scale to measure unobservable constructs, where 1 = strongly disagree, 2 = disagree, 3 = neutral (neither agree nor disagree), 4 = agree, and 5 = strongly agree (Zahid, 2024). Additionally, items phrased in the negative are acceptable in the literature. However, researchers prefer to use affirmative statements rather than negative statements (Younas & Porr, 2023). Therefore, during the questionnaire development process in this study, affirmative statements were chosen whenever possible to construct the items. As shown in Table 1, these are some of the questionnaire items.

TABLE 1. some of the questionnaire items

No.	Items	Source
SMU	I know how to report any risks or threats (such as harassment or bullying) that I face when using social media.	(Alrobaian et al., 2023)
CA	Mass media reports influence me to practice a safe cyber behaviour.	(Simonet & Teufel, 2019)
PB	My friends would approve of me practicing a safe cyber behaviour.	(Simonet & Teufel, 2019)
CSA	I keep myself informed and updated on cybersecurity threats and cybersecurity awareness best practices.	(Yusuf, 2024)
CSB	I update the software that I use.	(Bognár & Bottyán, 2024)

A. Data collection

To ensure the validity of the data, the sources of information and data collection methods are particularly important (Sekaran & Bougie, 2016). This study will collect raw data through a closed-ended self-administered questionnaire (Jayachandrababu et al., 2023). Since there are nine higher education institutions in Nantong, stratified sampling will be conducted from each institution based on the proportion of students, resulting in a total sample of 400 students. A carefully designed online questionnaire will be developed to collect raw data related to social environmental factors (social media use, cue to action, and peer behaviour) as well as cybersecurity awareness and behaviour. The questionnaire will be distributed to students via the Questionnaire Star platform for completion.

B. Data analysis and evaluation Hypothesis testing

The raw data collected from the questionnaire can be analysed using big data analysis software, such as SPSS. All respondents' answers to the questionnaire must be entered into the database columns in order, which is referred to as data entry. After data entry, the data is reviewed, filtered, and edited. In data analysis, structured models are typically used, which are generally divided into four parts: i) Data coding (Babbie & Mouton, 2005): This involves reviewing the collected data after it has been coded, prepared, and screened, with the aim of measuring and constructing items; ii) Exploratory factor analysis (EFA) and reliability testing (used to measure items and structures) are employed to determine the number of factors and models (Finch, 2019); iii) Confirmatory factor analysis (CFA) is used to validate the structural validity of the constructed items, where the validity and reliability of the measurements are tested through confirmatory factor analysis (Brown & Moore, 2012); iv) Hypothesis testing is conducted using structural equation modelling (SEM) (Mburu, 2014).

H_1, H_2, and H_3 are the factors influencing cybersecurity awareness. A statistical significance level of 0.05 is used to test whether each factor significantly influences cybersecurity awareness. H_4 is the hypothesis regarding the relationship between cybersecurity awareness and cybersecurity behaviour, and similar analyses will be used to test this hypothesis.

VI. EXPECTED CONTRIBUTIONS

This study aims to conduct an empirical investigation into the social environmental factors influencing cybersecurity awareness in higher education institutions in Nantong City, Jiangsu Province, China, by proposing a comprehensive conceptual framework that integrates the impact of social

Zhaopeng Hu, Md Gapar Md Johar, and Jacquline Tham, "Social Environmental Factors influencing Cybersecurity Awareness and Behaviour: A study of Higher Education Institutions in Nantong City, Jiangsu Province, China," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 8, Issue 3, pp. 62-67, 2025.

environmental factors on cybersecurity awareness and behaviour. This study has two main contributions: first, it will be applied to Nantong City, Jiangsu Province, China, aiming to fill the gap in this region and contribute to the field of cybersecurity for students in higher education institutions in Nantong City. Second, through this study, it is possible to enhance cybersecurity awareness among students in higher education institutions in Nantong City, improve cybersecurity behaviour, and reduce cybersecurity risks.

REFERENCES

[1]. Admass, W. S., Munaye, Y. Y., & Diro, A. A. (2024). Cyber security: State of the art, challenges and future directions. *Cyber Security and Applications*, *2*, 100031.

[2]. Ahamed, B., Polas, M. R. H., Kabir, A. I., Sohel-Uz-Zaman, A. S. M., Fahad, A. A., Chowdhury, S., & Rani Dey, M. (2024). Empowering Students for Cybersecurity Awareness Management in the Emerging Digital Era: The Role of Cybersecurity Attitude in the 4.0 Industrial Revolution Era. SAGE Open, 14(1), 21582440241228920.

[3]. Alanazi, M., Freeman, M., & Tootell, H. (2022). Exploring the factors that influence the cybersecurity behaviors of young adults. Computers in Human Behavior, 136, 107376.

[4]. Almansoori, A., Al-Emran, M., & Shaalan, K. (2023). Exploring the frontiers of cybersecurity behavior: A systematic review of studies and theories. Applied Sciences, 13(9), 5700.

[5]. Alqahtani, M. A. (2022). Factors affecting cybersecurity awareness among university students. *Applied Sciences*, *12*(5), 2589.

[6]. Alrobaian, S., Alshahrani, S., & Almaleh, A. (2023). Cybersecurity awareness assessment among trainees of the technical and vocational training corporation. *Big Data and Cognitive Computing*, *7*(2), 73.

[7]. Alsharida, R. A., Al-rimy, B. A. S., Al-Emran, M., & Zainal, A. (2023). A systematic review of multi perspectives on human Cybersecurity Behaviour. Technology in Society, 102258.

[8]. Alsmadi, D., Maqousi, A., & Abuhussein, T. (2024). Engaging in cybersecurity proactive Behaviour: awareness in COVID-19 age. Kybernetes, 53(1), 451-466.

[9]. Alzahrani, L. (2021). Statistical analysis of Cybersecurity Awareness issues in higher education institutes. International Journal of Advanced Computer Science and Applications, 12(11).

[10]. Babbie, E., & Mouton, J. (2005). Qualitative studies. The practice of social research.

[11]. Bhatnagar, N., & Pry, M. (2020). Student Attitudes, Awareness, and Perceptions of Personal Privacy and Cybersecurity in the Use of Social Media: An Initial Study. *Information Systems Education Journal*, *18*(1), 48-58.

[12]. Bleize, D. N., Tanis, M., Anschütz, D. J., & Buijzen, M. (2021). A social identity perspective on conformity to cyber aggression among early adolescents on WhatsApp. *Social Development*, *30*(4), 941-956.

[13]. Bognár, L., & Bottyán, L. (2024). Evaluating online security behavior: Development and validation of a personal cybersecurity awareness scale for university students. *Education Sciences*, *14*(6), 588.

[14]. Boyd, D. M., & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. *Journal of computer-mediated Communication*, *13*(1), 210-230.

[15]. Brown, T. A., & Moore, M. T. (2012). Confirmatory factor analysis. Handbook of structural equation modeling, 361, 379.

[16]. Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of information security and applications*, *42*, 36-45.

[17]. Chang, L. Y., & Coppel, N. (2020). Building cyber security awareness in a developing country: Lessons from Myanmar. *Computers & Security*, *97*, 101959.

[18]. Drogkaris, P., & Bourka, A. (2019). Cybersecurity culture guidelines: Behavioural aspects of cybersecurity. *European Union Agency for Network and Information Security (ENISA)*.

[19]. Du, J., Kalafut, A., & Schymik, G. (2024). The health belief model and phishing: determinants of preventative security behaviors. *Journal of Cybersecurity*, *10*(1), tyae012.

[20]. Elrayah, M., & Jamil, S. (2023). Impact of digital literacy and online privacy concerns on cybersecurity behaviour: The moderating role of cybersecurity awareness. *International Journal of Cyber Criminology*, *17*(2), 166-187.

[21]. Eltahir, M. E., & Ahmed, O. S. (2023). Cybersecurity awareness in African higher education institutions: A case study of Sudan. *Inf. Sci. Lett*, *12*(1), 171-183.

[22]. Ergen, A., Ünal, A. N., & Saygili, M. S. (2021). Is it possible to change the Cybersecurity Behaviours of employees? Barriers and promoters. Academic Journal of Interdisciplinary Studies, 10(4), 210.

[23]. Faith, B. F., Hamid, S., Norman, A., Johnson, O. F., & Eke, C. I. (2020, March). Relating factors of tertiary institution students' Cybersecurity Behaviour. In 2020 International Conference in Mathematics, Computer Engineering and Computer Science (ICMCECS) (pp. 1-6). IEEE.

[24]. Finch, W. H. (2019). Exploratory factor analysis (Vol. 182). Sage Publications.

[25]. Garba, A. A., Siraj, M. M., Othman, S. H., & Musa, M. A. (2020). A study on Cybersecurity Awareness among students in Yobe State University, Nigeria: A quantitative approach. Int. J. Emerg. Technol, 11(5), 41-49.

[26]. Hadee, A. N. A. (2022). The Adoption of Cybersecurity: An Analysis of Maldivian Internet Users' Behaviour Using the Health Belief Model.

[27]. Herath, T. B., Khanna, P., & Ahmed, M. (2022). Cybersecurity practices for social media users: a systematic literature review. *Journal of Cybersecurity and Privacy*, *2*(1), 1-18.

[28]. Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. European Journal of information systems, 18, 106-125.

[29]. Hu Dongxue. (2024). Survey research on the status quo of college students' awareness of network security--taking a college in Jilin as an example. International PR (17), 164-166. https://doi.org/10.16645/j.cnki.cn11-5281/c.2024.17.059.

[30]. Jayachandrababu, B., Sekhar, M. V., Gorantla, N. C., Kumar, N. R., & Burli, K. (2023). Assessing the knowledge, attitudes, and practices of undergraduate medical students regarding pharmacovigilance: a questionnaire-based study conducted at a tertiary care teaching hospital.

[31]. Kamarulzaman, M. S., Shuhidan, S. M., & Toha, A. J. (2022). Factors That Influence Information Security Behaviour of Home User. EDUCATUM Journal of Science, Mathematics and Technology, 9(2), 129-135.

[32]. Kerievsky, B. (1976). Security and confidentiality in a university computer network. *ACM SIGUCCS Newsletter*, *6*(3), 9-11.

[33]. Mburaimoh, M. M., & Samuel, K. A. (2025). The impact of social media on cybersecurity awareness. *UNIZIK Journal of Engineering and Applied Sciences*, *5*(2), 2587-2604.

[34]. Mburu, H. (2014). Application of Structural Equation Modeling in Hypothesis Testing. Mburu, HK (2014). Application of structural equation modeling in hypothesis testing. International Journal of Business and Public Management, 3(1).

[35]. Mohammed, M. A. R. A. M., & Bamasoud, D. M. (2022). The impact of enhancing awareness of cybersecurity on universities students: A survey paper. *Journal of Theoretical and Applied Information Technology*, *100*(15), 4756-4766.

[36]. Nantong Municipal Government(NMG).(2024), Number of college students enrolled in 9 colleges and universities in Nantong in 2024.https://www.nantong.gov.cn.

[37]. Ng, B. Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, *46*(4), 815-825.

[38]. Nilupú-Moreno, K., Salas-Riega, J. L., Ninaquispe-Soto, M., & Riega-Virú, Y. (2024). Cybersecurity in university students: A systematic review of the literature. In *International conference on WorldS4* (pp. 315-332). Springer, Singapore.

[39]. Nurse, J. R. (2021). Cybersecurity awareness. In *Encyclopedia of Cryptography, Security and Privacy* (pp. 1-4). Berlin, Heidelberg: Springer Berlin Heidelberg.

[40]. Quayyum, F., Cruzes, D. S., & Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction*, *30*, 100343.

[41]. Robinson, J. (2024). Likert scale. In Encyclopedia of quality of life and well-being research (pp. 3917-3918). Cham: Springer International Publishing.

[42]. Sales, J. N., Tiongco, R., Lu, S., Ruiz, M. J., Cruz, J., & Prudente, M. (2024). Personal Privacy and Cyber Security: Student Attitudes,

Awareness, and Perception on the Use of Social Media: Student Attitudes, Awareness, and Perception on the Use of Social Media. International Journal of Curriculum and Instruction, 16(1), 175-190.
[43]. Schilder, J. D., Brusselaers, M. B., & Bogaerts, S. (2016). The effectiveness of an intervention to promote awareness and reduce online risk Behaviour in early adolescence. Journal of youth and adolescence, 45, 286-300.
[44]. Sekaran, U., & Bougie, R. (2016). *Research methods for business: A skill building approach*. john wiley & sons.
[45]. Sharma, S., Kar, A. K., Gupta, M. P., Dwivedi, Y. K., & Janssen, M. (2022). Digital citizen empowerment: A systematic literature review of theories and development models. *Information Technology for Development*, *28*(4), 660-687.
[46]. Simonet, J., & Teufel, S. (2019, June). The influence of organizational, social and personal factors on cybersecurity awareness and behavior of home computer users. In IFIP international conference on ICT systems security and privacy protection (pp. 194-208). Cham: Springer International Publishing.
[47]. Singh, M., Verma, C., & Juneja, P. (2020, December). Social media security threats investigation and mitigation methods: A preliminary review. In Journal of Physics: Conference Series (Vol. 1706, No. 1, p. 012142). IOP Publishing.
[48]. Snyman, D., & Kruger, H. A. (2020). External contextual factors in information security Behaviour.
[49]. Taha, N., & Dahabiyeh, L. (2021). College students information security awareness: a comparison between smartphones and computers. Education and Information Technologies, 26(2), 1721-1736.
[50]. Tosun, N., Altinöz, M., Çay, E., Çinkiliç, T., Gülseçen, S., Yildirim, T., ... & Ünlü, N. (2020). A swot analysis to raise awareness about cyber security and proper use of social media: Istanbul sample. International Journal of Curriculum and Instruction, 12, 271-294.
[51]. Toukabri, O. (2024). Analysis of social media and phishing awareness among diverse higher education students: A Health Belief Model perspective.
[52]. Yildirim, M., & Erendor, M. E. (2024). A Comparative Analysis Of Cybersecurity Behaviours Of University Students. EDPACS, 1-18.
[53]. Younas, A., & Porr, C. (2023). A step-by-step approach to developing scales for survey research. Nurse researcher, 31(3).
[54]. Yusuf, A. A. (2024). *Employees' cybersecurity awareness and behaviour in South African higher education institutions* (Master's thesis, University of Pretoria (South Africa)).
[55]. Zahid, I. A., Hussein, S. A., & Mahdi, S. M. (2024). Measuring Individuals Cybersecurity Awareness Based on Demographic Features. Iraqi Journal for Electrical & Electronic Engineering, 20(1).
[56]. Zhang, Z., & Gupta, B. B. (2018). Social media security and trustworthiness: overview and new direction. *Future Generation Computer Systems*, *86*, 914-925.
[57]. Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cybersecurity awareness, knowledge and behavior: A comparative study. Journal of Computer Information Systems, 62(1), 82-97.