National Journal of Education Vol. XXIII No. (1)
January 2025
pISSN 0972-9569, eISSN 2584-2595

Cyber Security Awareness Among Higher Education Students

Mohini Mohan Kumbhakar*, Prof. Nagendra Kumar**

Abstract

Cyber security awareness is a fundamental element in safeguarding individuals, organizations, and nations against cyber threats. Among 759 million active internet users, 399 million users are from rural India. Therefore, the cyber security awareness among rural citizen plays a major role. This paper studied the level of cyber security awareness among rural undergraduate (UG) and postgraduate (PG) students in India enrolled in various educational institutions. Using a self-constructed tool (Cyber Security Awareness Test), data was collected from 148 students. The analysis revealed a mean score of 16.30 with a standard deviation of 4.97. The findings indicate that 39.19% of rural students scored below the mean, with significant unawareness of key cyber security concepts such as phishing, multi-factor authentication (MFA), pretexting and on other aspects. UG and PG students exhibited similar levels of awareness but a significant gender disparity was found, with female students scoring lower. The study suggests the need for educational interventions, particularly for female students, to improve awareness and fulfill knowledge gaps. By understanding the current status of cyber security awareness of higher education rural background students from the findings of this study, higher education institutions can develop the strategies to train and educate them about cyber security.

***Keywords**: Cyber security awareness, cyber-attacks, rural students, undergraduate students, postgraduate students.*

Introduction

Technology is deeply intertwined with each aspect of our lives globally. This increases our concern towards cyber security. The present era marked by digital transformation; rural areas are also not safe to the growing threats of cyber-attacks. Like other countries, India faced over 13.9 lakh cyber security incidents in 2022. It includes Phishing, ransom ware attacks, website damage and unauthorized network scanning or probing activities, data violation and many dangerous services happened to all types of users. While out of 759 million active internet users, 399 million users are from rural India, the cyber security awareness among

Junior Research Fellow, Faculty of Education, B.H.U.
****Professor, Faculty of Education, B.H.U.***

rural citizen plays a major role. Numerous studies emphasize the importance of cyber security awareness in reducing cyber threats. Increased awareness of cyber security can lead to better-informed decisions and more secure online behavior. According to a report on Cyber Security by Niti Aayog and Saraswat (n.d.), India ranked among the top five countries to be affected by cybercrime. As Whitman and Mattord (2020) clearly defined cyber security is a field encompassing practices, technologies and strategies aimed at safeguarding computers, networks and data from unauthorized access, attacks and harm. In the advancing world we live in it is crucial to recognize the significance of being aware of cyber security. With our growing dependence, on technology and the internet, for both professional aspects it becomes more essential to grasp and actively participate in cyber security practices. As stated by Disterer (2021), "cyber security awareness is the foundation upon which a strong security posture is built" (p. 45). Cyber security awareness is a broad notion that includes the skills necessary to identify, comprehend, and counteract cyber security threats. The studies highlight the significance of an all-encompassing approach to awareness that includes not only the technical understanding but also a deeper comprehension of the psychological and social dimensions of cyber security (Solms & Niekerk, 2022). This comprehensive viewpoint acknowledges the necessity for people and organizations to have a proactive and watchful mindset in addition to cyber security knowledge (Dumitraş, 2019).

Literature Review

Cyber Security awareness is a critical aspect of mitigating cyber threats and ensuring the security of digital environments. There are number of studies conducted to find the cyber security awareness among different stakeholders. The researcher focused on the different tools used in the studies to find the level of cyber security awareness, different stakeholders and key findings of different research papers.

Numerous methodologies were employed to assess Cyber Security awareness. One commonly used approach is the use of surveys and questionnaires. Daengsi et al. (2021) conducted a survey among employees of a multinational corporation to evaluate their awareness of phishing attacks. The study revealed that 65% of respondents were unable to identify phishing emails accurately. In a study by (Alharbi & Tassaddiq, 2021), participants engaged in simulated social engineering attacks, allowing researchers to assess their ability to recognize and respond to these threats.

Several frameworks and models have been proposed to conceptualize and measure Cyber Security awareness. Cyber security Awareness Inventory (CAIN) developed by Tempestini et al. (2023) is one such framework. CAIN comprises 46 items with True/False response scale. The CAIN has dimensions like: Assets in cyberspace, Cyber security controls, Threats against the security of cyberspace, Guidelines for stakeholders, Framework of information sharing and coordination and Roles of stakeholders in cyber security.

In addition to CAIN, the Cyber Security Scale (CS-S) by Arpaci & Sevinc, (2022) offers a holistic view of Cyber Security awareness within individuals. CS-S incorporates factors such as Availability, Authenticity, Confidentiality, Integrity, Possession/Control and Utility. Studies have identified that individual characteristics, such as age, education, and prior experience, significantly impact awareness levels. Moreover, organizational factors, such as training programs and security policies, play a crucial role in shaping awareness. Khando et al. (2021) investigated the impact of organizational factors and individual attributes on Cyber Security awareness levels. Their findings emphasize the role of organizational climate and policies in shaping employee awareness. Shillair et al. (2022) explored the impact of education and training programs on Cyber Security awareness. Their review encompassed studies that assessed the effectiveness of different educational interventions. Chatterjee et al. (2019) focused on assessing the Cyber Security awareness of internet users in India. They employed surveys and questionnaires to gather data and analyze the awareness levels, providing insights into the Indian context. Chaturvedi et al. (2024) explored the unique challenges and vulnerabilities in Cyber Security awareness from an Indian perspective. They identified region-specific issues that may impact awareness levels. Kant (2023) used a standard tool developed by Erol, Ahin, Ylmaznd & Haseski (2015) named PCSPS (Personal Cyber-security Provision Scale) to assess the personal cyber security provision levels of the students registered in higher education where he examined the knowledge and practices of this demographic regarding online security. After all these reviews the researchers did not come across any study which measured the cyber security awareness of rural undergraduate and post graduate students in higher education. Cyber security is the general issue related to online safety, data privacy and other aspects. So, we have considered the UG and PG students for this study. Therefore, in the present study the researchers have tried to find the answer of the following research question:

What is the level of cyber security awareness among students in higher education with reference to gender and level (UG& PG) of education?

Statement of the problem

To consider the above aspect the statement of the problem was formulated as:

Cyber Security Awareness Among Students in Higher Education

Operational Definitions of key terms:

Cyber security: "Measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack" (Merriam-Webster, 2020). In this study cyber security refers to the practice of defending computers, servers, mobile devices, electronic system, networks, and data from malicious attacks and unauthorized access.

Awareness: According to Dourish and Belloti (1992) "awareness is an understanding of the activities of others, which provides a context for your own activity."In the present study awareness deals with the consciousness of cyber security among rural undergraduate and postgraduate students.

Objectives

1. To compare the level of cyber security awareness between undergraduate and postgraduate students.
2. To compare the level of cyber security awareness between male and female students of higher education
3. To identify the key cyber security concepts where the rural students are least aware.

Null Hypothesis:

$H_0$1: There is no significant difference in the level of cyber security awareness between undergraduate and postgraduate students.

$H_0$2: There is no significant difference in the level of cyber security awareness between male and female students.

Method:

Descriptive survey method was used for this study.

Population and sample:

UG and PG students of Jharkhand state residing in rural areas studying in different universities were defined as the population in this study. Those students were selected in sample of this study who have been using internet for at least 2 years from Seraikela, East Singhbhum and West Singhbhum district through cluster sampling technique because out of the 4 divisions of Jharkhand, Kolhan division is comprises with above three districts and this is a segment. In this study, 296 students of UG and PG classes were taken as the sample randomly.

Table 1

Description of the sample in terms of years using internet

Years Using Internet	Representation in the sample
3-5 years	27.03%
6-8 years	28.38%
More than 8 years	44.59%

Tool for data collection:

After reviewing the various tools to study cyber security awareness, the researcher did not find any tool that is suitable for rural students. Few scales were there but they were not suitable for the present study. Therefore, a self-constructed test CSAT (Cyber Security Awareness Test) was prepared with 22 multiple choice questions having five options. Every fifth option in the questions was same "I do not have any information about this". Every correct answer was given one mark and for incorrect answer, no marks were given. The tool was standardized using test-retest reliability and the reliability coefficient was calculated 0.74 and validity was established using content validity.

The tool has five dimensions:

Dimension 1: Knowledge of cyber threats and risks

Dimension 2: Device security and secure practices

Dimension 3: Safe browsing habits

Dimension 4: Incident reporting and response

Dimension 5: Online communication and scam awareness

A Google form was created using the questions and it was communicated to the participants for gathering the data. The questions and options were available in English and Hindi languages. Range of the score was 0 to 22.

Techniques

Statistics used for the data analysis were Mean, Percentage, SD in descriptive statistics and t-test for the comparison of group means in the inferential statistics. The analysis was done using MS Excel Version 2021.

Data Analysis, Result and discussion:

A general description of rural students Cyber Security Awareness scores

Gathered data was analyzed according to item wise for assessing the cyber security awareness of the UG and PG rural students.

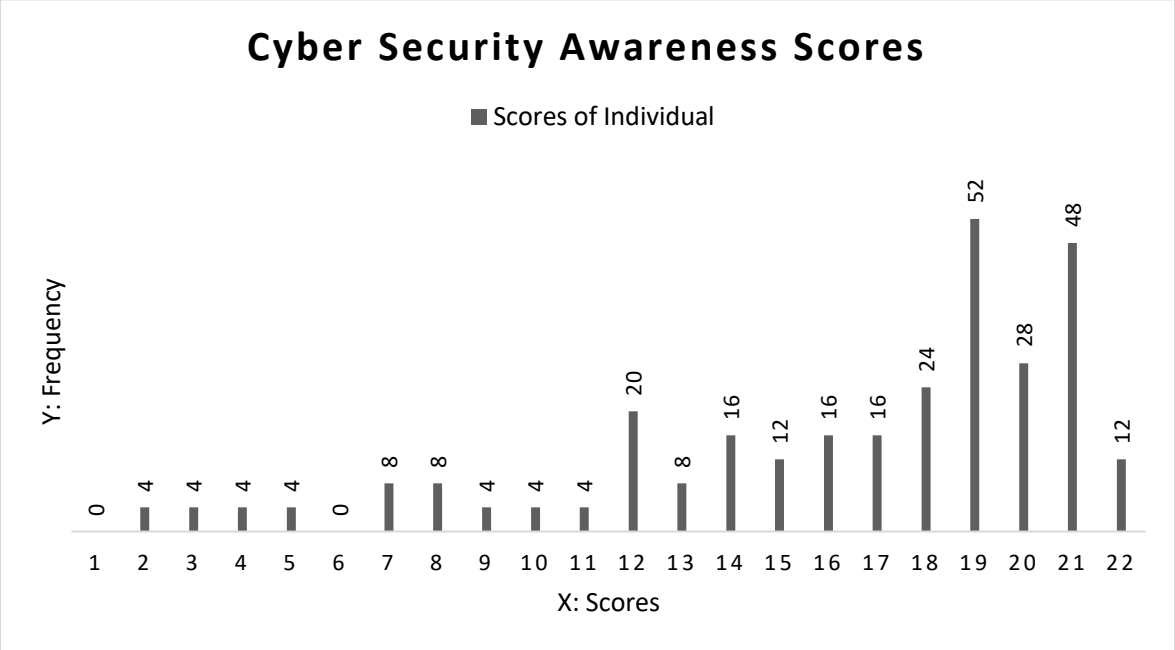
Table 2

Mean and SD of the Cyber Security Awareness scores of rural students in higher education

Mean	16.30
SD	4.97

The mean of the scores obtained from 296 students was found 16.30 and SD was found 4.97

Graph 1: Graphical presentation of Rural students Cyber Security Awareness scores



The above graph displays the distribution of scores among individuals and other aspects are described below:

Horizontal Axis (X-axis): Represents the scores of individuals, ranging from 1 to 22 where 12 respondents scored maximum marks

Vertical Axis (Y-axis): Represents the frequency of each score.

The graph also shows the scores of individuals

Most Frequent Score: The score of 19 is scored by most of the respondents, with 52 individuals achieving this score. This can be considered as mode.

Table 3: Level of Cyber Security Awareness among rural students in higher education

Level of Awareness	Score Range	Percentage of Students	Description
Low	1-11	10.81%	Below -1 SD: Significant gaps in understanding key cyber security concepts.
Average	12-21	85.13%	Between -1 SD and +1 SD: Moderate awareness, with room for improvement.
High	22	4.05%	Above +1 SD: Strong understanding of cyber security concepts.

The table presents the level of Cyber Security Awareness among rural students in higher education, classified into three categories—Low, Average, and High Awareness—based on their scores in the Cyber Security Awareness Test (CSAT). 10.81% of students have low awareness, indicating a critical need for interventions and awareness programs to address increase the cyber security awareness. The majority of rural students (85.13%) including both UG and PG possess an average level of cyber security awareness, suggesting that while they have some knowledge, there are still significant areas for improvement. Only 4.05% of students show high awareness, highlighting that few students are fully prepared to tackle the complex challenges of cyber security in the modern digital environment.

Table 4: Categorization of Level of Cyber Security Awareness of UG rural students

Level of Awareness	Score Range	Percentage of Students	Description
Low	01-11	18.60%	Below -1 SD: Significant gaps in understanding key cyber security concepts.
Average	12-21	67.44%	Between -1 SD and +1 SD: Moderate awareness, with room for improvement.
High	22	4.65%	Above +1 SD: Strong understanding of cyber security concepts.

The table presents the level of Cyber Security Awareness among UG students in higher education, classified into three categories—Low, Average, and High Awareness—based on their scores in the Cyber Security Awareness Test (CSAT). Among UG students, 18.60% have low awareness, signaling a critical need for targeted interventions to improve cyber security knowledge. The majority of UG students, 67.44%, fall into the average awareness category, indicating a moderate understanding but highlighting room for growth. Only 4.65% of UG students show high awareness, suggesting that very few are well-equipped to handle advanced cyber security challenges.

Table 5: Categorization of Level of Cyber Security Awareness among PG rural students

Level of Awareness	Score Range	Percentage of Students	Description
Low	01-11	11.90%	Below -1 SD: Significant gaps in understanding key cyber security concepts.
Average	12-21	85.71%	Between -1 SD and +1 SD: Moderate awareness, with room for improvement.
High	22	2.38%	Above +1 SD: Strong understanding of cyber security concepts.

The table presents the level of Cyber Security Awareness among PG students in higher education, classified into three categories—Low, Average, and High Awareness—based on their scores in the Cyber Security Awareness Test (CSAT). In this table, 11.90% PG students present low awareness, underscoring a need for enhanced training programs. Most PG students, 85.71%, have an average level of awareness, showing that while they possess some foundational knowledge, there remains a significant gap to be bridged. A minimal 2.38% of PG students exhibit high awareness, reflecting the limited number who are fully prepared to address cyber security threats in today's digital landscape.

Objective wise Analysis

1. First objective of the study was "To compare the level of cyber security awareness among undergraduate and postgraduate students." To asses this objective null hypothesis $H_0$1was framed.

$H_0$1"There is no significant difference in the level of cyber security awareness in undergraduate and postgraduate students."

Table 6

Course wise comparison of Cyber Security Awareness Scores

	N	Mean	SD	df	t-value	Significance level
UG Students	128	16.16	4.90	294	.42	.05
PG Students	168	16.40	5.08			

The mean of scores obtained by the UG and PG students in the CSAT (Cyber Security Awareness Test) was 16.16 and 16.40 and the SD was 4.90 and 5.08. The calculated value of t was found 0.42 and the table value for t at df 146 is 1.97 which is more than the calculated value. So, the null hypothesis "There is no significant difference in the level of cyber security awareness in undergraduate and postgraduate students" could not be rejected. It means the UG and PG rural students have similar awareness about Cyber Security.

2. Second objective of the study was "To compare the level of cyber security awareness among male and female students of higher education". To asses this objective null hypothesis $H_0$2 was framed.

$H_0$2: There is no significant difference in the level of cyber security awareness among male and female students.

Table 7: Gender wise comparison of scores

	N	Mean	SD	df	t-value	Significance level
Female Students	156	15.69	4.66	294	2.23	.05
Male Students	140	16.97	5.27			

The mean of scores obtained by the female and male students in the CSAT (Cyber Security Awareness Test) was 15.69 and 16.97 and the SD was 4.66 and 5.27. The calculated value of t was found 2.23 and the table value for t at df 146 is 1.97 which is less than the calculated value. So, the null hypothesis "There is no significant difference in the level of cyber security awareness among male and female students" is rejected. It means the male students have slight higher cyber security awareness than female students, and female rural students have low awareness about Cyber Security, there is need for targeted interventions to improve awareness among female students in rural areas.

3. The third objective of the study was "To identify the key cyber security concepts where rural students are least aware." To asses this objective responses were analyzed and reflected in below table

Table 8

Questions on which students responded they are not aware about the term

Items	**1**	**5**	**12**	**14**	**19**	**20**
Correct	184	204	116	124	184	112
Incorrect	32	36	92	84	40	68
Unknown	**80**	**56**	**88**	**88**	**72**	**116**

In the above table the serial number questions, total correct and incorrect responses are shown with the number of responses received for the option "I do not have any information about it" which is leveled as unknown.

Most wrong answered questions by UG and PG rural students are:

- Jailbreaking or rooting your devices will result in **116/296**
- How can you differentiate between a genuine website and a phishing site? **124/296**

- After completing a UPI/NET banking transaction on a friend's smart phone, the payment app suggests saving your UPI PIN/NET banking details for quicker transactions. What would be the most appropriate course of action?**112/296**

List of key cyber security concepts students are unaware about

- Phishing E-mail
- Multi-factor authentication (MFA)
- Jailbreaking or rooting devices
- Differentiating between a genuine website and a phishing site
- Suspicious emails
- Reporting Cyber security incidents
- Pretexting and its risks

Discussion

The survey results reveal key insights into the state of cyber security awareness among rural students in higher education, particularly regarding their familiarity with essential concepts and practices. Total 296 students participated in this research and the mean score was 16.30 with a standard deviation of 4.97. The awareness levels varied significantly across the population, with 39.19% of individuals scoring below the mean and 60.81% scoring above it. These findings suggest a few important observations in cyber security awareness that needs to be addressed.

In terms of educational level, the scores for undergraduate (UG) students and postgraduate (PG) students were statistically similar, with mean scores of 16.16 and 16.40, respectively. The percentage of UG students who scored below the mean was 35.14%, while 17.57% of PG students fell into this category. On the contrary, 36.49% of PG students scored above the mean, compared to 24.32% of UG students. These figures indicate that while PG students slightly outperformed UG students in cyber security awareness, the difference is not statistically significant. This could be attributed to a lack of dedicated cyber security education at both the undergraduate and postgraduate levels. When comparing male and female students, the mean scores were 16.97 for males and 15.69 for females. With this notable difference, the analysis resulted significant difference with reference to gender (Male and Female), suggesting that gender still plays a substantial role in determining cyber security awareness among rural students but the level of education does not. This outcome does not align with the hypothesis that both male and female students possess equal levels of

knowledge about cyber security. Based on this there is need to focus more on female education about cyber security. The study also highlighted areas where students exhibited significant unawareness. A substantial portion of participants struggled with understanding key cyber security terms, such as phishing (42%), multi-factor authentication (MFA) (28%), jailbreaking (44%), and pretexting (58%). One possible explanation for this unawareness could be the lack of targeted cyber security training programs and the absence of these topics in the curriculum. Given the increasing relevance of digital literacy, integrating these concepts into the education system would be a critical step toward enhancing the overall cyber security awareness of students. While the rural student population in higher education demonstrates a moderate level of cyber security awareness, there is a clear need for improvement, particularly in specific areas where knowledge gaps persist. Implementing educational interventions and including cyber security topics in the curriculum could help bridge these gaps and ensure students are better prepared to navigate the digital landscape safely.

Educational Implications

The increasing use of the internet in rural areas, particularly among students in higher education, has brought about new concerns regarding cyber security. With 399 million active internet users from rural India alone, the risk of cyber-attacks has become a significant threat. As technology becomes more integrated into education and daily life, rural students' lack of cyber security knowledge exposes them to potential threats like identity theft, online fraud, and data leaks. On the basis of present study few aspects can be incorporated by which cyber security awareness can be increased which are given below:

Integration of Cyber security into the Curriculum: The study highlights a significant gap in cyber security knowledge among rural students, especially on key concepts like phishing, multi-factor authentication, and pretexting. To address these deficiencies, educational institutions must incorporate cyber security awareness training into the curriculum at both undergraduate (UG) and postgraduate (PG) levels. This would ensure that students will be equipped with the necessary skills to recognize and control cyber threats, which is increasingly crucial in today's digital world.

Targeted Awareness Programs: The finding reflect that many students are unaware of fundamental cyber security concepts therefore a need of specialized awareness programs. Therefore, it is required to higher education institutions should organize workshops, seminars, and campaigns to educate students about the latest cyber threats, preventive

measures, and safe online practices. Such programs will help bridge the knowledge gap, especially in rural areas where digital literacy may lag behind urban areas. Practical simulations, such as identifying phishing emails or setting up multi-factor authentication, could be integrated into the education system. By using real-world scenarios, students will gain experience in recognizing and responding to cyber threats effectively.

Use of Multilingual Educational Tools: As the test used in this study to find the cyber security awareness was conducted in both English and Hindi, the study demonstrates the importance of providing educational materials in multiple languages to cater to diverse linguistic backgrounds. Ensuring accessibility to cyber security education through local languages significantly enhance understanding and engagement among rural students.

Focus on Equal Gender Awareness: From the findings significant difference was found between rural areas male and female students in terms of cyber security awareness, targeted interventions could ensure that female students remain equally informed. This could help in maintaining gender parity in cyber security literacy and encourage more female students to pursue careers in technology and cyber security so that we will be able to reduce the threats most of the times we see such as girls getting trapped in digital issues like online sexual abuse.

References:

Ahmad, Md. O., Tripathi, G., Siddiqui, F., Alam, M. A., Ahad, M. A., Akhtar, M. M., & Casalino, G. (2023). BAuth-ZKP—A Blockchain-Based Multi-Factor Authentication Mechanism for Securing Smart Cities. *Sensors*, *23*(5), 2757. https://doi.org/10.3390/s23052757.

Alharbi, T., & Tassaddiq, A. (2021). Assessment of Cybersecurity Awareness among Students of Majmaah University. *Big Data and Cognitive Computing*, *5*(2), 23. https://doi.org/10.3390/bdcc5020023

Alkhalil Z, Hewage C, Nawaf L and Khan I (2021) Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. Front. Comput. Sci. 3:563060. doi: 10.3389/fcomp.2021.563060.

Anderson, E., Durcikova, A., & Lichtenstein, Y. (2020). Antecedents of Cyber Security Awareness: Cyber Security Policy, Organizational Climate, and Individual Attributes. *Computers in Human Behavior*, 75, 255-263.

Arpaci, I., & Sevinc, K. (2022). Development of the cybersecurity scale (CS-S): Evidence of validity and reliability. *Information Development*, *38*(2), 218–226. https://doi.org/10.1177/0266666921997512

Buckley, J., Lottridge, D., Murphy, J. G., & Corballis, P. M. (2023). Indicators of employee phishing email behaviours: Intuition, elaboration, attention, and email typology. *International Journal of Human-Computer Studies*, *172*, 102996. https://doi.org/10.1016/j.ijhcs.2023.102996

Chatterjee, S., Kar, A. K., Dwivedi, Y. K., & Kizgin, H. (2019). Prevention of cybercrimes in

smart cities of India: from a citizen's perspective. *Information Technology & People*, *32*(5), 1153-1183.

Chaturvedi, M., Narain Singh, A., Prasad Gupta, M., & Bhattacharya, J. (2014). Analyses of issues of information security in Indian context. *Transforming Government: People, Process and Policy*, *8*(3), 374-397.

Chauhan, P. S., & Kshetri, N. (2021). 2021 State of the Practice in Data Privacy and Security. *Computer*, *54*(8), 125–132. https://doi.org/10.1109/MC.2021.3083916

Chen, R., & Li, D. (2018). Assessing Cyber Security Awareness: A Comparative Study of Two Large-Scale Organizations. *Information Systems Frontiers*, *20*(3), 611-626.

Choo, R. K., Liu, L., & Goh, A. (2019). Cyber security: Managing systems, conducting testing, and investigating intrusions. *Springer*.

Daengsi, T., Pornpongtechavanich, P., & Wuttidittachotti, P. (2022). Cybersecurity Awareness Enhancement: A Study of the Effects of Age and Gender of Thai Employees Associated with Phishing Attacks. *Education and Information Technologies*, *27*(4), 4729–4752. https://doi.org/10.1007/s10639-021-10806-7

Daengsi, T., Wuttidittachotti, P., Pornpongtechavanich, P., & Utakrit, N. (2021, June). A comparative study of cybersecurity awareness on phishing among employees from different departments in an organization. In *2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE)* (pp. 102-106). IEEE.

Disterer, G. (2018). Cyber security – Its Importance in the World of Technology. In Cyber security – Its Importance in the World of Technology (pp. 45-53). *Springer*.

Harris, S. (2020). Cyber security and Human Behavior: An Introduction to the Concept of People-Centric Security. *CRC Press*.

Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y., & Ochoa, M. (2019). Insight into insiders and it: A survey of insider threat taxonomies, analysis, modeling, and countermeasures. *ACM Computing Surveys (CSUR)*, *52*(2), 1-40.

Hu, S., Hsu, C., & Zhou, Z. (2022). Security Education, Training, and Awareness Programs: Literature Review. *Journal of Computer Information Systems*, *62*(4), 752–764. https://doi.org/10.1080/08874417.2021.1913671

Jayatilaka, A., Arachchilage, N. A. G., & Babar, M. A. (2024). Why People Still Fall for Phishing Emails: An Empirical Investigation into How Users Make Email Response Decisions. *arXiv preprint arXiv:2401.13199*.

Jakobsson, M., and Myers, S. (2006). Phishing and countermeasures: understanding the increasing problems of electronic identity theft. New Jersey: John Wiley and Sons.

Kant, R. (2023). Cyber-Security Awareness In India: How Much Students Of Higher Education Are Aware? *GESJ: Education Science and Psychology*, *2*(67), 59–72.

Khajuria, S., Sørensen, L. T., & Skouby, K. E. (Eds.). (2017). *Cyber security and privacy - bridging the gap*. River Publishers.

Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & Security*, *106*, 102267. https://doi.org/10.1016/j.cose.2021.102267

Klein, G., & Zwilling, M. (2023). The Weakest Link: Employee Cyber-Defense Behaviors While Working from Home. *Journal of Computer Information Systems*, 1–15. https://doi.org/10.1080/08874417.2023.2221200

Kumar, S., & Krishna, P. V. (2018). Cyber security: Threats, challenges, opportunities. *CRC Press*.

Mishra, A., & Panigrahi, R. (2021). Challenges and Vulnerabilities in Cyber Security Awareness: An Indian Perspective. *Journal of Information Security*, *12*(2), 91-104.

Mohammad, R. M., Thabtah, F., & McCluskey, L. (2012, December). An assessment of features related to phishing websites using an automated technique. In *2012 international conference for internet technology and secured transactions* , 492-497. IEEE.

Nord Layer. (2024). *Guarding the heart of giving: cyber security for NGOs*. https://nordlayer.com/blog/cybersecurity-for-ngos/

Picus Labs. (2023). *What Is Advanced Persistent Threat (APT)?* Retrieved December 20, 2023,from https://www.picussecurity.com/resource/glossary/what-is-advanced-persistent-threat-apt#:~:text=exploiting%20security%20vulnerabilities.-,Advanced%20Persistent%20Threats%20(APTs),approach%20taken%20by%20the%20attackers.

Rajivan, P., Gonzalez, C., & Zhao, X. (2018). Cyber Security Education and Training: A Review of Literature. *Computers & Security*, *76*, 257-276.

Reeves, A., Delfabbro, P., & Calic, D. (2021). Encouraging Employee Engagement With Cybersecurity: How to Tackle Cyber Fatigue. *SAGE Open*, *11*(1), 215824402110000. https://doi.org/10.1177/21582440211000049

Sachdeva, A., & Kaur, H. (2020). Cyber Security Awareness among Youth in India: An Empirical Study. *International Journal of Recent Technology and Engineering*, *8*(1), 4455-4461.

Schlette, D., Caselli, M., & Pernul, G. (2021). A comparative study on cyber threat intelligence: The security incident response perspective. *IEEE Communications Surveys & Tutorials*, *23*(4), 2525-2556.

Schneier, B. (2019). Click here to kill everybody: Security and survival in a hyper-connected world. W. W. Norton & Company.

Shillair, R., Esteve-González, P., Dutton, W. H., Creese, S., Nagyfejeo, E., & Von Solms, B. (2022). Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise. *Computers & Security*, *119*, 102756. https://doi.org/10.1016/j.cose.2022.102756

Sundararajan, V., & Rashid, A. (2019). Beyond Clicking: Dwell Time Analysis for Enhanced Cyber Security Awareness. *Computers & Security*, 82, 212-227

Tempestini, G., Rovira, E., Pyke, A., & Di Nocera, F. (2023). The Cybersecurity Awareness INventory (CAIN): Early Phases of Development of a Tool for Assessing Cybersecurity Knowledge Based on the ISO/IEC 27032. *Journal of Cyber security and Privacy*, *3*(1), 61–75. https://doi.org/10.3390/jcp3010005

Verma, P., & Hwang, T. (2018). Assessing Cyber Security Awareness among Indian Internet Users. *Procedia Computer Science*, 132, 665-672.

Whitman, M. E., & Mattord, H. J. (2020). Principles of Information Security. *Cengage Learning.*

Wilhelm, T. (2013). Privilege Escalation. In *Professional Penetration Testing*, 271–306. Elsevier. https://doi.org/10.1016/B978-1-59749-993-4.00010-0

Zahid, I., Hussein, S., & Mahdi, S. (2024). Measuring Individuals Cybersecurity Awareness Based on Demographic Features. *Iraqi Journal for Electrical and Electronic Engineering*, *20*(1), 58–67. https://doi.org/10.37917/ijeee.20.1.6

Zain, M. R., Zahari, M. H., & Zainol, M. N. A. (2023). Inter-agency information sharing coordination on humanitarian logistics support for urban disaster management in Kuala Lumpur. *Frontiers in Sustainable Cities*, *5*, 1149454.