A Students' Perspective on Cybersecurity Awareness and Education

Ronnie B. Santelices

Catanduanes State University, College of Engineering and Architecture

DOI: https://dx.doi.org/10.47772/IJRISS.2025.903SEDU0597

Received: 14 October 2025; Accepted: 20 October 2025; Published: 04 November 2025

ABSTRACT

The increasing reliance on digital technologies in education has heightened students' exposure to cybersecurity risks, prompting the need for proactive interventions to strengthen awareness and education. This study investigated the cybersecurity awareness and education of Catanduanes State University (CatSU) students, focusing on their demographic profile in terms of gender, academic year level, and internet access devices, while also examining the relationship between education and awareness. Using a quantitative research design, a stratified random sample of 386 students was surveyed through a structured questionnaire adapted from established research instruments, measured on a 5-point Likert scale. Descriptive and inferential statistics were employed to analyze the data, with findings showing generally high levels of cybersecurity awareness and education among students. Results revealed that second-year students displayed stronger awareness compared to other levels, while laptop users exhibited greater familiarity with protective practices, reflecting the role of device use in shaping online security behavior. Gender differences were minimal but suggested the need to boost technical confidence and consistent practice across groups. Correlation analysis confirmed a strong positive relationship ($r = 0.670$, $p < 0.01$) between cybersecurity education and awareness, emphasizing the impact of structured learning on students' protective behaviors. The study concludes that effective and practical cybersecurity education programs—integrated into the curriculum through workshops, simulations, and real-world applications—are essential in equipping students with the knowledge and skills to recognize, mitigate, and respond to cyberthreats. These findings have significant implications for higher education institutions, underscoring the importance of fostering a cyber-resilient culture that prepares students to navigate the complexities of today's interconnected digital environment securely and responsibly.

Keywords: Cybersecurity, Cybersecurity Awareness, Cybersecurity Education, CatSU students, Demographics

INTRODUCTION

In today's increasingly interconnected world, cybersecurity has become a fundamental concern for individuals, organizations, and educational institutions. With the rapid integration of digital technologies in both personal and academic environments, the potential risks associated with cyber threats, such as identity theft, data breaches, and malware attacks, have surged. Educational institutions, particularly universities, have become prime targets for cybercriminals, who exploit vulnerabilities in their networks and student behavior. As the student body is often seen as a weak link in the cybersecurity chain, it is imperative to assess their awareness and understanding of cybersecurity principles.

At Catanduanes State University (CatSU), the adoption of digital platforms for learning and administrative purposes has increased the need for robust cybersecurity education. However, despite the institution's efforts, it is unclear how well students are equipped to identify, prevent, and respond to cyber threats. This gap in knowledge can leave students vulnerable to various cyberattacks, potentially compromising both personal and institutional data. As cybersecurity awareness is a critical factor in preventing such threats, understanding the level of knowledge and education among students is essential.

This study aims to assess the level of cybersecurity awareness and education among CatSU students, exploring how demographic factors such as gender, academic year, and internet access devices influence their cybersecurity knowledge. By examining these factors, the study seeks to identify areas of strength and

weakness in students' cybersecurity understanding, providing valuable insights into how the university can enhance its cybersecurity education initiatives. Through this research, the goal is to contribute to the development of a more secure digital environment for students and faculty alike, fostering responsible online behavior and improving the university's overall cybersecurity culture.

RESEARCH METHODOLOGY

This study employed a quantitative research design to assess the level of cybersecurity awareness and education among students at Catanduanes State University (CatSU). A survey-based approach was chosen for data collection, as it allows for efficient gathering of information from a large group of participants and provides a clear, measurable understanding of students' awareness and education in cybersecurity.

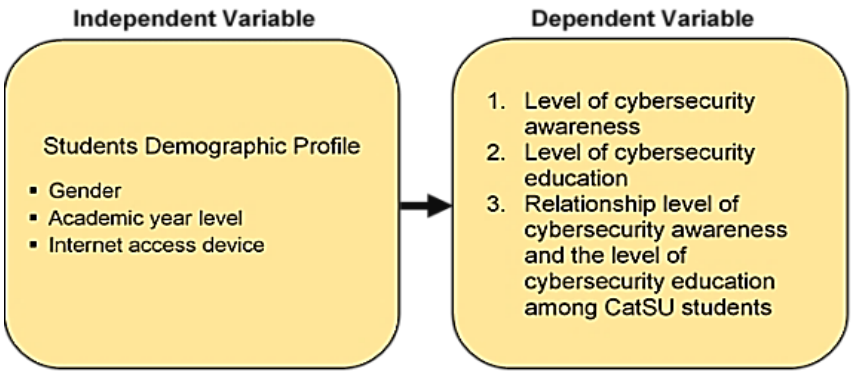
Research Design

The research design focused on the systematic collection and analysis of quantitative data to evaluate the levels of cybersecurity awareness and education among students. The methodology involved distributing structured surveys or questionnaires to a representative sample of students from various academic disciplines to assess their understanding of cybersecurity concepts, prior experiences with cyber-related incidents, and involvement in cybersecurity education initiatives. This approach ensured a comprehensive understanding of students' exposure to cybersecurity topics and their preparedness to mitigate risks. Statistical analysis methods were employed to analyze the collected data, utilizing both descriptive and normative statistics. Descriptive statistics provided insights into the fundamental characteristics of the independent variables, such as gender, academic year level, and type of internet access device. On the other hand, normative (inferential) statistics were applied to examine relationships between the independent and dependent variables, aligning with the research objectives. These statistical methods identified trends, patterns, and correlations, offering a clearer understanding of the levels of cybersecurity awareness and education, as well as their determinants and associations. This approach enabled the research to uncover critical insights into students' cybersecurity knowledge and engagement with educational opportunities.

Conceptual/Theoretical Framework

The schematic representation of cybersecurity awareness and education among CatSU students is displayed in Figure 1. The study's independent and dependent variables are displayed in the conceptual paradigm.

Figure 1. Conceptual Framework



The students' demographic profile makes up the independent variables. Its dependent variable is the level of education and awareness regarding cybersecurity.

The conceptual framework for this study is based on examining the interrelated factors that influence the levels of cybersecurity awareness and education among CatSU students. The demographic profile of students, including their gender, academic year level, and the type of internet access device they use, is identified as a key independent variable that may affect their level of cybersecurity awareness and education. Understanding these demographic factors is vital because they provide context for assessing individual differences in cybersecurity knowledge, exposure, and behavior patterns. Furthermore, the framework establishes a

connection between these variables and the dependent variables, specifically the students' level of cybersecurity awareness and education.

The conceptual framework emphasizes three primary research objectives: assessing the level of cybersecurity awareness, determining the level of cybersecurity education, and exploring the relationship between these two dependent variables. These objectives aim to evaluate how demographic characteristics, such as gender, academic year, and internet device use, impact the students' understanding of cybersecurity concepts and threats. Additionally, this framework provides a foundation for analyzing gaps in knowledge, identifying key challenges, and proposing strategies for improving cybersecurity education and awareness. Ultimately, the conceptual model seeks to demonstrate the dynamic interaction between demographic factors, cybersecurity awareness, and education to inform targeted educational interventions and resource allocation strategies at CatSU.

Population and Sample

The population for this study consisted of students enrolled at CatSU during the academic year 2023–2024. To ensure the sample was representative of the entire student body, a stratified random sampling technique was employed. Stratified random sampling was used to ensure that different demographic groups (such as gender, academic year level, and internet access device) were proportionally represented in the sample. The total student population at CatSU was approximately 11,828, with students spread across nine different colleges.

Using Slovin's formula for sample size determination, the study calculated the required sample size at a 5% margin of error, resulting in a final sample size of 386 students. The sample included an equal representation of male and female students and was divided across all year levels (first year to fourth year), ensuring that the sample reflected the diversity of the student population. Participants were selected randomly from different academic programs, with particular attention given to ensuring balanced representation from the various colleges and courses.

Data Collection Instrument

A structured questionnaire was developed to assess students' cybersecurity awareness and education. The questionnaire was designed with both closed and Likert-scale questions, focusing on the following areas:

1. Demographic Information: Participants were asked about their gender, academic year, and the devices they use for internet access (e.g., mobile phone, laptop, tablet, desktop).
2. Cybersecurity Awareness: Questions assessed students' knowledge of key cybersecurity concepts, such as identifying potential online threats (e.g., phishing, malware), using secure passwords, safeguarding personal information, and recognizing the importance of cybersecurity in daily activities.
3. Cybersecurity Education: The survey also examined the participants' experiences with formal or informal cybersecurity education, including participation in training sessions, workshops, or online courses. Students were asked about their exposure to cybersecurity topics within their academic curriculum and their willingness to receive further education on cybersecurity.

The questionnaire was pre-tested with a small group of students to ensure clarity, reliability, and validity. Based on feedback from the pre-test, some questions were revised for better understanding. The final version of the questionnaire consisted of 30 items, with a mix of multiple-choice and Likert-scale questions ranging from Strongly Agree (5) to Strongly Disagree (1).

Data Collection Procedure

Data collection took place over a two-week period during the second semester of the academic year. The survey was administered in person during students' free periods in classrooms across different colleges. This allowed for maximum participation while ensuring that students from various disciplines and academic levels were included in the study. Informed consent was obtained from all participants, assuring them that their responses would remain confidential and used solely for research purposes.

The data collection process was supervised by trained research assistants who provided guidance and answered any questions from participants. Additionally, the assistants ensured that all participants completed the survey independently and without external influence.

Data Analysis

The collected data were analyzed using descriptive statistics to summarize and describe the key trends in students' cybersecurity awareness and education. The responses from the Likert-scale questions were quantified, and the General Weighted Average (GWA) was calculated for each attribute to assess the overall level of awareness and education. The data were also analyzed for significant differences based on demographic factors, using ANOVA (Analysis of Variance) to compare groups across gender, academic year levels, and device usage.

To explore the relationship between cybersecurity education and awareness, correlation analysis was conducted to determine whether higher levels of education were associated with greater cybersecurity awareness among students. All data analysis was performed using SPSS (Statistical Package for the Social Sciences) software, which provided both frequency distributions and statistical significance tests to draw conclusions from the data.

RESULTS AND DISCUSSION

Demographic profile of CatSU students in terms of gender, academic year level, and internet access device

A fundamental understanding of the various traits influencing CATSU students' online habits and cybersecurity awareness may be gained from their demographic profile. A thorough image of the students' digital involvement may be obtained by examining important variables like the distribution of genders, academic year level, and preferred internet access devices. Finding patterns and trends, such as the most popular device kinds or the platforms that control their online presence, is made possible by analyzing these demographics. Designing successful educational strategies and interventions to raise cybersecurity awareness that are suited to the individual requirements and preferences of the student body requires this knowledge.

Figure 2. Gender

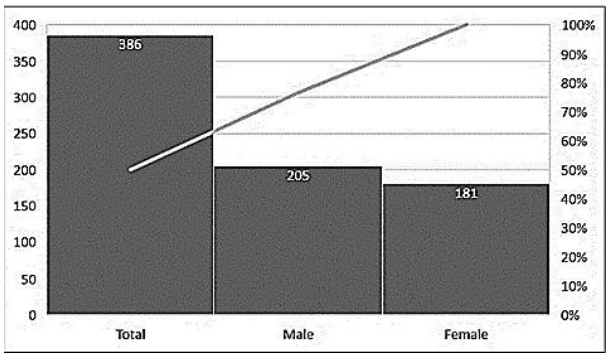


Figure 3. Academic Year Level

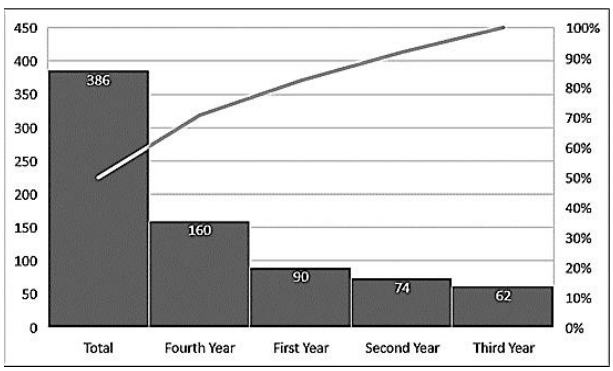


Figure 3. Academic Year Level

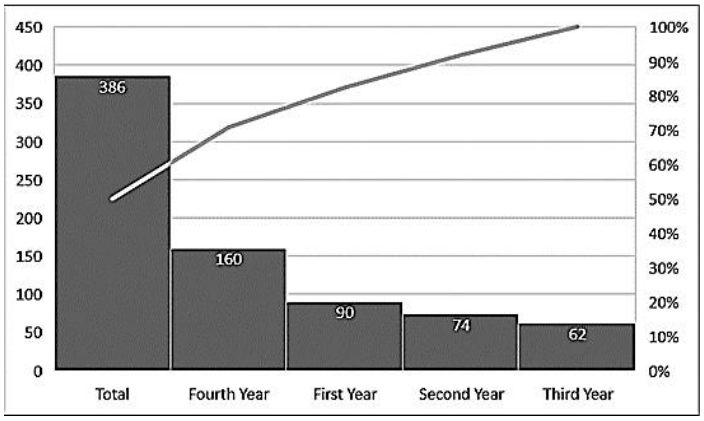
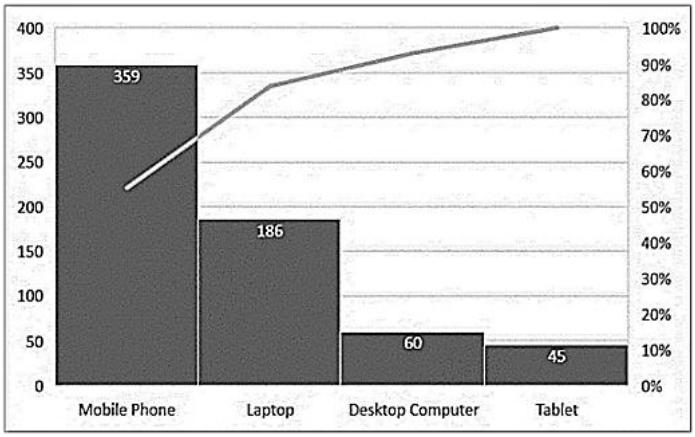


Figure 4. Internet Access Device



Figures 2, 3, and 4 provide key insights into the demographics and online habits of the 386 survey respondents. Figure 2 reveals a fairly balanced gender distribution, with 53% or 205 identifying as male and 47% or 181 as female, indicating equitable gender representation among students. Figure 3 shows that fourth-year students constitute the largest group (41%, or 160 individuals), followed by first-year students (23%, or 89 individuals), second-year students (19%, or 73 individuals), and third-year students (16%, or 62 individuals), suggesting that older students are more actively involved in academic research and related activities. This may be attributed to their advanced academic standing, familiarity with university systems, or greater participation in extracurricular and school-related events. Figure 4 highlights that 93% of respondents (359 individuals) use mobile phones as their primary device for internet access, underscoring the dominance of mobile technology in shaping students' online engagement and exposure to cybersecurity risks. This trend emphasizes the importance of developing cybersecurity awareness initiatives tailored to address the unique vulnerabilities associated with mobile phone use.

Level of cybersecurity awareness among CatSU students in terms of its demographic profile

Assessing cybersecurity awareness among students is essential for understanding their ability to navigate today's digital environment safely. At CatSU, this evaluation examines how demographic factors—such as gender, academic year, and internet access devices—affect students' knowledge, attitudes, and online behaviors. The analysis aims to identify gaps in cybersecurity awareness and pinpoint specific groups that may require focused educational interventions. Central to this study is the evaluation of 15 attributes, coded A1 to A15, which encompass key dimensions of cybersecurity awareness. These attributes include familiarity with basic concepts, threat recognition, proactive security practices, and attitudes toward cybersecurity education. By analyzing these attributes across demographic groups, the study provides a detailed perspective on variations in cybersecurity awareness, helping to identify areas for improvement. This comprehensive approach ensures targeted and effective initiatives to enhance students' understanding of cybersecurity, ultimately promoting safer online behaviors and fostering a more secure digital environment for CatSU students.

Table 1. Cybersecurity Awareness Concept

Code	Attribute Description
A1	Familiarity with the term "cybersecurity" and understanding its significance in today's digital world.
A2	Awareness of various cybersecurity threats, including phishing scams, malware infections, and ransomware attacks.
A3	Ability to recognize and avoid suspicious links or attachments in emails or messages.
A4	Understanding the importance of using strong passwords and regularly updating them for online accounts.
A5	Caution when sharing personal information online, avoiding sharing it with strangers or on untrusted websites.
A6	Awareness of the risks associated with public WI-FI networks and taking precautions to protect data.
A7	Understanding the importance of keeping devices updated with the latest security patches and software updates.
A8	Regularly backing up important data to prevent loss due to cyberattacks or device malfunctions.
A9	Awareness of the potential consequences of cybersecurity breaches, such as identity theft, financial fraud, and reputational damage.
A10	Concern about the growing sophistication of cyber threats and the evolving nature of cybersecurity risks.
A11	Belief that cybersecurity is a shared responsibility among individuals, organizations, and governments.
A12	Commitment to taking proactive measures to protect against cyber threats and cybersecurity incidents.
A13	Belief that everyone, regardless of technical expertise, should have access to cybersecurity education and awareness resources.
A14	Confidence in the ability to identify and avoid cyber threats, with a preparedness to handle cybersecurity incidents.
A15	Openness to learning more about cybersecurity and improving knowledge and skills in the field.

Figure 5 reveals minimal differences in the General Weighted Average (GWA) across the 15 attributes (A1 to A15) between male and female participants, indicating similar levels of cybersecurity awareness. Males scored slightly higher in A4 (importance of strong passwords) and A5 (caution with personal information), suggesting greater engagement in these areas. Meanwhile, females performed equally or slightly better in A14 (confidence in avoiding cyber threats) and A15 (openness to learning more about cybersecurity). Overall, the results highlight a high and equitable level of cybersecurity awareness among both genders, with balanced understanding and practices across the evaluated attributes.

Figure 5. Level of Cybersecurity Awareness in terms of Gender

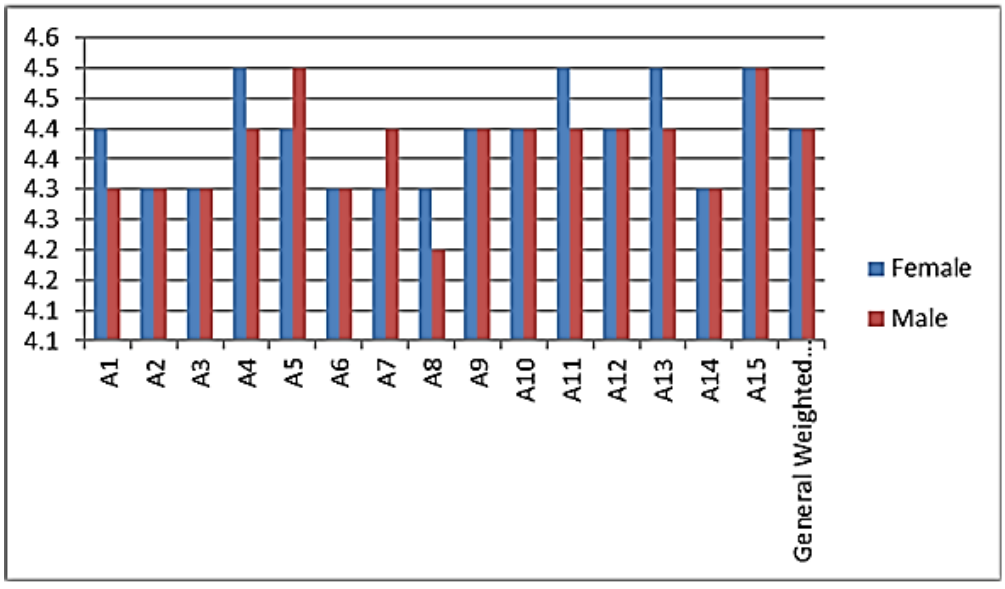


Figure 6. Level of Cybersecurity Awareness in terms of Year Level

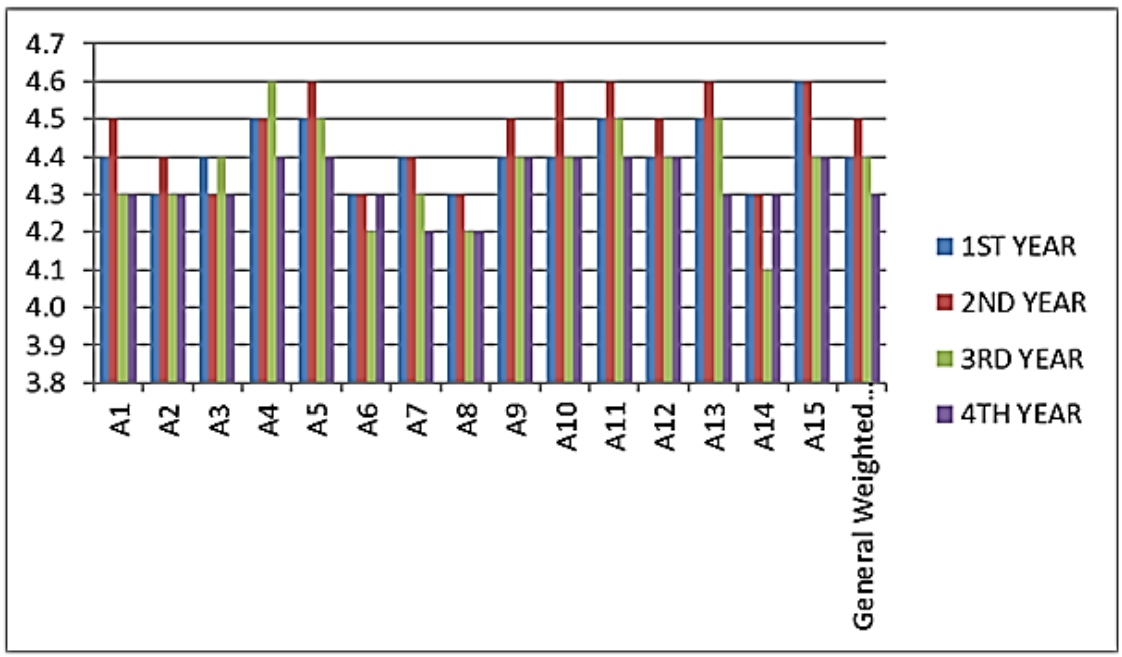
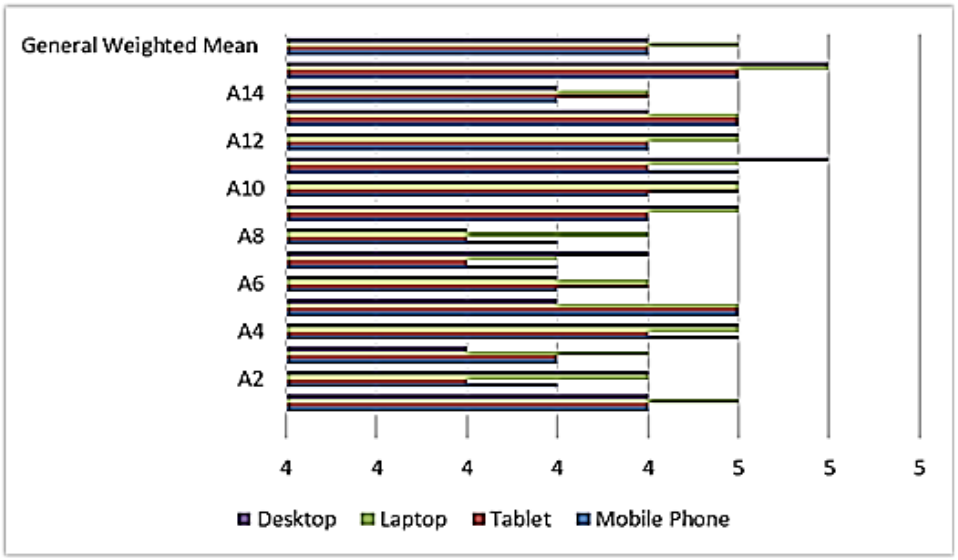


Figure 7. Level of Cybersecurity Awareness in terms of Internet Access Device



Figures 6 and 7 reveal key insights into cybersecurity awareness across academic year levels and device usage. Fourth-year students consistently achieve the highest GWA for attributes (A1–A15), reflecting their advanced understanding due to formal education and experience, while first-year students show foundational knowledge needing improvement. Second-year and third-year students display progressive growth, underscoring the role of academic progression in enhancing awareness. In device usage, laptop users score highest (4.5), excelling in areas like understanding cybersecurity and breach consequences, likely due to their use for formal tasks. Desktop, mobile, and tablet users follow closely, with minor variations in threat awareness and password practices.

These findings emphasize the influence of gender, academic year, and device type on cybersecurity awareness. Gender analysis reveals balanced awareness with slight variations in specific areas, while academic progression correlates with improved understanding. Device usage highlights laptops' advantage in fostering stronger security practices. By examining these factors, educators and policymakers can identify areas for improvement and develop targeted interventions to enhance students' knowledge and promote a culture of cybersecurity awareness across all demographics.

Table 2. Overall responses for Cybersecurity Awareness Attributes

Attributes	FREQUENCY COUNT					Weighted mean	Quantitative Response	Quantitative Interpretations
	5	4	3	2	1			
A1	181	178	25	2	0	4.4	4	Agree
A2	155	195	33	3	0	4.3	4	Agree
A3	164	187	31	4	0	4.3	4	Agree
A4	198	172	15	1	0	4.5	5	Strongly Agree
A5	216	143	23	2	2	4.5	5	Strongly Agree
A6	162	183	35	6	0	4.3	4	Agree
A7	161	188	36	1	0	4.3	4	Agree
A8	158	182	42	4	0	4.3	4	Agree
A9	180	178	28	0	0	4.4	4	Agree
A10	184	180	21	1	0	4.4	4	Agree
A11	199	167	20	0	0	4.5	5	Strongly Agree
A12	186	181	19	0	0	4.4	4	Agree
A13	203	157	26	0	0	4.5	5	Strongly Agree
A14	160	183	38	5	0	4.3	4	Agree
A15	216	152	16	2	0	4.5	5	Strongly Agree
General Weighted Mean						**4.4**	**4**	**Agree**

Table 2 presents the frequency counts, weighted mean, and quantitative responses for various cybersecurity awareness attributes, with a General Weighted Mean (GWM) of 4.4, indicating a high level of awareness among respondents. Attributes A4 (strong passwords), A5 (caution with personal information), A11 (shared responsibility), A13 (accessible education), and A15 (willingness to learn) scored the highest at 4.5, reflecting strong agreement on key cybersecurity practices. Attributes A2 (threat awareness), A3 (avoiding suspicious links), and A6 (caution with public Wi-Fi) scored slightly lower at 4.3, suggesting areas for improvement. These findings highlight the need for ongoing education to reinforce and sustain cybersecurity best practices.

Level of cybersecurity education among CatSU students in terms of its demographic profile

The table below summarizes 15 key statements reflecting various aspects of cybersecurity education, such as prior experiences, preferred learning methods, and beliefs about the importance and delivery of cybersecurity education. These characteristics highlight attitudes and expectations about how cybersecurity knowledge is acquired and applied, providing a foundation for comparing trends across gender groups or other demographic factors.

Table 3. Cybersecurity Education Experiences

Code	Attribute Description
E1	I have received formal cybersecurity education or training in the past, such as through school courses, online modules, or workshops.
E2	The cybersecurity education or training I received was informative, engaging, and helped me enhance my cybersecurity knowledge and skills.
E3	I would like to receive additional cybersecurity education or training to further improve my cybersecurity awareness and preparedness.
E4	I find online courses to be a convenient and effective way to learn about cybersecurity.
E5	I prefer hands-on learning experiences, such as workshops or seminars, to gain practical cybersecurity skills.
E6	I believe that interactive games or simulations can be effective tools for engaging learners and teaching cybersecurity concepts.
E7	I would like to receive cybersecurity education or training regularly, at least once a year, to stay updated on the latest threats and trends.
E8	I believe that schools and universities should prioritize cybersecurity education and integrate it into their curricula for all students.
E9	I support the idea of making cybersecurity education mandatory for all students, regardless of their academic discipline.
E10	I believe that cybersecurity education should be tailored to the specific needs and interests of different student groups.
E11	I prefer cybersecurity education that focuses on practical skills and knowledge that can be directly applied to real-world scenarios.
E12	I believe that cybersecurity education should be engaging, interactive, and incorporate multimedia elements to enhance learning.
E13	I support the involvement of qualified and experienced cybersecurity professionals in developing and delivering cybersecurity programs.
E14	I believe that cybersecurity education should be regularly updated to reflect the latest threats, vulnerabilities, and emerging trends.
E15	I strongly believe that cybersecurity education is essential for students to become responsible digital citizens and navigate the online world safely.

Figure 8 highlights the general weighted mean and specific responses for cybersecurity education experiences by gender, showing consistent levels of involvement for both male and female respondents, with an overall mean of 4.3. Slight variations are observed in individual experiences (E1–E15), with females scoring marginally higher in E5, E10, and E14, and males in E7, but these differences are minimal and within the 4.0–4.5 range. The findings indicate that gender does not significantly influence cybersecurity education experiences, as both groups demonstrate high familiarity and satisfaction. Overall, the consistently high scores reflect effective education delivery, with opportunities for continuous improvement.

Figure 8. Level of Cybersecurity Education in terms of Gender

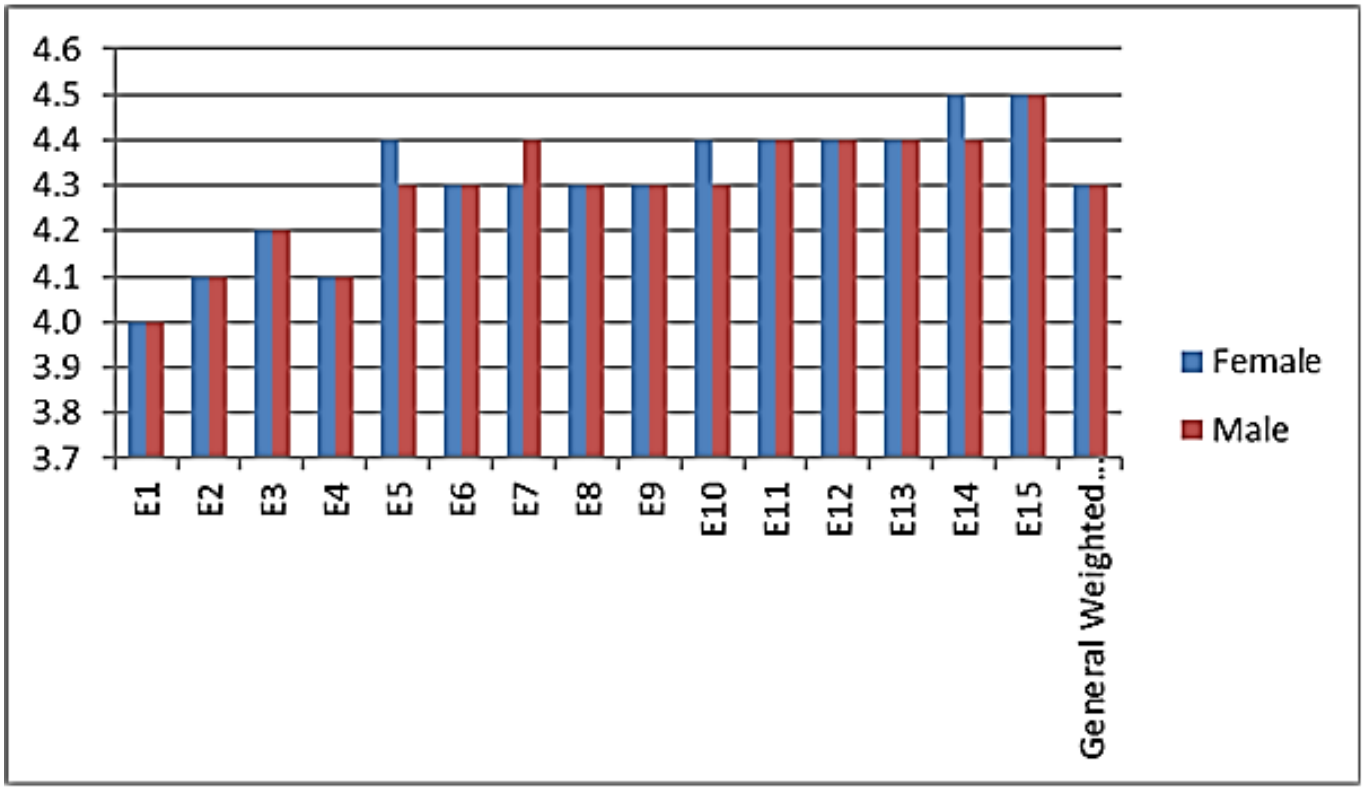


Table 4. Overall responses for Cybersecurity Education Attributes

Attributes	FREQUENCY COUNT					Weighted mean	Quantitative Response	Quantitative Interpretations
	5	4	3	2	1			
E1	120	175	72	18	1	4.0	4	Agree
E2	133	175	67	8	3	4.1	4	Agree
E3	148	183	51	2	2	4.2	4	Agree
E4	129	172	73	10	2	4.1	4	Agree
E5	187	152	46	1	0	4.4	4	Agree
E6	152	191	41	1	1	4.3	4	Agree
E7	169	184	32	1	0	4.3	4	Agree
E8	165	178	39	2	2	4.3	4	Agree
E9	166	179	38	1	2	4.3	4	Agree
E10	173	180	32	0	1	4.4	4	Agree
E11	181	176	29	0	0	4.4	4	Agree
E12	191	171	23	0	1	4.4	4	Agree
E13	180	179	27	0	0	4.4	4	Agree
E14	197	168	21	0	0	4.5	5	Strongly Agree
E15	217	150	19	0	0	4.5	5	Strongly Agree
General Weighted Mean for Cybersecurity Education Experiences						4.3	4	Agree

Figure 9. Level of Cybersecurity Education in terms of Academic Year Level

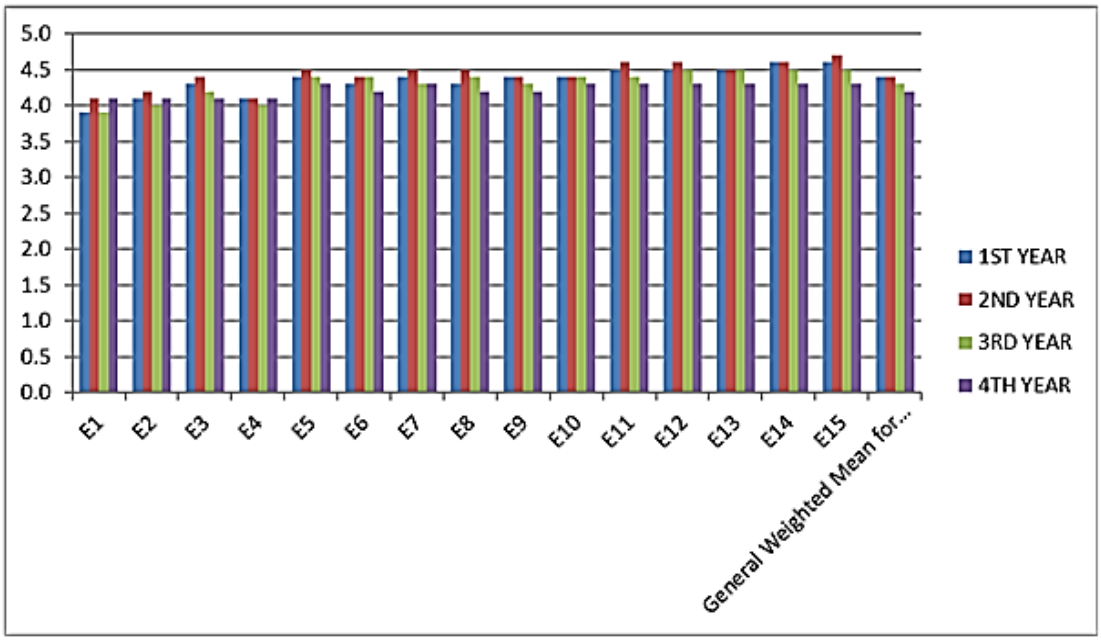


Figure 10. Level of Cybersecurity Education in terms of Internet Access Device

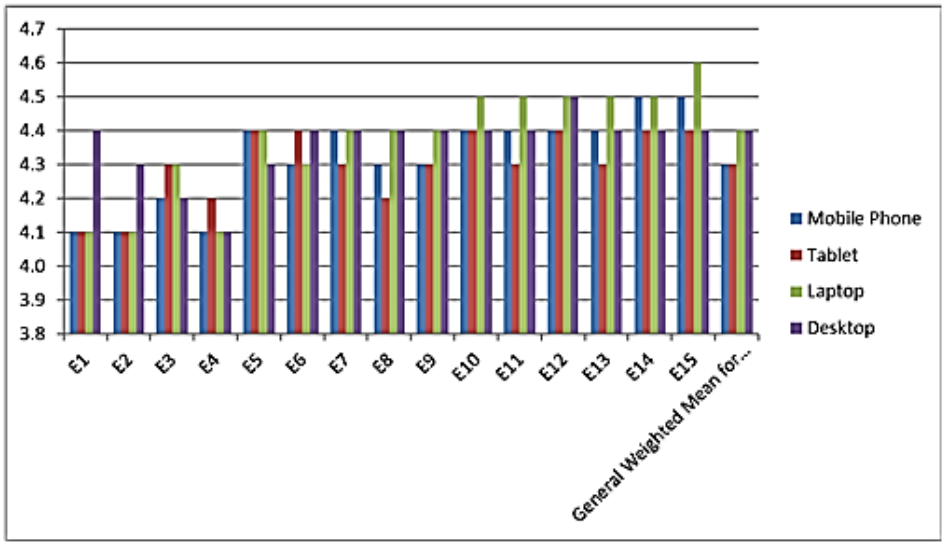


Figure 9 shows slight variations in cybersecurity education experiences across academic year levels, with a general weighted mean decreasing from 4.4 in the 1st and 2nd years to 4.3 in the 3rd year and 4.2 in the 4th year. This suggests a diminishing perception of engagement or satisfaction as students advance academically. Second-year students report the highest scores, especially in items E11 to E15 (4.6–4.7), while fourth-year students show lower scores, particularly in areas like E6 to E9. These results may indicate that while early exposure to cybersecurity concepts is well-received, engagement declines over time, possibly due to increased workloads or content redundancy. Introducing advanced, practical applications in higher year levels could help sustain interest and satisfaction. Figure 10 compares device categories, showing that Laptops and Desktops consistently achieve higher scores, particularly in E10, E11, and E15, while Mobile Phones and Tablets have slightly lower averages, especially in E1, E3, and E8. Despite these differences, performance converges in most items, with Laptops and Desktops being more preferred or effective across the evaluated criteria.

The overall data on cybersecurity education experiences reveals a strong positive consensus among students, with a general weighted mean of 4.3, indicating that students generally agree with the effectiveness of their cybersecurity education. Attributes E14 and E15, both scoring 4.5 ("Strongly Agree"), highlight the highest satisfaction, suggesting that practical applications or relevant aspects of the education are particularly well-received. Other attributes, including E5, E10, E11, E12, and E13, also perform well with means of 4.4,

indicating consistent positive feedback. However, attributes such as E1, E2, and E4, with slightly lower means of 4.0 to 4.1, suggest areas for minor improvement. Overall, the results from Table 4 reflect a generally favorable evaluation of students' cybersecurity education experiences.

Relationship between the level of cybersecurity awareness and education among CatSU students

Results from Table 5 show a strong positive correlation (r = 0.670) between the level of cybersecurity awareness and the quality of cybersecurity education among CatSU students, which is statistically significant at the 0.01 level (p = 0.000). This indicates that as students' cybersecurity education improves, their awareness of cybersecurity also increases. The correlation highlights the crucial role of educational initiatives, such as formal training, coursework, and activities, in enhancing students' understanding of cybersecurity risks, practices, and solutions. With a sample size of 386, the data provides strong evidence that education significantly influences students' readiness to engage in secure online behaviors.

Table 5. Relationship between Cybersecurity Awareness and Education

Correlations				
			Awareness	Education
Spearman's rho	Awareness	Correlation Coefficient	1.00	.670**
		Sig. (2-tailed)	.	0.00
		N	386.00	386.00
	Education	Correlation Coefficient	.670**	1.00
		Sig. (2-tailed)	0.00	.
		N	386.00	386.00
** Correlation is significant at the 0.01 level (2-tailed).				
p-value =	0.000			
Interpretation =	Significant			

The significant relationship emphasizes the importance of integrating comprehensive cybersecurity education into the academic curriculum in order to effectively raise awareness. Strengthening educational programs allows students to gain a better understanding of potential threats and learn important skills for protecting themselves in the digital world. This positive correlation also implies that students who receive higher-quality cybersecurity education are better prepared to identify, assess, and address cyber risks, emphasizing the importance of consistent learning opportunities, hands-on training, and exposure to real-world cybersecurity scenarios. Overall, the findings support the notion that targeted education is critical to developing a cyber-aware and resilient student population.

CONCLUSIONS AND RECOMMENDATIONS

The study highlights the crucial connection between cybersecurity education and awareness among CatSU students, showing that effective educational interventions significantly enhance students' ability to recognize and respond to cyber threats. The strong correlation indicates the vital role of structured programs in fostering a cyber-aware student body. Fourth-year students demonstrated higher levels of awareness, likely due to increased academic exposure and practical experience, while first-year students displayed lower awareness, underscoring the need for early cybersecurity education. Disparities in awareness based on device usage were also observed, with laptop users exhibiting higher proficiency due to engagement with tasks requiring stricter security practices. Minimal gender differences suggest equitable access to education, but tailored programs are

still necessary to accommodate diverse learning needs. Overall, these findings emphasize the importance of a comprehensive, curriculum-integrated approach to cybersecurity education to equip students with the skills needed to navigate the digital landscape securely.

To enhance cybersecurity awareness and its practical application among CatSU students, several recommendations are proposed. First, integrating comprehensive cybersecurity education into the core curriculum across all disciplines is essential, ensuring progressive learning from basic to advanced concepts. Tailored training programs should address specific gaps, such as safe public Wi-Fi usage and advanced threat recognition. Device-specific campaigns can raise awareness of cybersecurity best practices for mobile, tablet, and laptop users, addressing unique vulnerabilities. Additionally, regular updates and refresher courses should be introduced to keep students informed of emerging threats and defense mechanisms. Finally, collaboration with cybersecurity experts to develop engaging real-world training programs will help reinforce learning, fostering stronger student engagement and better knowledge retention.

REFERENCES

1. Al Shamsi, A. A. (2019). Effectiveness of Cyber Security Awareness Program for young children: A Case Study in UAE Effectiveness of Cyber Security Awareness Program for young children View project Sentiment Analysis for Arabic Dialects View project Effectiveness of Cyber Security. International Journal of Information Technology and Language Studies (IJITLS), 3(2), 8–29. https://doi.org/10.13140/RG.2.2.28488.14083
2. Alharbi, T., & Tassaddiq, A. (2021). Assessment of cybersecurity awareness among students of Majmaah University. Big Data and Cognitive Computing, 5(2). https://doi.org/10.3390/bdcc5020023
3. Alsiddig, M. D. E., Badwi, A. A. alraheem A., & Idriss, O. I. A. (2020). Cyber security awareness among students and faculty members in a Sudanese college. Electrical Science & Engineering, 2(2), 24–28. https://doi.org/10.30564/ese.v2i2.2477
4. Blažič, B. J. (2021). The cybersecurity labour shortage in Europe: Moving to a new concept for education and training. Technology in Society, 67(September). https://doi.org/10.1016/j.techsoc.2021.101769
5. Brooks, C. (2023). Cybersecurity Trends & Statistics; More Sophisticated And Persistent Threats So Far In 2023. Forbes. https://www.forbes.com/sites/chuckbrooks/2023/05/05/cybersecurity-trends--statistics-more-sophisticated-and-persistent-threats-so-far-in-2023/
6. Corradini, I., & Nardelli, E. (2020). Developing Digital Awareness at School: A Fundamental Step for Cybersecurity Education. In Advances in Intelligent Systems and Computing: Vol. 1219 AISC. Springer International Publishing. https://doi.org/10.1007/978-3-030-52581-1_14
7. Crick, T., Davenport, J. H., Irons, A., & Prickett, T. (2019). A UK Case Study on Cybersecurity Education and Accreditation. Proceedings - Frontiers in Education Conference, FIE, 2019-Octob, 1–16. https://doi.org/10.1109/FIE43999.2019.9028407
8. Erendor, M. E., & Yildirim, M. (2022). Cybersecurity Awareness in Online Education: A Case Study Analysis. IEEE Access, 10, 52319–52335. https://doi.org/10.1109/ACCESS.2022.3171829
9. Garba, A. A., Siraj, M. M., & Othman, S. H. (2022). An assessment of cybersecurity awareness level among Northeastern University students in Nigeria. International Journal of Electrical and Computer Engineering, 12(1), 572–584. https://doi.org/10.11591/ijece.v12i1.pp572-584
10. Mai, P. T., & Tick, A. (2021). Cyber security awareness and behavior of youth in smartphone usage: A comparative study between university students in hungary and Vietnam. Acta Polytechnica Hungarica, 18(8), 67–89. https://doi.org/10.12700/APH.18.8.2021.8.4
11. Maranga, J., Maranga, M. J., & Nelson, M. (2019). Emerging Issues in Cyber Security for Institutions of Higher Education Innovation Methodologies in Information Technology View Project Computer Security View project Emerging Issues in Cyber Security for Institutions of Higher Education. IJCSN-International Journal of Computer Science and Network, 8(4), 371–379. www.IJCSN.org
12. Matyokurehwa, K., Rudhumbu, N., Gombiro, C., & Mlambo, C. (2021). Cybersecurity awareness in Zimbabwean universities: Perspectives from the students. Security and Privacy, 4(2). https://doi.org/10.1002/spy2.141
13. Moallem, A. (2019). Cyber Security Awareness Among College Students. Advances in Intelligent Systems and Computing, 782, 79–87. https://doi.org/10.1007/978-3-319-94782-2_8

14. Mogoane, S. N., & Kabanda, S. (2019). Challenges in Information and Cybersecurity program offering at Higher Education Institutions. 12, 202–190. https://doi.org/10.29007/nptx
15. Mohamed, N. E. (2021). Measuring Cyber Security Awareness of Students : A Case Study at Fahad Bin Sultan University. International Journal of Computer Science and Mobile Computing, 9(6), 141–155.
16. Moletsane, T., & Tsibolane, P. (2020). Mobile Information Security Awareness among Students in Higher Education : An Exploratory Study. 2020 Conference on Information Communications Technology and Society, ICTAS 2020 - Proceedings, November. https://doi.org/10.1109/ICTAS47918.2020.233978
17. NAGYFEJEO, E., & SOLMS, B. Von. (2020). Why Do National Cybersecurity Awareness Programmes Often Fail? International Journal of Information Security and Cybercrime, 9(2), 18–27. https://doi.org/10.19107/ijisc.2020.02.03
18. Potgieter, P. (2019). The Awareness Behaviour of Students on Cyber Security Awareness by Using Social Media Platforms: A Case Study at Central University of Technology. 12, 272–262. https://doi.org/10.29007/gprf
19. Rahim, N. H. A., Hamid, S., & Kiah, M. L. M. (2019). Enhancement of Cybersecurity Awareness Program on Personal Data. Malaysian Journal of Computer Science, 32(3), 221–245.
20. Rahman, N. A. A., Sairi, I. H., Zizi, N. A. M., & Khalid, F. (2020). The importance of cybersecurity education in school. International Journal of Information and Education Technology, 10(5), 378–382. https://doi.org/10.18178/ijiet.2020.10.5.1393
21. Raju, R., Rahman, N. H. A., & Ahmad, A. (2022). Cyber Security Awareness In Using Digital Platforms Among Students In A Higher Learning Institution. Asian Journal of University Education, 18(3), 756–766. https://doi.org/10.24191/ajue.v18i3.18967
22. Ricci, J., Breitinger, F., & Baggili, I. (2019). Survey results on adults and cybersecurity education. Education and Information Technologies, 24(1), 231–249. https://doi.org/10.1007/s10639-018-9765-8
23. Taha, N., & Dahabiyeh, L. (2021). College student's information security awareness: a comparison between smartphones and computers. Education and Information Technologies, 26(2), 1721–1736. https://doi.org/10.1007/s10639-020-10330-0
24. Ulven, J. B., & Wangen, G. (2021). A Systematic Review of Cybersecurity Risks in Higher Education. In Future Internet (Vol. 13, Issue 2). https://doi.org/10.3390/fi13020039
25. Venter, I. M., Blignaut, R. J., Renaud, K., & Venter, M. A. (2019). Cyber security education is as essential as "the three R's." Heliyon, 5(12), 0–7. https://doi.org/10.1016/j.heliyon.2019.e02855
26. ZAHIDAH ZULKIFLI, NURUL NUHA ABDUL MOLOK, NOOR HAYANI ABD RAHIM, S. T. (2020). Cyber Security Awareness Among Secondary School Students in Malaysia. Journal of Information Systems and Digital Technologies, 2(2), 28–41.
27. Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. Journal of Computer Information Systems, 62(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269