Cybersecurity Fundamentals Training Among Middle School Students: Building a Strong Foundation

Qingsong Zhao[1], Urska Cvek[1] and Kevin Zhao[2]
[1]Department of Computer Science, Louisiana State University Shreveport, One University Pl, Shreveport, LA 71115, U.S.A.
[2]Caddo Magnet High School, 1601 Viking Dr, Shreveport, LA 71101, U.S.A.

Keywords: Cybersecurity, Internet Security, Cybersecurity Awareness, Cybersecurity Knowledge, Cybersecurity Fundamentals, Cybersecurity Training, Awareness Evaluation.

Abstract: Cyber threats and cybercrimes pose serious challenges for individuals and organizations. Cybersecurity awareness (CSA) training helps mitigate these risks, but its effectiveness depends on accurately assessing participants' CSA levels. Without a solid understanding of cybersecurity fundamentals (CSF), trainees often overestimate their awareness. This study investigates the impact of foundational cybersecurity knowledge on self-assessment accuracy in a CSA training program. Conducted during a summer camp for 61 middle school students, the research involved five phases of targeted instruction and evaluations. We developed a comprehensive program with pre-, mid-, and post-training evaluations to measure participants' awareness. The findings reveal that while students initially overestimated their CSA, training improved both their quiz scores and self-assessment accuracy. This study provides valuable insights into the design of effective CSA training programs and self-assessment tools, offering practical guidelines for middle school students and broader audiences.

1 INTRODUCTION

In today's digital world, cyber threats pose significant challenges for individuals and organizations (Rawat et al., 2019). Middle school students, heavily reliant on the Internet for education and entertainment, are increasingly exposed to risks like phishing, malware, and cyberbullying (Norton, 2021). Despite frequent technology use, they often lack the knowledge to protect themselves, leaving them vulnerable. Cybersecurity awareness (CSA) involves recognizing risks and best practices, but a solid understanding of cybersecurity fundamentals (CSF) is crucial for effective defense (Al-Shanfari et al., 2020). However, many students lack this foundation, limiting their ability to assess their awareness accurately and fostering a false sense of security (CompTIA, 2024).

While technology is vital, the human factor is critical in mitigating cyber risks (Michael, 2008). Education and training must balance technical concepts with behavioural strategies (Zwilling, Moti, et al., 2022). However, most programs emphasize CSA over CSF, neglecting foundational knowledge critical for applying these concepts (Johnson, 2019). This paper addresses this gap by integrating CSF into CSA education for middle school students, enhancing their self-assessments and cybersecurity practices. It reviews related work, outlines research methodology, presents results, and concludes with findings and recommendations, offering future research directions.

2 RELATED WORK

The fields of CSA and CSA training have recently gained significant attention, with studies investigating methods for improving user understanding of cyber risks and best practices. CSA includes knowledge of security threats, policies, and the ability to respond to digital risks (Akter et al., 2022). Effective CSA training helps users align their actions with organizational security, comply with regulations, and adopt best practices (Bauer, et al., 2017). However, threats like social engineering highlight the need for continuous CSA training (Bitton et al., 2020), as cyber threats evolve.

Research shows that understanding CSA can significantly influence compliance with practices (Lee et al., 2016). Psychological factors such as self-

Zhao, Q., Cvek, U. and Zhao, K.
Cybersecurity Fundamentals Training Among Middle School Students: Building a Strong Foundation.
DOI: 10.5220/0013144500003899
Paper published under CC license (CC BY-NC-ND 4.0)
In *Proceedings of the 11th International Conference on Information Systems Security and Privacy (ICISSP 2025) - Volume 2*, pages 176-183
ISBN: 978-989-758-735-1; ISSN: 2184-4356
Proceedings Copyright © 2025 by SCITEPRESS – Science and Technology Publications, Lda.

efficacy, risk awareness, and social support play a vital role in shaping CSA (Zhou et al., 2020). Studies have explored the relationship between CSA, CSF, and behavior in various populations. For instance, Zwilling et al. (2022) found that higher CSF knowledge correlates with CSA. Bauer et al. (2017) observed that well-designed security training improves CSA in the banking sector.

Different methodologies to enhance CSA include a cost-benefit analysis framework to optimize training (Zhang et al., 2021), and research on gaming technology in cybersecurity education (Alotaibi et al., 2016). Hijji and Alam (2022) proposed a CSA training framework for remote workers, which proved effective. Most CSA programs focus on adults in corporate settings, though there is a lack of CSA among academic staff, students, and parents (Ahmad et al., 2018). Ahmad et al. (2018) also highlight the moderate CSA among parents, emphasizing the importance of early cybersecurity education.

Interest in children’s CSA is increasing due to the rise in Internet use among youth. Studies have explored risks like password practices, online privacy, and phishing (Prior & Renaud, 2020), and platforms have been developed to teach children about these risks (Desimpelaere et al., 2020). Despite this, children's CSA programs are fewer than those for adults (Sulaiman et al., 2022). Overall, CSA plays a critical role in mitigating cyber threats, and continuous, tailored education is essential. Future research should focus on innovative methods to address evolving cybersecurity threats.

3 RESEARCH METHODOLOGY

The research methodology aims to identify gaps between students' self-assessed and actual CSA, examine the CSA-CSF relationship, and test strategies to improve both through targeted training.

3.1 Aims

The study aims to: 1. Identify disparities between middle school students' self-assessed and measured CSA levels using Likert scale surveys and quizzes; 2. Examine the relationship between self-assessed CSA and CSF understanding using self-reported surveys and quizzes; 3. Test strategies to enhance CSA and CSF through targeted training modules in a summer camp setting.

3.2 Research Questions

This study addresses the following research questions: 1. How accurately do students' self-assessed CSA levels reflect their actual CSA as measured by quizzes? 2. What factors contribute to discrepancies between students' self-assessments and their actual CSA, such as gaps in understanding key cybersecurity threats? 3. Which educational content most effectively enhances both self-assessed and actual CSA?

3.3 Research Hypotheses

Our research is guided by the following hypotheses: H1: Students tend to overestimate their CSA levels compared to their actual CSA; H2: Instruction in CSF significantly improves students' CSF knowledge as measured by quiz performance; H3: Increased understanding of CSF leads to more accurate self-assessment of CSA; H4: Practical CSA training improves the students' actual CSA levels; H5: Engaging in CSA training and practice improves students' self-assessed CSA.

4 RESEARCH DESIGN

The research methodology aims to identify gaps between students' self-assessed and actual CSA, examine the CSA-CSF relationship, and test strategies to improve both through targeted training.

4.1 Participants and Demographics

This research was part of the LSU Shreveport Summer Cybersecurity Camp (LSUS IRB #2023-061), a 4-week program offering 3 hours of daily cybersecurity awareness training for middle school students. Funded by LSUS Continuing Education, the camp was offered free of charge and open to all regional middle school students. Of the 69 students who registered, 61 completed the camp and all related surveys, while the remaining 8 did not finish and were excluded from the study.

Table 1: Participant demographic information.

Variable	Items	n	Percentages %
Sex	Female	29	47.5%
	Male	32	52.5%
Grade	6th	18	29.5%
	7th	22	36.0%
	8th	21	34.5%

Participant demographics are outlined in Table 1, showing that our overall population was approximately half female and half male and equally distributed across the three middle school grades (grades 6-8). Our sex distribution within each grade was similar (although the data is not shown).

4.2 Phases

The study was organized into five phases, aimed at evaluating and enhancing specific aspects of CSA and CSF.

Phase 1: Initial Survey: Phase 1 involved baseline data collection to measure students' CSA and CSF: 1. Basic Information Questionnaire: Demographic and educational data; 2. CSA self-evaluation: Students self-assessed their CSA levels; 3. CSA quiz: An objective quiz measured actual CSA; 4. CSF evaluation: A quiz assessed CSF knowledge.

Phase 2: CSF Instruction: Following Phase 1, students participated in two weeks (750 minutes) of CSF lessons. Topics included Cybersecurity Terminology, Information System Components, Threats, Ethical Hacking, Incident Response, and Encryption. The lessons involved slides, lectures, discussions, games, and hands-on activities.

Phase 3: Midterm Survey: After CSF instruction, students reassessed their CSA (self-evaluation) and took a CSF quiz to measure improvements.

Phase 4: CSA Instruction and Practice: Phase 4 aimed to improve CSA with lectures and activities covering Password Security, Phishing, Privacy Protection, Social Engineering, and Malware. The content was tailored to address security in daily activities such as smartphone use, social media, and gaming. Students worked in small groups, completing quizzes and receiving feedback to refine the training.

Phase 5: Final Survey: The final phase assessed the program's impact: 1. Final CSA self-evaluation: Students rated their CSA as in earlier phases; 2. Final Quiz: A final quiz compared CSA with previous evaluations.

Table 2: Study Phases (x denotes conducting the action).

Phase	Basic Info Questionnaire	CSA Self-Evaluation	CSA Quiz-Evaluation	CSF Quiz-Evaluation
1	x	x	x	x
2				
3		x		x
4				
5		x	x	

This multi-phase design enables a thorough analysis of students' self-perceived and actual CSA, CSF training effectiveness, and the impact of practical CSA improvements. The five phases and corresponding surveys are illustrated in Table 2.

4.3 Survey Design

The questionnaires were designed to collect comprehensive data through four assessments: basic information, CSA self-evaluation, CSA quiz, and CSF quiz. These were based on the NIST/NICE framework (NICE 2020) and other research studies (Zwilling et al., 2022).

Table 3: CSA evaluation questions.

CSA Key Area	CSA Question Group
Password	CSA 1: I understand password and password security
	CSA 2: I take steps to create and use strong passwords
Phishing	CSA 3: I am aware of common phishing attacks
	CSA 4: I follow best practices protect against email phishing
ID and Privacy	CSA 5: I know ID and privacy and how to protect them
	CSA 6: I practice safe behaviour to protect my Personally Identifiable Information
Social Engineering Attack	CSA 7: I can identify social engineering attacks
	CSA 8: I take measures to avoid social engineering attack
Malware	CSA 9: I am aware of malware and malware attacks
	CSA 10: I leverage resources to mitigate malware risks

Basic Information Questionnaire: Gathered demographic and background data, including device usage, cyber risk perceptions, training, and experiences with cyber incidents.

CSA Self-Evaluation (Table 3): Measured students' confidence in cybersecurity across five areas (Password Security, Phishing, ID Protection, Social Engineering, and Malware) using a Likert scale. Two sets of questions per area assessed awareness and practical application, scored from 0 to 10, totalling up to 100 points.

CSA Quiz-Evaluation (Table 3): Assessed students' actual knowledge in the same five areas through objective questions, similar to the self-evaluation, with scores totalling 100 points.

CSF Quiz-Evaluation (Table 4): Evaluated knowledge in five critical cybersecurity domains: Cybersecurity Basics, System Components, Risks & Access Management, Identification & Authentication, and Ethical Hacking & Incident Response, with scores totalling 100 points.

Cronbach's alpha was calculated for reliability: CSA Self-Evaluation (0.90), CSA Quiz (0.77), and CSF Quiz (0.73), indicating acceptable reliability.

The survey design provided valuable insights into students' cybersecurity awareness, revealing discrepancies between perceived and actual knowledge, guiding the development of targeted educational strategies to improve cybersecurity competency.

Table 4: CSF evaluation questions.

CSF Key Area	CSF Question Group
Cybersecurity Basics	CSF 1: Understanding Key Cybersecurity Terms and Definitions
	CSF 2: Core Cybersecurity Principles and Best Practices
System Components & Network	CSF 3: Critical Information System Components and Their Roles
	CSF 4: Networking Fundamentals for Cybersecurity
Risks & Access Management	CSF 5: Identifying and Managing Risks, Threats, and Vulnerabilities
	CSF 6: Implementing Effective Access Control Strategies
Identification, Authentication & Encryption	CSF 7: Techniques for Identification and Authentication in Cybersecurity
	CSF 8: Data Encryption Methods and Their Importance in Cybersecurity
Ethical Hacking & Incident Response	CSF 9: Ethical Hacking: Methods and Techniques for Testing Security
	CSF 10: Developing and Implementing Effective Incident Response Plans

5 RESULTS AND ANALYSIS

This section presents the study's findings, comparing assessments before and after the training.

5.1 Descriptive Statistics

The research was conducted through a free CSA training summer camp for middle school students, with 61 out of 69 participants completing the program and surveys. Participant demographics (Table 1) indicate an equal gender distribution and a balanced representation across grades 6-8 (ages 12 to 14).

Table 5: Basic information questionnaire results.

Variable	Items	n	%
Internet Daily Usage	1 – 3 Hours	15	24.6%
	4 – 6 Hours	32	52.4%
	7 and above	14	23.0%
Top 3 Activities	Videos/Movie	53	86.9%
	Gaming	42	68.9%
	Music	41	67.2%
	Chatting	30	49.2%
	Learning	14	23.0%
Very Familiar Apps	Video Games	42	68.9%
	Web Browsers	38	62.3%
	Social Media Apps	30	49.2%
Biggest Cyber Risk Perception	Identity theft	17	27.9%
	Losing data	16	26.2%
	Violation of privacy	13	21.3%
	Financial loss	8	13.1%
	Being influenced by misinformation	7	11.5%
Device Usage	Smartphone	42	68.9%
	Personal Computer (Desktop/Laptop)	18	29.5%
	Tablet	1	1.6%
Received Formal Training	Yes	24	39.3%
	No	37	60.7%
Parental Control	Yes	36	59.0%
	No	25	41.0%
Cyber Incident Vitim	Yes	14	23%
	No	47	77%

The study first collected basic demographic information and cybersecurity-related behaviours among the participants. Table 5 summarizes the data, highlighting that 52.4% of students spend 4-6 hours on the Internet daily, with the top three activities being watching videos/movies (86.9% of students), gaming (68.9% of students), and listening to music (67.2% of students). Most students identified themselves as very familiar with video games (68.9% of students) and web browsers (62.3% of students), while identity theft (27.9% of students) and losing data (26.2% of students) were perceived as the biggest cybersecurity risks. Interestingly, 39.3% of students had previously received formal cybersecurity training, and 59.0% of students reported parental control over their Internet usage. Notably, 23% of students had experienced a cyber-incident in the past.

5.2 Survey Data

This section presents the students' self-assessed CSA scores, CSA quiz scores, and CSF quiz scores collected from the initial, midterm, and final surveys in the project.

5.2.1 Initial Survey Data

The initial survey assessed students' CSA through self-evaluation and quiz evaluations. Table 6 shows that students generally rated themselves higher in CSA than their quiz results reflected. For example, the average of self-evaluation was 6.78, while the quiz-evaluation average was only 4.18. This discrepancy was consistent across all categories, indicating an overestimation of their CSA.

Similarly, the initial quiz-evaluation of CSF revealed low scores across the board (Table 7). For instance, the average score for CSF was 2.86, indicating a need for improved understanding of basic cybersecurity principles.

Table 6: Initial self-evaluation and quiz-evaluation of CSA.

Question Group	Self-evaluation		Quiz-evaluation	
	Mean	Standard Deviation	Mean	Standard Deviation
CSA 1	6.40	3.33	4.67	3.22
CSA 2	6.78	3.09	3.77	3.06
CSA 3	6.14	3.06	4.47	3.11
CSA 4	6.69	3.20	4.8 0	3.46
CSA 5	7.12	3.08	4.47	3.71
CSA 6	6.48	3.51	3.61	3.55
CSA 7	6.40	3.54	3.73	3.38
CSA 8	6.78	3.09	3.52	3.43
CSA 9	7.50	2.80	4.51	3.59
CSA 10	7.54	3.07	4.26	3.77
Average	6.78	3.18	4.18	3.43

Table 7: Initial quiz-evaluation of CSF.

Question Group	Quiz-evaluation	
	Mean	Standard Deviation
CSF 1	1.93	2.69
CSF 2	3.28	3.25
CSF 3	3.40	3.27
CSF 4	1.93	2.45
CSF 5	3.57	3.46
CSF 6	2.21	2.97
CSF 7	2.42	2.93
CSF 8	4.02	3.37
CSF 9	3.07	3.08
CSF 10	2.79	2.83
Average	2.86	3.03

5.2.2 Midterm Survey Data

After 2-week instruction on CSF, a midterm survey was conducted. The results, presented in Tables 8 and 9, showed modest improvements in students' self-evaluation scores for CSA. However, the quiz evaluations for CSF indicated significant gains, as the average score increased from 2.86 to 6.14. This suggests that the instructional content was effective in enhancing students' fundamental cybersecurity knowledge.

Table 8: Midterm self-evaluation of CSA.

Question Group	Self-evaluation	
	Mean	Standard Deviation
CSA 1	4.63	3.32
CSA 2	6.15	3.4
CSA 3	4.18	3.22
CSA 4	4.75	3.38
CSA 5	5.70	3.60
CSA 6	4.71	3.57
CSA 7	5.00	3.48
CSA 8	5.41	3.48
CSA 9	5.45	3.66
CSA 10	4.26	3.31
Average	5.02	3.44

Table 9: Midterm quiz-evaluation of CSF.

Question Group	Quiz-evaluation	
	Mean	Standard Deviation
CSF 1	5.49	3.5
CSF 2	5.86	3.44
CSF 3	6.56	3.51
CSF 4	6.68	3.41
CSF 5	5.66	3.59
CSF 6	5.94	3.54
CSF 7	6.23	3.38
CSF 8	6.60	3.33
CSF 9	7.09	2.97
CSF 10	5.29	3.74
Average	6.14	3.44

5.2.3 Final Survey Data

The final survey, conducted after the completion of all instructional phases, showed further improvement in both self-evaluation and quiz-evaluation scores for

CSA (Table 10). The average score for CSA in the self-evaluation rose to 6.84, closely matching the quiz-evaluation score of 6.74. This alignment between self-evaluation and quiz results indicates that students' perceptions of their cybersecurity awareness had become more accurate by the end of the program.

Table 10: Final self-evaluation and quiz-evaluation of CSA.

Question Group	Self-evaluation		Quiz-evaluation	
	Mean	Standard Deviation	Mean	Standard Deviation
CSA 1	6.93	3.25	7.13	3.26
CSA 2	6.72	3.15	6.43	3.34
CSA 3	6.52	3.69	6.48	3.72
CSA 4	6.80	3.39	7.25	3.03
CSA 5	7.13	3.20	6.56	3.33
CSA 6	7.01	2.89	6.19	3.22
CSA 7	6.89	3.53	6.80	2.97
CSA 8	6.72	3.37	7.09	3.14
CSA 9	6.52	3.15	7.09	3.17
CSA 10	7.13	3.38	7.35	3.22
Average	6.84	3.30	6.84	3.24

5.3 Statistical Analysis

This section presents the students' self-assessed CSA scores, CSA quiz scores, and CSF quiz scores on line charts (Figure 1 – Figure 5), demonstrating that the data supports all hypotheses (H1-H5).

5.3.1 H1: Students Tend to Overestimate Their CSA Levels Compared to Their Actual CSA

By comparing the initial CSA self-evaluation scores with the initial CSA quiz evaluation scores, Figure 1 indicates that students who struggle to accurately assess their CSA levels tend to overestimate their capabilities.

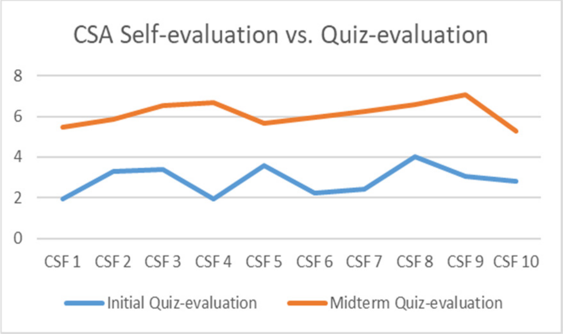

Figure 1: CSA self-evaluation vs. quiz-evaluation.

5.3.2 H2: Instruction in CSF Significantly Improves Students' CSF Knowledge as Measured by Quiz Performance

By comparing the initial CSF quiz evaluation scores with the midterm quiz evaluation scores obtained after CSF instruction, Figure 2 demonstrates that students have significantly improved their CSF knowledge.

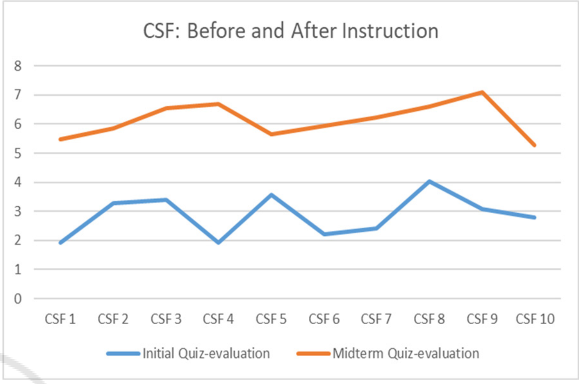

Figure 2: CSF before and after instruction.

5.3.3 H3: Increased Understanding of CSF Leads to More Accurate Self-Assessment of CSA

Figure 3 compares CSA self-evaluation scores before and after CSF instruction, clearly indicating that students were able to self-assess their CSA more accurately after acquiring greater CSF knowledge.

5.3.4 H4: Practical CSA Training Improves the Students' Actual CSA Levels

Figure 4 compares students' final quiz-evaluation scores before and after CSA instruction, demonstrating that the instruction significantly enhances CSA levels.

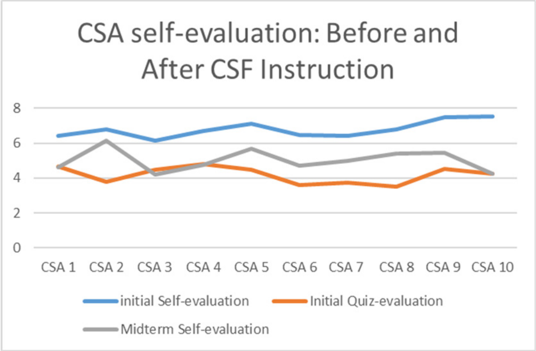

Figure 3: CSA self-evaluation before and after CSF instruction.

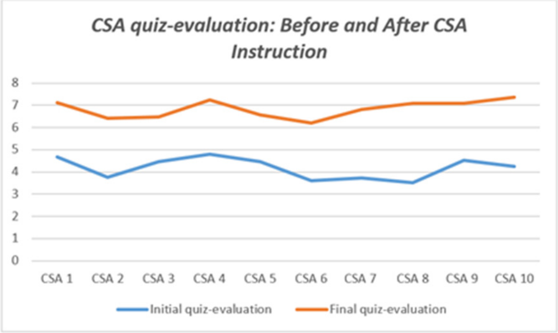

Figure 4: CSA quiz-evaluation before and after CSA instruction.

5.3.5 H5: Engaging in CSA Training and Practice Improves Students' Self-Assessed CSA

The absolute difference between the Initial CSA Self-evaluation and Initial CSA Quiz-evaluation highlights the disparity in how students assessed their CSA before the program. Similarly, the absolute difference between the Final CSA Self-evaluation and Final CSA Quiz-evaluation reflects their evaluation accuracy after the program. Figure 5 shows a significant reduction in this disparity following the program, indicating a notable improvement in students' ability to accurately evaluate their CSA.

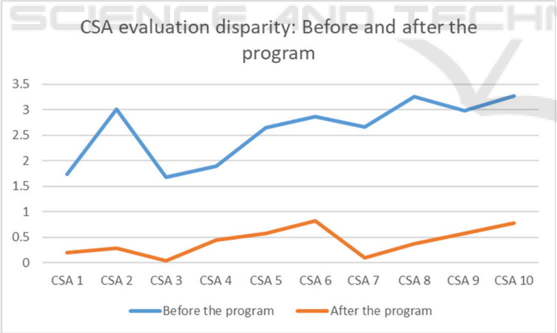

Figure 5: CSA evaluation disparity: before and after the program.

5.4 Paired Sample T-Tests

Additionally, we conducted paired sample t-tests to evaluate the statistical significance of the observed changes. Table 11 summarizes the results, confirming that all hypotheses are upheld by the data. The t-tests consistently produced very low p-values, indicating that the training had a significant positive impact on both self-evaluation and quiz scores.

Table 11: Research Analysis.

#	Data	Result
H1	Initial CSA Self-evaluation vs. Initial CSA Quiz-evaluation	t-statistic: 42.294 p-value: 0.000
H2	Initial CSF Quiz-evaluation vs. Midterm CSF Quiz-evaluation	t-statistic: -25.800 p-value: 0.000
H3	Absolute difference between Initial CSA Self-evaluation and Initial CSA Quiz-evaluation vs. Absolute difference between Midterm CSA Self-evaluation and Initial CSA Quiz-evaluation	t-statistic: 18.404 P-value: 2.343e-26
H4	Initial CSA Quiz-evaluation vs. Final CSA Quiz-evaluation	t-statistic: 26.5935 p-value: 6.6865e-35
H5	Absolute difference between Initial CSA Self-evaluation and Initial CSA Quiz-evaluation vs. Absolute difference between Final CSA Self-evaluation and Final CSA Quiz-evaluation	t-statistic: 20.4914 p-value: 8.8948e-29

6 CONCLUSIONS

The statistical analysis confirms that the CSA and CSF training provided during the camp significantly improved students' cybersecurity awareness. The alignment between students' self-evaluations and their quiz-evaluation scores by the end of the camp suggests that the program effectively enhanced both their actual knowledge and their ability to accurately self-assess that knowledge. This highlights the importance of CSA and CSF training in cybersecurity education.

7 FUTURE WORK

Future research should explore the long-term retention of cybersecurity knowledge among middle school students and investigate the effectiveness of different teaching methods in various educational settings. Additionally, expanding the study to include a more diverse group of students and exploring the role of parental involvement in cybersecurity education could provide further insights into improving cybersecurity awareness at a young age.

REFERENCES

Rawat, Danda B., Doku, Ronald, & Garuba, Moses. (2019). "Cybersecurity in Big Data Era: From Securing Big Data to Data-Driven Security." Proceedings of the IEEE International Conference on Services Computing (SCC), 2019, pp. 10-1109. https://doi.org/10.1109/TSC.2019.2907247.

"Understanding Cyber Threats." Norton. Retrieved from https://us.norton.com/internetsecurity-malware-what-are-cyber-threats.html (This is a website source and not a conference proceeding.)

Al-Shanfari, Issam, Mohamed, Warusia, & Abdullah, Raihana. (2020). "Identify of Factors Affecting Information Security Awareness and Weight Analysis Process." Proceedings of the International Conference on Advances in Engineering and Technology Research, 2020, vol. 9, pp. 2249-8958. https://doi.org/10.35940/ijeat.C4775.029320.

"Cyber Security Fundamentals." (2024). CompTIA. Retrieved from https://www.comptia.org/ (This is a web source, not a conference proceeding.)

Michael, K. (2008). "Social and Organizational Aspects of Information Security Management." Proceedings of the IADIS e-Society Conference, 9-12 April, Algarve, Portugal, pp. 1-8.

Zwilling, Moti, et al. (2022). "Cyber Security Awareness, Knowledge and Behavior: A Comparative Study." Proceedings of the 62nd International Conference on Information Systems and Security, Jan. 2022, pp. 82–97. https://doi.org/10.1080/08874417.2020.1712269.

Alotaibi, F., Furnell, S., Stengel, I., & Papadaki, M. (2016). "A Review of Using Gaming Technology for Cyber-Security Awareness." Proceedings of the International Conference on Information Systems and Security Research, 2016, vol. 6(2), pp. 660-666.

Johnson, M. (2019). "Cybersecurity Awareness Training: Why it Fails." Proceedings of the 12th International Conference on Information Security and Privacy, 2019, pp. 121-127.

Akter, Shahriar, et al. (2022). "Reconceptualizing Cybersecurity Awareness Capability in the Data-Driven Digital Economy." Proceedings of the Annals of Operations Research International Conference, Aug. 2022. https://doi.org/10.1007/s10479-022-04844-8.

Bauer, S., & Bernroider, E. W. (2017). "An Empirical Study of Information Security Awareness Programs in the Banking Sector." Proceedings of the International Conference on Information Security and Applications, 2017, vol. 35, pp. 23-33.

Bitton, R., Gonen, Y., Giyora, I., & Elovici, Y. (2020). Phishing attacks detected: Leveraging phishing awareness to predict training improvements. Information Security Journal: A Global Perspective, 29(1), 18-30.

Lee, S. Y., & Rao, H. R. (2016). Cybersecurity Awareness Capabilities (CSAC): Impact on cybersecurity compliance. Journal of Computer Information Systems, 56(4), 310-319.

Zhou, Y., Zhang, Y., Wu, X., & Chen, D. (2020). Exploring psychological factors in cybersecurity awareness: Self-efficacy, risk awareness, and social support. Computers in Human Behavior, 107, 106281.

Zwilling, M., Netzer, D., Dell, M., & Yechezkel, G. (2022). The influence of cybersecurity awareness on the adoption of cybersecurity tools across countries. Computers & Security, 108, 102319.

Zhang, Z., He, W., Li, W., & Abdous, M. H. (2021). Cybersecurity awareness training programs: A cost–benefit analysis framework. Industrial Management & Data Systems, 121(3), 613-636.

Hijji, M., & Alam, G. (2022). Cybersecurity Awareness and Training (CAT) framework for remote working employees. Sensors, 22(22), 8663.

Ahmad, N., Mokhtar, U. A., Fauzi, W. F. P., Othman, Z. A., Yeop, Y. H., & Sheikh Abdullah, S. N. H. (2018). Cyber Security Situational Awareness among Parents. 2018 Cyber Resilience Conference (CRC), Putrajaya, Malaysia, pp. 1-3. doi: 10.1109/CR.2018.8626830.

Prior, S., & Renaud, K. (2020). Age-appropriate password “best practice” ontologies for early educators and parents. International Journal of Child-Computer Interaction, 23–24, Article 100169.

Desimpelaere, L., Hudders, L., & Van de Sompel, D. (2020). Knowledge as a strategy for privacy protection: How a privacy literacy training affects children’s online disclosure behavior. Computers in Human Behavior, 110, Article 106382.

Sulaiman, N. S., et al. (2022). A Review of Cyber Security Awareness (CSA) Among Young Generation: Issue and Countermeasure. In Al-Emran, M., Al-Sharafi, M. A., Al-Kabi, M. N., & Shaalan, K. (Eds.), Proceedings of International Conference on Emerging Technologies and Intelligent Systems. ICETIS 2021. Lecture Notes in Networks and Systems (Vol. 322). Springer, Cham. https://doi.org/10.1007/978-3-030-85990-9_76

National Institute of Standards and Technology (NIST). (2020). National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NIST Special Publication 800-181 Rev. 1). https://doi.org/10.6028/NIST.SP.800-181r1.