



Learning Cybersecurity Through Play: The Effectiveness of CyberMonopoly as a Serious Board Game for Junior High School Students

Panca Desti Ratnaningrum, Rizki Hikmawan*

Department of Information Systems and Technology Education, Universitas Pendidikan Indonesia, Purwakarta Campus, Indonesia.

*Corresponding Author. Email: hikmariz@upi.edu

Abstract: This study aims to implement CyberMonopoly, a serious board game-based learning medium designed to align with the characteristics of junior high school students, and evaluate its effectiveness in improving their understanding of fundamental cybersecurity concepts. The study employed a quantitative approach using a pre-experimental one-group pretest-posttest design. The participants comprised 26 eighth-grade students from SMP Negeri 2 Purwakarta, Indonesia, who were selected through saturated sampling. Data were collected using a 20-item questionnaire administered before and after the learning intervention. The data were analyzed using descriptive statistics, the Shapiro-Wilk normality test, the Wilcoxon signed-rank test, and N-gain analysis. The findings showed an increase in the mean score from 52.85 on the pretest to 89.31 on the posttest. The Wilcoxon signed-rank test revealed a statistically significant difference between the pretest and posttest scores ($Z = -4.461$, $p < .001$), with all 26 participants showing an improvement in their scores. Furthermore, the mean N-gain score was 0.78, indicating a high level of improvement. Students also demonstrated active participation and positive interactions throughout the learning activities. The novelty of this study lies in the development and empirical evaluation of a non-digital board game-based learning medium that presents cybersecurity concepts within contexts relevant to junior high school education. Overall, CyberMonopoly shows potential as an innovative supplementary learning medium for strengthening students' understanding of fundamental cybersecurity concepts.

Article History

Received: 17-06-2026

Revised: 11-08-2026

Accepted: 04-09-2026

Published: 20-10-2026

Key Words:

Board Game;

Cybersecurity Learning;

Cybermonopoly;

Serious Game.

How to Cite: Ratnaningrum, P. D., & Hikmawan, R. (2026). Learning Cybersecurity Through Play: The Effectiveness of CyberMonopoly as a Serious Board Game for Junior High School Students. *Jurnal Paedagogy*, 13(4), 1524-1531. <https://doi.org/10.33394/jp.v13i4.21329>



<https://doi.org/10.33394/jp.v13i4.21329>

This is an open-access article under the [CC-BY-SA License](#).



Introduction

The massive development of digital transformation in Indonesia has placed junior high school students as one of the most active groups of internet users, both for learning purposes and daily social activities (Liberty Jemadu & Dicky Prastya, 2021). However, the high intensity of the use of digital technology has not been balanced with adequate cybersecurity readiness and awareness among students. Data shows that Indonesia has experienced hundreds of millions of cyberattacks, with various forms of threats such as phishing, malware, and data leaks potentially targeting various groups of users, including students (Radip, 2023). This condition is exacerbated by the lack of a formal curriculum that explicitly discusses cybersecurity literacy at the junior secondary education level, so that most students do not have enough basic knowledge to protect themselves in the digital space (Paundu et al., 2026). Therefore, strengthening cybersecurity literacy since junior high school is an urgent need, considering that the digital threats faced by students are real, complex, and constantly evolving (Ibrahim et al., 2024). This condition shows that there is a



gap between the level of exposure to students' digital technology and their cybersecurity literacy readiness.

In response to this need, various efforts have been made to integrate cybersecurity education into learning practices, one of which is through a serious gaming approach. Serious games are defined as games that are designed with the primary purpose of education or training, not just entertainment (Prasetya & Syidada, 2025). In the context of cybersecurity education, serious games have proven to be effective in improving students' understanding of concepts because they present digital risk scenarios in a contextual and interactive manner (Raffaghelli et al., 2022). However, most serious game development for cybersecurity learning is still dominated by screen-based digital formats, such as computer simulations and online game applications, which are capable of realistically representing the cyber environment (Alnajim et al., 2023). Nonetheless, digital game-based learning tends to place students on individualistic learning activities, where there is more interaction between players and game systems than with fellow students (Ahamed et al., 2024). Therefore, an alternative learning approach is needed that not only focuses on understanding concepts, but is also able to create more active learning engagement.

In response to these conditions, serious board games emerged as an alternative to a promising learning approach (Rahmawati & Ratnawati, 2024). Educational board games are designed to convey specific concepts and scenarios through face-to-face co-play activities (Souvi et al., 2024). In the context of cybersecurity education, a game-based approach has proven effective in increasing awareness and understanding of risks through simulations that resemble real conditions (Hart et al., 2020). Serious games are also able to create an active learning environment that encourages participants to understand concepts through hands-on experience (Jayakrishnan et al., 2023). This approach is supported by Experiential Learning Theory, which explains learning as a process of transforming concrete experiences into knowledge through reflection, conceptualization, and active experimentation (Radović et al., 2022). In CyberMonopoly, students experience cybersecurity scenarios through gameplay and apply the concepts learned to subsequent game situations, helping connect abstract cybersecurity concepts with concrete learning experiences. Additionally, board games allow for more intense social interaction than digital-based learning (Rye & Torres, 2023). In this context, CyberMonopoly was developed as a serious board game that adapts Monopoly's mechanics to represent the digital asset ecosystem, cyber threats, and data protection strategies. The selection of Monopoly as a basic mechanical framework is based on the student's level of familiarity with the game (Malik et al., 2020).

Although research on serious games in cybersecurity learning has grown rapidly, there are still a number of research gaps that need to be addressed. First, most research still focuses on digital-based approaches and gamification, while empirical studies on the use of non-digital games such as board games in the context of cybersecurity learning are still relatively limited. Second, existing research generally emphasizes more on improving cognitive aspects without directly testing the effectiveness of learning media in the context of real classes at the junior high school level (Sailer & Homner, 2020). Third, the development of structured and contextual cybersecurity learning, especially for school-age students, is still a challenge in its implementation (Blažič, 2024). However, there have not been many studies that have empirically tested the effectiveness of board games in cybersecurity learning in the context of junior high school students in Indonesia through experimental design in real classrooms. Therefore, this study seeks to fill this gap through the development of



CyberMonopoly as a board game-based learning media that is implemented directly in learning to test students' increased understanding of cybersecurity concepts.

The novelty of this research explicitly lies in three main aspects(Hiranya et al., 2026). First, in terms of media design, CyberMonopoly is a mechanical adaptation of the Monopoly game that systematically represents the concept of the cybersecurity ecosystem, including digital assets, cyber threats, and risk mitigation strategies, which are still limited to be developed and tested in the context of junior high school learning in Indonesia(Carvalho, 2024). Second, in terms of implementation, this study tested the use of serious board games directly in classroom learning through a pseudo-experimental design(Qomariasih, 2024). Third, in terms of context, this study produces empirical evidence regarding the effectiveness of board games in improving cybersecurity understanding in junior high school students in Indonesia, which is still limited in the international literature(Affan et al., 2024). Thus, this research contributes to the development of innovative learning media and strengthens empirical evidence related to the effectiveness of non-digital game approaches in cybersecurity education.

Building on this background, the present study aims to: (1) examine the implementation of CyberMonopoly as a learning medium for cybersecurity education among junior high school students; and (2) empirically evaluate the effectiveness of CyberMonopoly in enhancing students' understanding of fundamental cybersecurity concepts. From a theoretical perspective, this study contributes to the growing body of research on the use and effectiveness of board game-based learning media in cybersecurity education, an area that remains relatively underexplored. From a practical perspective, the findings are expected to offer evidence-based recommendations for educators and curriculum developers in adopting innovative learning media to enhance cybersecurity literacy among the younger generation.

Research Method

This study adopted a quantitative approach with a pre-experimental research design using a one-group pretest-posttest model. The design involved only one group of participants without a control group or randomization. The participants first completed a pretest to measure their initial understanding, followed by a learning intervention using CyberMonopoly as the instructional medium. After the intervention, a posttest was administered to determine changes in students' understanding of basic cybersecurity concepts.

The research was conducted in March 2026 at SMP Negeri 2 Purwakarta during a single meeting, with the implementation adjusted to the available time allocation for the Informatics subject. The participants comprised 26 eighth-grade students selected through a saturated sampling technique, in which all students from the selected class were included as research participants. During the learning activity, the students were organized into four small groups, with each group consisting of 6–7 students. This grouping was intended to facilitate collaborative learning and support active interaction in accordance with the characteristics of board game-based learning. The design of CyberMonopoly is presented in Figure 1, illustrating the board layout and key components of the game used in the study.



Figure 1. CyberMonopoly Design

CyberMonopoly is a serious board game designed to represent basic cybersecurity concepts through asset-based, threat-based, and protection-based game mechanics. This learning media consists of a game board, 20 security cards, 20 attack cards, dice, game pieces, and game money as a transaction tool. The security cards and attack cards represent threat dynamics and data protection strategies, while other components support the gameplay process. The integration of these elements creates an interactive and contextual learning experience and encourages students' cognitive and social engagement.

The research procedure began with administering a pretest to measure students' initial understanding of cybersecurity concepts. The same instrument was used for both the pretest and posttest, consisting of 20 questionnaire items developed based on the cybersecurity competency indicators. Before data collection, the instrument was reviewed through expert judgment by the academic supervisor to ensure the relevance, clarity, and appropriateness of the items to the learning objectives. The instrument was then empirically tested using Pearson's Product-Moment correlation based on data from 20 respondents. At a 5% significance level, the table r-value was 0.444. The validity test results showed that all 20 items had correlation coefficients ranging from 0.515 to 0.900, with significance values below 0.05. Thus, all items met the criteria for empirical validity. The reliability of the instrument was assessed using Cronbach's Alpha, which yielded a coefficient of 0.911, indicating high internal consistency. The validated instrument was subsequently used in both the pretest and posttest to enable a direct comparison of students' understanding before and after the treatment. Learning activities were then conducted through group-based gameplay using CyberMonopoly. Before gameplay, the researcher explained the rules and game mechanics to the students. During the gameplay, students engaged in group discussions and decision-making based on the threat and protection scenarios presented on the game board and cards. After the activity, students were given a posttest to measure the improvement in understanding.

Data collection was carried out using written test instruments administered during the pretest and posttest stages. The use of paper-based tests was adjusted to school policies that do not allow the use of mobile phone devices during learning. The test instruments were developed based on cybersecurity competency indicators, including understanding of digital assets, types of cyber threats, and data protection strategies, with language adapted to the characteristics of junior high school students.

The data obtained were analyzed quantitatively by comparing pretest and posttest results. The analysis began with a normality test using the Shapiro-Wilk method to determine



data distribution. Since the data did not fully meet the normality assumption, the Wilcoxon Signed Rank Test was used to determine the significance of differences in learning outcomes before and after treatment. In addition, the N-Gain calculation was used to measure the level of improvement in students' understanding.

Results and Discussion

The results are presented based on descriptive and inferential statistical analysis.

Table 1. Descriptive Statistics of Pretest and Posttest Scores

Variabel	N	Average	Min	Max
Pretest	26	52,85	40	65
Posttest	26	89,31	80	100

As presented in Table 1, the implementation of CyberMonopoly resulted in a notable improvement in students' learning outcomes. The mean score increased from 52.85 in the pretest to 89.31 in the posttest. This result indicates that students had a relatively limited initial understanding of basic cybersecurity concepts, which subsequently improved considerably following the learning intervention.

The improvement was observed across the entire group of participants, as reflected in the increase in both the minimum and maximum scores. The minimum score rose from 40 to 80, while the maximum score increased from 65 to 100. These results indicate that the improvement in learning outcomes was experienced broadly by the participants rather than being concentrated among only a few students. To identify the most appropriate statistical analysis for the data, a normality test was subsequently performed using the Shapiro-Wilk method.

Table 2. Normality Test

	Kolmogorof-Smirnov			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Pretest	.126	26	.200*	.955	26	.296
Posttest	.145	26	.171	.917	26	.038

The normality test results indicated that the pretest data followed a normal distribution (Sig. > 0.05), while the posttest data did not meet the assumption of normality (Sig. < 0.05). Consequently, a non-parametric statistical approach was selected for further analysis. The Wilcoxon Signed-Rank Test was employed to determine whether there was a significant difference between the students' pretest and posttest scores.

As presented in Table 3, all 26 participants obtained positive ranks, indicating that their posttest scores were higher than their corresponding pretest scores. There were no negative ranks or ties among the participants. Furthermore, the Wilcoxon Signed-Rank Test results in Table 4 demonstrated a statistically significant difference between the pretest and posttest scores ($Z = -4.461$, $p < 0.001$). This finding confirms that students experienced a significant improvement in their scores following participation in the CyberMonopoly learning activity.

Table 3. Wilcoxon Test

		N	Mean Rank	Sum of Ranks
Posttest - Pretest	Negative Ranks	0a	.00	.00
	Positive Ranks	26b	13.50	351.00
	Ties	0c		



Total	26
Table 4. Wilcoxon Test	
	posttest- pretest
z	-4.461b
Asymp. Sig. (2-tailed)	<.001

All students fall into the positive ranks category, indicating that every student experienced an increase in scores. This demonstrates that the improvement is consistent and not caused by random variation. To measure the magnitude of improvement, the N-Gain score was calculated:

$$N - Gain = \frac{89,31-52,85}{100-52,85} = 0.78 \quad (1)$$

The calculation results show an N-Gain value of 0.78, which is considered high. This indicates that the increase in student understanding is not only statistically significant but also highly effective in the learning context. Therefore, the use of CyberMonopoly media can be considered effective in helping students better understand cybersecurity concepts.

The results of the study showed a significant improvement in students' understanding after the use of CyberMonopoly as a learning medium. This is shown by the increase in the average score from 52.85 in the pretest to 89.31 in the posttest, and reinforced by the results of the Wilcoxon test which showed a significant difference. In addition, the N-Gain value of 0.78 which is in the high category shows that the learning media used is able to provide an effective increase in understanding. This increase not only shows a change in the score quantitatively, but also indicates that CyberMonopoly is able to facilitate a more meaningful learning process. In this context, the use of board games as a learning medium allows students to understand cybersecurity concepts through hands-on experience, rather than just passively receiving information. Play activities that involve decision-making, group discussions, and cyber threat simulations provide opportunities for students to actively construct their understanding.

These findings are in line with the concept of serious games which states that game-based learning can increase student engagement and understanding through contextual and interactive approaches(Prasetya & Syidada, 2025). In addition, the results of this study also state that the use of interactive media in learning is able to increase concept understanding because students are directly involved in the learning process(Raffaghelli et al., 2022). In the context of cybersecurity, simulation-based approaches such as those applied in CyberMonopoly allow students to understand digital risks more realistically(Hart et al., 2020). Furthermore, the effectiveness of CyberMonopoly can also be explained through the board-game-based learning characteristics that emphasize social interaction. In contrast to digital games that tend to be individualized, board games encourage collaboration between students through shared discussions and decision-making. This is in line with research (Rye & Torres, 2023) which states that board games have the advantage of creating more intense social interaction in the learning process. This interaction plays an important role in strengthening students' understanding because there is a direct exchange of ideas and clarification of concepts between students.

In addition, the increase in students' understanding is also influenced by the representation of cybersecurity concepts packaged in the form of game elements. The digital assets, attack cards, and security cards contained in CyberMonopoly serve as visual media as well as a real simulation of the concepts learned. This supports the theory that contextual and



experiential learning will be easier for students to understand (Jayakrishnan et al., 2023). Thus, students not only understand concepts theoretically, but are also able to relate them to real-life situations they may encounter in everyday life. The N-Gain value of 0.78, which falls into the high category, indicates that CyberMonopoly was effective in supporting students' understanding of basic cybersecurity concepts. This finding implies that the use of a non-digital board game can provide an effective alternative for delivering cybersecurity learning in junior high school, particularly by presenting abstract concepts through concrete and interactive game elements.

Conclusion

Based on the findings of this study, CyberMonopoly was successfully implemented as a serious board game-based learning medium for cybersecurity education at the junior high school level. The results demonstrated a considerable improvement in students' learning outcomes, with the mean score increasing from 52.85 on the pretest to 89.31 on the posttest. The Wilcoxon Signed-Rank Test further confirmed that the difference between the pretest and posttest scores was statistically significant ($Z = -4.461$, $p < 0.001$), and all 26 students demonstrated an improvement in their scores. In addition, the N-Gain score of 0.78, which falls within the high category, indicates a substantial increase in students' understanding of fundamental cybersecurity concepts. These findings suggest that CyberMonopoly has the potential to serve as an effective non-digital learning medium that promotes interactive, collaborative, and experiential learning in cybersecurity education for junior high school students.

Recommendation

Based on the research findings, educators are encouraged to consider CyberMonopoly as an alternative learning medium for supporting cybersecurity education at the junior high school level. The findings also suggest that board game-based learning media can be further developed and adapted to different learning contexts and subjects that require conceptual understanding and active student engagement. Future development of other non-digital game-based learning media is also recommended to enrich collaborative and interactive learning strategies. Furthermore, game design should remain aligned with learning objectives and competency indicators to ensure that gameplay activities effectively support the intended learning outcomes.

References

- Affan, Y., Rubia, F., JiangBin, Z., Afzal, W., & Raza, S. (2024). Can serious gaming tactics bolster spear-phishing and phishing resilience?: Securing the human hacking in Information Security. *ScienceDirect*. <https://doi.org/10.1016/j.infsof.2024.107426>
- Ahamed, B., Rashed, M., Polas, H., Kabir, A. I., Soheli-uz-zaman, A. S., Fahad, A. Al, & Chowdhury, S. (2024). *Empowering Students for Cybersecurity Awareness Management in the Emerging Digital Era : The Role of Cybersecurity Attitude in the 4.0 Industrial Revolution Era*. March, 1–14. <https://doi.org/10.1177/21582440241228920>
- Alnajim, A. M., Habib, S., Islam, M., & Alrawashdeh, H. S. (2023). *SS symmetry Exploring Cybersecurity Education and Training Techniques: A Comprehensive Review of Traditional , Virtual Reality ,.*
- Blažič, A. J. B. B. J. (2024). Toward effective learning of cybersecurity: new curriculum agenda and learning methods. *CYBERSECURITY*. <https://doi.org/10.1093/cybsec/tyae018>



- Carvalho, C. V. De. (2024). *An Educational Escape Room Game to Develop Cybersecurity Skills*.
- Hart, S., Margheri, A., Paci, F., & Sassone, V. (2020). Riskio: A Serious Game for Cyber Security Awareness and Education. *ScienceDirect*. <https://doi.org/10.1016/j.cose.2020.101827>
- Hiranya, N., Rune, W., & Basel, H. (2026). A systematic scoping review on game-based cybersecurity awareness. *International Journal of Information Security*, 25(2), 1–75. <https://doi.org/10.1007/s10207-026-01239-9>
- Ibrahim, A., Mckee, M., Sikos, L. F., Member, S., & Johnson, N. F. (2024). *A Systematic Review of K-12 Cybersecurity Education Around the World*. 12(March).
- Jayakrishnan, G., Banahatti, V., & Lodha, S. (2023). *Design and Execution Challenges for Cybersecurity Serious Games : An Overview*.
- Liberty Jemadu, & Dicky Prastya. (2021). *Kominfo: Literasi Digital Indonesia Belum Mencapai Status Baik*. Suara.com. <https://www.suara.com/tekno/2021/11/10/160219/kominfo-literasi-digital-indonesia-belum-mencapai-status-baik>.
- Malik, S. I., Mostafa Al-Emran, Roy Mathew, Ragad M Tawafak, & Ghaliya Alfarsi. (2020). Comparison of E-Learning, M-Learning and Game-based Learning in Programming Education – A Gendered Analysis. *EMERGING TECHNOLOGIES IN LEARNING*.
- Paundu, A. W., Nurtanio, I., Ilham, A. A., Niswar, M., Bustamin, A., Alief, M., Imran, F., Aryandi, M., Husein, K., Simang, Y., Husein, A. A., Fahreza, R., Atda, A. T. N., Informatika, D. T., Teknik, F., & Hasanuddin, U. (2026). *Edukasi Keamanan Siber sebagai Upaya Peningkatan Literasi Digital Guru dan Siswa di SMAN 3 Polewali*. 9, 210–219.
- Prasetya, N. I., & Syidada, S. (2025). *Integrasi Serious Games dalam Pengembangan Platform Pembelajaran Pemrograman*. 5(1), 12–26.
- Qomariasih, F. A. R. H. S. H. K. N. (2024). Implementation of Game-Based Learning to Enhance Security Awareness Against Child Cyber Grooming Attacks. *IEEE XPLORE*. <https://doi.org/10.1109/ICITISEE63424.2024.10729941>
- radip. (2023). *BSSN Catat 361 Juta Serangan Siber Masuk ke Indonesia per Oktober 2023, Malware Jadi Ancaman Utama*. radip.id. <https://www.radip.id/2023/10/16/bssn-catat-361-juta-serangan-siber-masuk-ke-indonesia-per-oktober-2023-malware-jadi-ancaman-utama/>.
- Radović, S., Hummel, H. G. K., & Vermeulen, M. (2022). Design - based research with mARC ID model: designing experiential learning environments. *Learning Environments Research*, 25(3), 803–822. <https://doi.org/10.1007/s10984-021-09394-7>
- Raffaghelli, J. E., Rodríguez, M. E., & Ba, D. (2022). *Computers & Education Applying the UTAUT model to explain the students ' acceptance of an early warning system in Higher Education*. 182(February). <https://doi.org/10.1016/j.compedu.2022.104468>
- Rahmawati, V., & Ratnawati, E. (2024). *PENERAPAN MEDIA PEMBELAJARAN ULAR TANGGA UNTUK MENINGKATKAN PEMAHAMAN MAHASISWA SEMESTER 5 TADRIS IPS A UIN SIBER SYEKH NURJATI CIREBON DALAM PEMBELAJARAN IPS*. 1, 1–8.
- Rye, S., & Torres, P. J. (2023). *Playing at the school table : Systematic literature review of board , tabletop , and other analog game-based learning approaches*. June. <https://doi.org/10.3389/fpsyg.2023.1160591>
- Sailer, M., & Homner, L. (2020). *The Gamification of Learning : a Meta-analysis*. 77–112.
- Souvi, W., Ningtyas, R., El-yunusi, M. Y. M., Sunan, U., Surabaya, G., & Agama, P. (2024). *Keaktifan siswa melalui pembelajaran permainan edukatif di sd dumas surabaya*. 3(2), 89–100.