



CHYPER: A Low-Cost, Card-Based Solution for Building Cybercrime Resistance Among Middle School Students

Nurul Maulida, Rizki Hikmawan*

Department of Information Systems and Technology Education

Universitas Pendidikan Indonesia.

*Corresponding Author. Email: hikmariz@upi.edu

Abstract: This study aims to develop CHYPER, a low-tech educational card game, and examine changes in students' conceptual understanding of cybersecurity. The study employed a one-group pretest–posttest pre-experimental design involving 21 junior high school students in Purwakarta, Indonesia. CHYPER consists of 62 cards designed based on the CIA Triad and the NIST Cybersecurity Framework. Data were collected using a 20-item Likert-scale questionnaire and analyzed using descriptive statistics, the Shapiro–Wilk test, the Wilcoxon signed-rank test, and N-gain analysis. The mean score increased from 70.95 on the pretest to 77.62 on the posttest. The Wilcoxon signed-rank test revealed a statistically significant difference between the pretest and posttest scores ($Z = -3.164$, $p = .002$), whereas the mean N-gain score was 0.22 (22.16%), indicating a low level of improvement. These findings suggest that CHYPER has potential as a supplementary learning medium for introducing basic cybersecurity concepts to junior high school students, although the magnitude of improvement was limited.

Article History

Received: 18-06-2026

Revised: 10-08-2026

Accepted: 17-09-2026

Published: 20-10-2026

Key Words:

Educational Card Game;
Cybersecurity Literacy;
CHYPER; CIA Triad;
NIST Cybersecurity
Framework.

How to Cite: Maulida, N., & Hikmawan, R. (2026). CHYPER: A Low-Cost, Card-Based Solution for Building Cybercrime Resistance Among Middle School Students. *Jurnal Paedagogy*, 13(4), 1397-1409. <https://doi.org/10.33394/jp.v13i4.21330>



<https://doi.org/10.33394/jp.v13i4.21330>

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



Introduction

Advances in information and communication technology have integrated the digital space into students' learning activities and social interactions, while also introducing various cyber risks in the context of education (Whitelock et al., 2024). Amid the accelerating digital transformation in Indonesia, data from the Central Statistics Agency (BPS) show that the proportion of internet users among Generation Z stands at 34.49%, with users who have completed junior high school or its equivalent accounting for 22.36%, positioning junior high school students as an active group within the national digital ecosystem (Badan Pusat Statistik, 2024). Intense digital engagement among adolescents of junior high school age is associated with increased exposure to various online risks (Chen et al., 2025; Jeong, 2025; Zou et al., 2024). From a developmental perspective, junior high school students' capacity to independently recognize and manage digital risks remains limited, thus requiring the strengthening of preventive cybersecurity literacy through appropriate pedagogical approaches (Gómez et al., 2025). The disparity between the high intensity of students' digital activities and the limited reinforcement of cybersecurity literacy highlights an educational challenge relevant to the global agenda for quality and safe education in the digital age (Nations, 2015).

Students' vulnerability in the digital environment is becoming increasingly relevant when considered in relation to various forms of cyber threats that can impact the data and devices they use. National monitoring data published by the National Cyber and



Cryptography Agency shows that 514,508 instances of ransomware activity were detected in Indonesia's cyberspace throughout 2024 (Badan Siber dan Sandi Negara, 2024). Ransomware is a highly complex topic because it requires an understanding of attack mechanisms, the cybercrime ecosystem, and detection and mitigation strategies all of which are typically discussed in technical and professional contexts. (Cui et al., 2026; Kumar et al., 2025). This complexity poses a challenge when introducing ransomware to middle school students, especially if the material is presented in a technical manner or solely through lectures. Although middle school students are not expected to have an in-depth understanding of how ransomware works, they need a basic understanding of the risks to the data and devices they use in their daily digital activities. Therefore, introducing ransomware at the middle school level should focus on the ability to recognize risky situations, maintain data security, and understand basic preventive measures. This underscores the need for a cybersecurity education approach that emphasizes conceptual understanding and risk awareness through interactive learning media that do not rely on highly complex technology. (Ismail et al., 2024; Katsantonis et al., 2025; Yasin et al., 2024).

A low-tech approach to cybersecurity education should not be viewed as an inferior solution compared to digital approaches, because the effectiveness of learning is determined more by the appropriateness of the pedagogical design than by the complexity of the technology used (Qiao et al., 2022; Sousa et al., 2023). Sousa et al. (2023) demonstrate that serious games and non-digital learning media such as board games, tabletop games, and card games are effective in enhancing learner engagement, conceptual understanding, and experiential learning, particularly for abstract and complex subject matter. In the context of cybersecurity, tabletop serious games have proven capable of facilitating reflective discussions and a more meaningful understanding of attack scenarios and defense strategies compared to lecture-based approaches (Hart et al., 2020) including through role-based gamification approaches that model threat dynamics and mitigation systematically (Luh et al., 2021). Similar findings are demonstrated by the card game Crypto Go, which successfully simplifies complex cryptographic concepts into interactive and accessible physical activities (González-tablas et al., 2020). Furthermore, the development of adaptive serious games in cybersecurity education has shown a significant increase in learners' risk awareness and engagement compared to conventional training methods (Hodhod et al., 2023; Yasin et al., 2024). Consistent with these findings, a systematic review by Sodikin & Hikmawan (2023) literature also emphasizes that game elements such as challenges, roles, feedback, and competition contribute positively to intrinsic motivation and learning effectiveness (C. Chen, 2025; Katsantonis et al., 2025), making low-tech cyber pedagogy-based gamification a relevant approach to bridge the complexity of cybersecurity material with the learning characteristics of middle school students.

The game-based learning approach can be examined through Experiential Learning Theory. According to Kolb (1984, as cited in Rahmi, 2024), learning occurs through a process involving concrete experience, reflective observation, abstract conceptualization, and active experimentation. In the context of game-based learning, students have the opportunity to build knowledge through direct experience, interaction, practice, and reflection during the game (Singh et al., 2021). This approach is relevant to CHYPER because students are presented with attack and defense scenarios, then determine their actions based on the game conditions and observe the consequences of their decisions. This process enables students to connect their gaming experiences with a contextual understanding of cybersecurity concepts (Rahmi, 2024; Singh et al., 2021).



Although various studies have examined the use of serious games, gamification, and interactive learning media in the context of cybersecurity, most of these studies still focus on higher education or professional training and tend to address cyber threats in general terms. Research that specifically addresses ransomware as a preventive education topic for middle school students particularly through a low-tech approach aligned with students' learning characteristics remains relatively limited. This situation highlights the need for educational media that can simplify the complexity of ransomware material without compromising its educational substance, while also being tailored to the learning characteristics of middle school students.

Based on these needs, this study developed CHYPER, a low-tech educational card game designed as a cybersecurity learning medium for middle school students. CHYPER uses attack and defense mechanisms to introduce threat scenarios and protective measures in a contextual manner through hands-on activities without digital devices. This study aims to develop CHYPER as a cybersecurity educational tool and to analyze changes in students' conceptual understanding after participating in lessons using the game. This study contributes to the development of low-tech cybersecurity learning tools that support the contextual introduction of threat concepts and cybersecurity protection strategies to junior high school students.

Research Method

This study employs a quantitative approach with a one-group pretest-posttest pre-experimental design. A total of 21 students from Purwakarta Public Junior High School were selected as participants through purposive sampling, taking into account the diversity of digital skills among early adolescents as a representation of the target population. The intervention consisted of the CHYPER educational card game, a low-tech medium developed based on the CIA Triad (Confidentiality, Integrity, Availability) and the NIST Cybersecurity Framework (Casaril, 2025; Li & Liu, 2021). The cybersecurity competency indicators that served as the basis for developing the cards and evaluation instruments included: (1) the ability to recognize the types and characteristics of ransomware threats, (2) an understanding of the basic principles of data and system protection, (3) awareness of the processes for detecting and responding to cybersecurity incidents, (4) an understanding of data recovery and system continuity efforts, and (5) an understanding of the concepts of confidentiality, integrity, and availability of information (the CIA Triad). These indicators emphasize conceptual understanding and risk awareness rather than operational technical skills, making them appropriate for the goal of preventive education at the junior high school level.

The CHYPER game uses 62 cards consisting of 28 attack cards, 28 defense cards, and 6 special cards. A total of 21 students were divided into four groups, each consisting of 5 or 6 students. The game was conducted in two sessions: the first session was attended by groups 1 and 2, while the second session was attended by groups 3 and 4. This division was implemented so that the researcher could provide guidance and monitor the game more closely. Before the game began, all cards were shuffled into a single deck. Each player then received five cards as their starting hand, while the remaining cards were used as the Reserve Deck.

On each turn, a player could choose to attack an opponent using one Attack card or draw two cards from the Reserve Deck. If a player was targeted for an attack, they had to counter using a Defense card. If a player does not have a Defense card, they are allowed to draw two cards from the Reserve Deck as a defensive measure. If they still do not obtain a



Defense card, the attack is declared successful. Points are awarded based on the value of the cards played. If the value of the Defense card is equal to or greater than that of the Attack card, the defending player earns 2 points. Conversely, if the value of the Attack card is higher, the attacking player earns points equal to the difference between the two card values. In addition, there are Special cards that do not have a point value but provide specific functions: Cyber Insurance to cancel one attack, Incident Response to draw two cards from the Reserve Deck, and Data Recovery to take one Defense card from the opponent. The game ends when the Reserve Deck is depleted, and the player with the highest number of points is declared the winner.

Data collection was conducted using a questionnaire with a 1–5 Likert scale, administered as a pretest and posttest during a single learning session. The questionnaire consisted of 20 statements based on the cybersecurity competency indicators described earlier, with the same instrument used in both measurement phases to ensure consistency. The instrument was evaluated through empirical validity and internal consistency tests before being used in data analysis. Item validity testing was conducted using Pearson's product-moment correlation based on data from 20 respondents. At a 5% significance level, the table r value used was 0.444. The test results showed that all 20 items had correlation coefficients ranging from 0.452 to 0.874 with significance values less than 0.05; thus, all items met the criteria for empirical validity. The internal consistency of the instrument was tested using Cronbach's Alpha because the instrument employed a Likert scale with several response categories (Yusup, 2018). The reliability test yielded a Cronbach's Alpha value of 0.911, with Corrected Item-Total Correlation values ranging from 0.382 to 0.850.

Data analysis was conducted in four stages. Descriptive statistics were used to provide an overview of the data; the Shapiro-Wilk normality test was used as a prerequisite for selecting inferential tests; the Wilcoxon Signed-Rank Test was used to test the significance of the difference between pretest and posttest scores selected because the posttest data were not normally distributed ($p < 0.05$) and the N-Gain Score was used to measure the extent of the increase in students' conceptual understanding (Ahmad & Sari, 2025; Sullivan & Feinn, 2012).

Results and Discussion

Attack cards represent various forms of ransomware threats, while defense cards illustrate strategies for protection and mitigation against those threats. Special cards serve as supporting elements that add variety to game strategies while also representing incident management actions. Visual examples of each card type are shown in Figure 1, Figure 2, and Figure 3. The gameplay is illustrated in Figure 4.

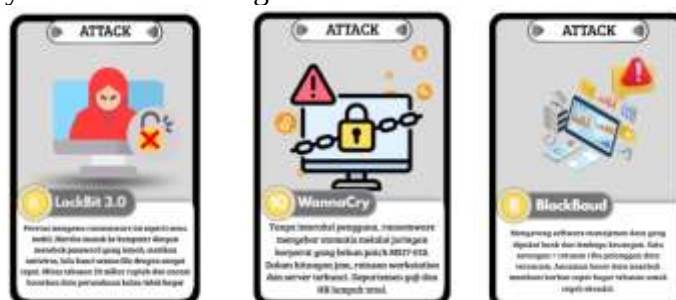


Figure 1. Examples of Attack Cards

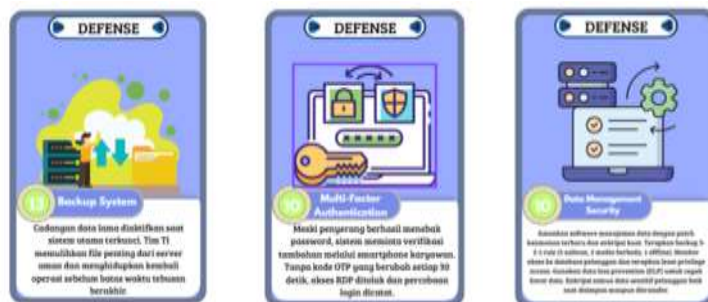


Figure 2. Examples of Defense Cards



Figure 3. Examples of Special Cards



Figure 4. Implementation of the CHYPER Card Game in the Classroom

The results of the CHYPER card game development show that there are 28 pairs of attack and defense cards organized based on the relationship between types of ransomware threats and relevant mitigation strategies. Each attack card is paired with one or more defense cards that represent efforts to protect against the impact of attacks on the confidentiality, integrity, and availability of systems.

Table 1. Representative Attack–Defense Card Mapping and CIA Triad Mechanisms

No.	Attack Card	Defense Card	CIA Triad Mechanism
1)	LockBit 3.0	Backup System, Multi-Factor Authentication	Availability, Confidentiality
2)	WannaCry	Patch Management, Network Segmentation, Endpoint Protection	Availability, Integrity



3)	Locky	Disable Macros, Email Security, Endpoint Protection	Confidentiality, Integrity
4)	Petya	Endpoint Protection, Backup System, Account Lockout Policy	Availability, Confidentiality
5)	DoppelPaymer	Network Segmentation, Zero Trust, Privileged Access Management	Confidentiality, Integrity

Table 1 presents representative examples of attack–defense card mappings in CHYPER. The selected pairs illustrate how different ransomware threats are associated with specific defense strategies and cybersecurity protection mechanisms. The mapping shows that the defense strategies in CHYPER address different dimensions of the CIA Triad according to the type of protection they provide. Backup systems primarily support Availability by enabling data recovery and system continuity after an attack, while Multi-Factor Authentication, Zero Trust, and Privileged Access Management mainly support Confidentiality by restricting unauthorized access. Preventive measures such as Patch Management, Disable Macros, and Endpoint Protection contribute to maintaining Integrity by reducing vulnerabilities and preventing malicious activities that may compromise systems. Network Segmentation and other access-control mechanisms may address more than one CIA dimension because cybersecurity risks are interconnected. Overall, the mapping connects ransomware attack scenarios with practical defense strategies and introduces students to the basic relationship between cyber threats and the principles of Confidentiality, Integrity, and Availability through gameplay.

Data analysis was conducted in stages, beginning with descriptive statistics, followed by normality tests, and concluding with comparative tests. Descriptive statistics were used to obtain an overview of the distribution of students' pretest and posttest scores. A summary of the descriptive statistics is presented in Table 2. Documentation of the pretest and posttest administration is shown in Figure 5.



Figure 5. Administration of Student Pretests and Posttests

Table 2. Descriptive Statistics for the Pretest and Posttest

Data	N	Mean	Std. Deviasi	Min-Max
Pretest	21	70,95	10,12	48 - 86
Posttest	21	77,62	11,33	48 -90



Based on Table 2, the average posttest score of 77.62 was higher than the pretest score of 70.95, with a difference of 6.67 points. This indicates a trend toward improved conceptual understanding among students after participating in instruction using the CHYPER card game.

Before conducting the comparative test, a normality test was first performed to determine the data distribution as a prerequisite for selecting an inferential test. The Shapiro-Wilk test was used because the sample size was relatively small, $n = 21 < 50$ (Sari et al., 2024). The null hypothesis for the normality test was formulated as H_0 , stating that the data are normally distributed, and H_1 , stating that the data are not normally distributed. The decision criterion used was that H_0 is accepted if $\text{Sig.} > 0.05$ (Sonjaya et al., 2025). The results of the normality test are presented in Table 3.

Table 3. Results of the Shapiro-Wilk Normality Test

Data	Statistics	df	Sig.
Pretest	0,954	21	0,408
Posttest	0,875	21	0,012

Based on Table 3, the pretest data were normally distributed ($\text{Sig.} = 0.408 > 0.05$), whereas the posttest data were not normally distributed ($\text{Sig.} = 0.012 < 0.05$). Since one of the data sets did not meet the assumption of normality, a comparative test was conducted using the nonparametric Wilcoxon Signed-Rank Test as an alternative to the Paired Sample T-Test (Ahmad & Sari, 2025). The formulated hypotheses are H_0 , which states that there is no significant difference between the pretest and posttest scores, and H_1 , which states that there is a significant difference between the two scores, with the criterion that H_0 is rejected if the Asymp. Sig. (2-tailed) value is < 0.05 . The results of the Wilcoxon test are presented in Table 4 and Table 5.

Table 4. Wilcoxon Signed-Rank Test Ranks

Ranks	N	Mean Rank	Sum of Ranks
Negative Ranks (Posttest < Pretest)	4	4.13	16.50
Positive Ranks (Posttest > Pretest)	15	11.57	173.50
Ties (Posttest = Pretest)	2	-	-

Table 5. Wilcoxon Signed-Rank Test Statistics

Test Statistics	Posttest-Pretest
Z	-3.164
Asymp. Sig. (2-tailed)	0.002

Based on Table 4, out of 21 students, 15 showed an increase in posttest scores, 4 showed a decrease, and 2 showed no change. The positive ranks had a mean rank of 11.57 and a sum of ranks of 173.50, while the negative ranks had a mean rank of 4.13 and a sum of ranks of 16.50. As shown in Table 5, the Wilcoxon Signed-Rank Test yielded a Z-value of -3.164 with an Asymp. Sig. (2-tailed) of 0.002. Since $p = 0.002 < 0.05$, H_0 is rejected, indicating a statistically significant difference between the pretest and posttest scores. However, this statistical significance does not necessarily indicate a substantial practical improvement, as the subsequent N-Gain analysis showed an average gain of 0.22, which falls into the low category.

The decline in scores among the four students may have been influenced by several contextual factors. First, the intervention was conducted during the month of Ramadan, specifically after the students had completed a short-term Islamic boarding school program,



so their physical condition and concentration may not have been optimal (Rahmansyah et al., 2025). Second, some students were unable to complete the posttest because they had to leave the activity early. Third, the intervention was conducted in only one learning session, so the understanding developed during the activity may not have been fully consolidated by the time the posttest was administered (Wang et al., 2022).

It is important to understand that the statistical significance yielded by the Wilcoxon test and the magnitude of the improvement measured by the N-Gain Score are two distinct concepts. The Wilcoxon test demonstrates that the difference between pretest and posttest scores is not due to chance, whereas the N-Gain Score measures the substantive magnitude of that improvement. Thus, a statistically significant result does not always imply a substantial practical improvement (Sullivan & Feinn, 2012). Although the Wilcoxon test has demonstrated a significant difference between pretest and posttest scores, the magnitude of the improvement in students' conceptual understanding needs to be further measured quantitatively. To that end, the N-Gain Score was used as an index that illustrates the comparison between the actual gain achieved by students and the maximum possible gain (Hake, 1999 in Harianja et al., 2024). The calculation results are presented in Table 6.

Table 6. Results of the N-Gain Score Calculation Test

Data	Mean Pretest	Mean Posttest	N-Gain	Category
Understanding Cybersecurity	70,95	77,62	0,22	Low

Based on Table 5, the average N-Gain Score of 0.22, or 22.16%, falls into the low category ($g < 0.3$) (Harianja et al., 2024). This result must be interpreted contextually, given that the students' average pretest score was already relatively high at 70.95, meaning that the potential for improvement was mathematically limited (Staus et al., 2021). Furthermore, the intervention was conducted in only one learning session, which also affected the magnitude of the gain that could be achieved (Wang et al., 2022). There were also 4 students who experienced a decrease in their posttest scores, which can be explained by individual variations in engagement during gameplay as well as the students' conditions while taking the posttest (Staus et al., 2021).

Overall, the analysis results indicate that the CHYPER card game is statistically effective in improving junior high school students' conceptual understanding of cybersecurity, although the magnitude of the improvement remains in the low category. These findings indicate that a single-session intervention provides a measurable and meaningful initial impact, but further reinforcement is still needed to achieve improvements in the moderate-to-high range.

Discussion

The CHYPER card game was designed based on two internationally standardized conceptual frameworks the CIA Triad and the NIST Cybersecurity Framework to ensure the content's relevance to current cybersecurity practices (Casaril, 2025; Li & Liu, 2021). The choice of a low-tech approach in this study was a pedagogical decision based on considerations of inclusivity and learning effectiveness. Chen (2025) demonstrated that low-tech learning media can bridge the digital divide while fostering deeper cognitive engagement, given that digital media often divert students' attention toward the technological interface rather than the substance of the material. This argument is reinforced by Sousa et al. (2023), who concluded that tabletop analog games consistently produce meaningful collaborative learning experiences, particularly in concretizing abstract concepts into representations that are easily understood by students. The three-component card structure comprising attack cards, defense cards, and special cards directly represents the dynamics of



threats and responses in a real-world cybersecurity context. This structural approach aligns with the design of the card games Riskio (Hart et al., 2020) and Crypto Go (González-tablas et al., 2020), which have been used to represent the relationship between cyber threats and mitigation strategies in a format that is understandable to students without a technical background. The resulting mapping of 28 pairs of attack and defense cards demonstrates that CHYPER functions not merely as an educational entertainment medium, but as a structured learning system that requires students to think critically about the consequences of threats and defense strategies simultaneously.

A Wilcoxon Signed-Rank Test yielded a Z-value of -3.164 with a p-value of 0.002 ($p < 0.05$), indicating a statistically significant difference between students' pretest and posttest scores. Of the total 21 students, 15 students, or 71.4%, showed an increase in their scores, indicating that the majority of students demonstrated higher scores after the learning intervention. This finding aligns with the conclusions of Sodikin & Hikmawan (2023) in their systematic review, which states that gamification approaches in cybersecurity education consistently yield more significant improvements in understanding compared to conventional learning methods. Furthermore, Katsantonis et al. (2025) demonstrated that even collaborative tabletop games without digital components can meaningfully enhance cybersecurity awareness, provided that the game mechanics are designed to encourage active decision-making a characteristic explicitly embedded in the card-interaction mechanics of CHYPER. It is worth noting that this effectiveness was achieved under less-than-optimal conditions specifically, during the month of Ramadan following a short-term Islamic boarding school program, with some students leaving the session before it ended. The fact that the difference in scores remained statistically significant under such conditions actually strengthens the argument that the CHYPER card game possesses an intrinsic appeal capable of sustaining student engagement even under limited conditions (Qiao et al., 2022).

The extent of the improvement in conceptual understanding, as measured by the N-Gain Score, yielded an average value of 0.22, which falls into the low category ($g < 0.3$). Interpreting this result requires consideration of the students' initial level of understanding and the characteristics of the measurement instrument. The relatively high pretest mean score of 70.95 out of a maximum of 100 indicates that students already possessed a considerable level of conceptual understanding before participating in the CHYPER intervention. This condition may be related to students' prior learning experiences, particularly through Informatics lessons that introduce concepts related to digital safety, data protection, responsible technology use, and information security. Therefore, students did not begin the intervention from a condition of minimal knowledge, which may have limited the magnitude of improvement that could be observed after the intervention.

The relatively high pretest score also needs to be considered from the perspective of the measurement instrument. The questionnaire consisted of 20 Likert-scale items designed to assess students' conceptual understanding of ransomware threats, data and system protection, incident response, data recovery, and the CIA Triad. Empirical validity testing showed that all 20 items met the validity criteria, with item correlation coefficients ranging from 0.452 to 0.874. The instrument also demonstrated good internal consistency, with a Cronbach's Alpha coefficient of 0.911. These findings provide empirical support for the validity and consistency of the instrument; however, validity and reliability results do not necessarily guarantee that all items are equally sensitive to changes in students' conceptual understanding. Some items may have been relatively familiar or easy for students because they were related to concepts previously encountered in Informatics learning or everyday



digital experiences. Thus, the relatively high pretest score may indicate a restricted range for improvement rather than a complete ceiling effect. This condition is consistent with the argument that relatively high baseline scores can mathematically limit the potential magnitude of learning gains (Staus et al., 2021). The relatively modest increase in the mean score, from 70.95 to 77.62, should therefore be interpreted in light of the students initial level of understanding.

In addition, the single-session intervention inherently limited the opportunity for students to consolidate their understanding over a longer period, as demonstrated by Wang et al. (2022), who found that intervention duration is a significant predictor of the magnitude of learning gains in game-based learning. The implementation conditions, which took place during Ramadan following a short-term Islamic boarding school program, may also have affected students' cognitive state and concentration (Rahmansyah et al., 2025). These factors may have contributed to individual variations in posttest scores, including the four students who experienced a decline in scores. Nevertheless, the statistically significant difference indicated by the Wilcoxon test suggests that a measurable change occurred after the intervention. However, given the low N-Gain value, CHYPER should be interpreted as providing an initial contribution to cybersecurity conceptual understanding, rather than as a comprehensive or standalone solution. This finding remains consistent with literature indicating that single-session serious game-based interventions can produce measurable initial effects as a foundation for cybersecurity literacy (Ismail et al., 2024; Yasin et al., 2024).

Conclusion

This study developed the CHYPER educational card game as a low-tech cybersecurity learning medium for junior high school students, using the CIA Triad and the NIST Cybersecurity Framework as conceptual foundations. The game provides a structured way to introduce ransomware threats and corresponding defense strategies through attack, defense, and special cards. The results showed a statistically significant difference between students' pretest and posttest scores based on the Wilcoxon Signed-Rank Test ($Z = -3.164$, $p = 0.002$). However, the average N-Gain score was 0.22 (22.16%), which falls into the low category. This finding indicates that although a measurable change in students' conceptual understanding occurred after the intervention, the magnitude of improvement was limited. The result should be interpreted in relation to the relatively high pretest score (70.95), the single-session intervention, and the implementation context. Therefore, CHYPER can be considered a supplementary and initial learning medium for introducing basic cybersecurity concepts, rather than a comprehensive standalone solution.

Recommendation

- 1) For Game Designers and Educational Developers:
CHYPER can be further improved by refining its visual design, game instructions, and attack-defense mechanics, while strengthening the connection between cybersecurity threats, defense strategies, and the CIA Triad
- 2) For Educators and School Policy Makers:
Future research should use longer intervention periods, larger samples, and control or comparison groups to provide stronger evidence of CHYPER's contribution to cybersecurity learning. Further validation of the assessment instrument is also



recommended to improve its sensitivity in measuring changes in students' understanding.

3) For Future Researchers:

Future research should use longer intervention periods, larger samples, and control or comparison groups to provide stronger evidence of CHYPER's contribution to cybersecurity learning. Further validation of the assessment instrument is also recommended to improve its sensitivity in measuring changes in students' understanding.

References

- Ahmad, F., & Sari, N. I. (2025). *Exploring the Wilcoxon Test in Science Education : A Literature Review of Empirical Research*. 7(2).
- Casari, F. (2025). International Journal of Critical Infrastructure Protection Developing security metrics for space systems : A study considering the NIST Cybersecurity Framework 2 . 0 and the NIS2. *International Journal of Critical Infrastructure Protection*, 51(August), 100805. <https://doi.org/10.1016/j.ijcip.2025.100805>
- Chen, C. (2025). Low-tech serious games in higher education: bridging the digital divide and enhancing student thinking and performance. *Humanities and Social Sciences Communications*, 4, 1–10. <https://doi.org/10.1057/s41599-024-04341-2>
- Chen, S., Huang, T., Chang, K., Chang, F., Chiang, S. C., Chiu, C., Chen, P., Miao, N., & Chuang, H. (2026). Computers in Human Behavior Association between school phone restriction policies and adolescents ' cyberbullying , gambling , and substance use behaviors. *Computers in Human Behavior*, 177(October 2025), 108898. <https://doi.org/10.1016/j.chb.2025.108898>
- Cui, B., Hu, Y., Qu, T., He, Y., & Sun, L. (2026). High-Confidence Computing A novel zero-day ransomware detection approach based on CVAE and. *High-Confidence Computing*, 6(1), 100338. <https://doi.org/10.1016/j.hcc.2025.100338>
- Gómez, P., Nogueira-lópez, A., Li, D., Salmerón-ruiz, M. A., & Rial-boubeta, A. (2025). *Age of smartphone access : implications for problematic internet use and online risk behaviors*. 103. <https://doi.org/10.1016/j.anpede.2025.503937>
- González-tablas, A. I., Vasco, M. I. G., & Cascos, I. (2020). *Shuffle , Cut , and Learn : Crypto Go , a Card Game for Teaching Cryptography*. 1–13. <https://doi.org/10.3390/math8111993>
- Harianja, M. R., Yusup, M., Siahaan, S. M., Sriwijaya, U., & Kunci, K. (2024). *Uji N-Gain pada Efektivitas Penggunaan Game dengan Strategi SGQ untuk Meningkatkan Berpikir Komputasi dalam Literasi Energi*. 13. <https://doi.org/10.19109/intelektualita.v13i2.25168>
- Hart, S., Margheri, A., Paci, F., & Sassone, V. (2020). *Computers & Security Riskio : A Serious Game for Cyber Security Awareness and Education*. 95. <https://doi.org/10.1016/j.cose.2020.101827>
- Hodhod, R., Hardage, H., & Abbas, S. (2023). *CyberHero : An Adaptive Serious Game to Promote Cybersecurity Awareness*.
- Ismail, M., Thorakkattu, N., Alalawi, M., & Alrabaee, S. (2024). Computers in Human Behavior Reports Cybersecurity activities for education and curriculum design : A survey. *Computers in Human Behavior Reports*, 16(June), 100501. <https://doi.org/10.1016/j.chbr.2024.100501>
- Jeong, E. (2025). Computers in Human Behavior Reports Sex differences in smartphone use



- profiles and the association with life satisfaction among South Korean second-year middle-school students : A latent profile analysis. *Computers in Human Behavior Reports*, 17(December 2024), 100575. <https://doi.org/10.1016/j.chbr.2024.100575>
- Katsantonis, M. N., Manikas, A., Partarakis, N., & Mavridis, I. (2025). Yellow training : a collaborative tCOFELET tabletop serious game for cybersecurity awareness and training. *International Journal of Information Security*, 24(4), 1–25. <https://doi.org/10.1007/s10207-025-01086-0>
- Kumar, S., Singh, S. K., Sarin, S., Kumari, C., Arya, V., Nandhini, N., Gupta, B. B., & Tai, K. (2025). Cyber Security and Applications Leveraging dynamic embeddings and reinforcement learning with bayesian networks for ransomware resiliences. *Cyber Security and Applications*, 3(November 2024), 100095. <https://doi.org/10.1016/j.csa.2025.100095>
- Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security ; Emerging trends and recent developments. *Energy Reports*, 7, 8176–8186. <https://doi.org/10.1016/j.egyr.2021.08.126>
- Luh, R., Temper, M., Tjoa, S., Schrittwieser, S., & Janicke, H. (2021). PenQuest : a gamified attacker / defender meta model for cyber security assessment and education. *Journal of Computer Virology and Hacking Techniques*, 16(1), 19–61. <https://doi.org/10.1007/s11416-019-00342-x>
- Nations, U. (2015). *Transforming our world: the 2030 Agenda for Sustainable Development*. United Nations. <https://sdgs.un.org/2030agenda>
- Qiao, S., Zainuddin, S. S. Y. Z., Ng, D. T. K., & Chu, S. K. W. (2022). *Examining the effects of mixed and digital gamification on students ' learning performance , cognitive engagement and course satisfaction*. (February), 1–20. <https://doi.org/10.1111/bjet.13249>
- Rahmansyah, N., Kurniati, I., Aisha, A. A. N., Mardiani, E., Putri, F. E., & Sugiyono. (2025). Analisa pengaruh puasa terhadap performa dan minat belajar siswa sdn gandaria utara 03 selama bulan ramadhan. *Jurnal Ilmiah Manajemen, Organisasi Dan Bisnis*, 14, 1–6.
- Rahmi, W. (2024). *Analytical Study of Experiential Learning : Experiential Learning Theory in Learning Activities*. 5, 115–126. <https://doi.org/10.62775/edukasia.v5i2.1113>
- Siber, D. O. K. (2024). *Lanskap keamanan siber indonesia 2024* (Number 70).
- Singh, P., Hoon, T. S., Nasir, A. M., Ramly, A. M., Rasid, S. M., & Meng, C. C. (2021). *Card game as a pedagogical tool for numeracy skills development*. 10(2), 693–705. <https://doi.org/10.11591/ijere.v10i2.20722>
- Sodikin, R. A., & Hikmawan, R. (2023). *Analysis of Gamification in Cybersecurity Education for Students: A Systematic Literature Review*. 8(2).
- Sonjaya, R. P., Aliyya, F. R., & Naufal, S. (2025). *Pengujian Prasyarat Analisis Data Nilai Kelas : Uji Normalitas dan Uji Homogenitas*. 9, 1627–1639.
- Sousa, C., Rye, S., Sousa, M., Torres, P. J., Perim, C., & Ennami, S. A. M. F. (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>
- Statistik, B. P. (2024). *Statistik Telekomunikasi Indonesia 2024*. <https://www.bps.go.id/id/publication/2025/08/29/beaa2be400eda6ce6c636ef8/statistik-telekomunikasi-indonesia-2024.html>
- Staus, N. L., Connell, K. O., & Storksdieck, M. (2021). *Addressing the Ceiling Effect when*



- Assessing STEM Out-Of-School Time Experiences.* 6(July), 1–9.
<https://doi.org/10.3389/feduc.2021.690431>
- Sullivan, G. M., & Feinn, R. (2012). *Using Effect Size—or Why the P Value Is Not Enough.* (September), 279–282.
- Wang, L. H., Chen, B., Hwang, G. J., Guan, J. Q., & Wang, Y. Q. (2022). Effects of digital game - based STEM education on students ' learning achievement : a meta - analysis. *International Journal of STEM Education.* <https://doi.org/10.1186/s40594-022-00344-0>
- Whitelock, D., Goshtasbpour, F., Pitt, B., Ferguson, R., Whitelock, D., Goshtasbpour, F., Pitt, B., & Ferguson, R. (2024). Capacity building for digital education. *Open Learning: The Journal of Open, Distance and e-Learning*, 39(2), 105–111.
<https://doi.org/10.1080/02680513.2024.2317894>
- Yasin, A., Fatima, R., Jiangbin, Z., Afzal, W., & Raza, S. (2024). Can serious gaming tactics bolster spear-phishing and phishing resilience? : Securing the human hacking in Information Security. *Information and Software Technology*, 170(February), 107426. <https://doi.org/10.1016/j.infsof.2024.107426>
- Yusup, F. (2018). *UJI VALIDITAS DAN RELIABILITAS INSTRUMEN PENELITIAN KUANTITATIF.* 7(1), 17–23.
- Zou, W., Purington, A., Masur, P. K., Whitlock, J., & Bazarova, N. N. (2024). Computers & Education Examining learners ' engagement patterns and knowledge outcome in an experiential learning intervention for youth ' s social media literacy. *Computers & Education*, 216(May 2023), 105046.
<https://doi.org/10.1016/j.compedu.2024.105046>