KARYA ILHAM PUBLISHING
CONNECTING MINDS, BRIDGING IDEAS, INSPIRING READERS

Journal of Advanced Research in Computing and Applications

Journal homepage:
https://karyailham.com.my/index.php/arca/index
ISSN: 2462-1927

Beyond the Board: CYBERPOLY as a Multidimensional Gamified Learning Tool for Cybersecurity Awareness

Sakinah Ali Pitchay[1,2,*], Anis Syahira Suhaimi[3], Farida Ridzuan[1,2], Azni Haslizan Ab Halim[1,2], Najwa Hayaati Mohd Alwi[1,2]

[1] Cybersecurity & Systems Research Unit, Universiti Sains Islam Malaysia, 71800, Negeri Sembilan, Malaysia
[2] Faculty of Science and Technology, Universiti Sains Islam Malaysia, 71800 Negeri Sembilan, Malaysia
[3] Universiti Malaya,50603 Kuala Lumpur, Malaysia

ARTICLE INFO

Article history:
Received 30 June 2025
Received in revised form 8 August 2025
Accepted 20 September 2025
Available online 6 October 2025

Keywords:
cybersecurity awareness; gamification; mobile learning; digital literacy; serious games

ABSTRACT

Cyberpoly is a mobile gamification platform designed to enhance cybersecurity awareness through an interactive board game format. Motivated by a survey of 210 secondary and university students revealing significant gaps in cyber literacy, Cyberpoly addresses three core challenges: evolving online behaviors, limited knowledge of cyber-attack prevention, and the need for sustained, engaging learning. This initiative aligns with Cybersecurity Malaysia's report, which indicates a 21.22% increase in cybercrime over the past five years. Cyberpoly integrates Naqli and Aqli knowledge, introducing Arabic concepts such as Tawakkal, Ta'alim, Iktikaf, and Muhasabah to promote culturally relevant cyber hygiene education. Key features include a password complexity indicator, offline access, portability, and a lifelong learning orientation. Gameplay spans four quiz levels—beginner to professional—mapped to Bloom's Taxonomy to support cognitive development. Correct answers yield in-game currency, which serves as a player's salary; the game concludes when the balance reaches zero. Developed using the DevSecOps methodology in Android Studio, Cyberpoly underwent functional and security testing, followed by user acceptance evaluation. Results show that 98.4% of participants found the app practical and user-friendly, with strong agreement on its effectiveness in raising awareness of cyberattacks. By combining gamification elements with culturally grounded content, Cyberpoly offers a scalable, industry-relevant solution to foster cyber literacy and digital resilience.

1. Introduction

Nowadays, the use of Internet in our daily life has become unavoidable. According to the Malaysian Communications and Multimedia Commission's (MCMC) Internet Users Survey (IUS), the percentage of Internet users in 2020 grew by 1.3% from 87.4% in 2018 to 88.7%. The survey also aims to understand the trends in Internet activity among users. Most people use the Internet to communicate with one another, visit social networking sites, search for information, and engage in

* *Corresponding author.*
E-mail address: sakinah.ali@usim.edu.my (Sakinah Ali Pitchay)

https://doi.org/10.37934/arca.40.1.106116

entertainment [1]. In 2023, 68.4% of business executives noted increased concerns about cyber threats, with financially motivated attacks accounting for 72% of breaches [9]. MyCERT's reports for 2023 and 2024 found that fraud was the leading type of reported cybersecurity incident, emphasizing the financial drivers behind cybercrime [9][10]. New behaviour during the COVID-19 pandemic affects every aspect of our lives. An employee who works from home, as well as students with online distance learning, increases the network usage rate, making data privacy extremely relevant. The lockdown period has had a profound impact on people's lives as the world progressively adapts to dealing with the COVID-19 issue. The new behaviour affects every aspect of our lives, from how we work to how we shop to how we relax [2]. Threats have increased in response to the growing need for information technology management, resulting in a lack of control over confidential data [3]. It was stated that malicious systems have spread across various mechanisms and are constantly increasing in complexity, making it more difficult to avoid their harmful and devastating effects. It was also reported that the usage rate of social networks has increased significantly worldwide in recent years. For instance, according to the Digital 2020 Global Overview Report, there were 3.8 billion social media users worldwide, making data piracy and privacy extremely relevant.

The second issue is the lack of knowledge on how to prevent cyber-attacks. Although people go online every day, many of them still lack knowledge on how to protect their data and network from cyberattacks. According to cybersecurity incident statistics prepared by Cybersecurity Malaysia's (CSM) Cyber999 Assistance Centre, as of October 2020, there have been 9,042 cases of fraud, crimes, and malicious codes**.** A 21.22% increase in cybercrime cases over the past five years is alarming. The Chief Executive Officer of CSM said there were 8,770 cases in the same timeframe in 2019, representing a 3.1% increase. Incident statistics indicate that users are often unaware of credential information protection, leaving them vulnerable when online. Reported incidents in 2021 show a decline in the number of fraud cases, which totalled 7,098. However, it remained the highest reported incident and was followed by the intrusion, as per the Malaysia Computer Emergency Response Team (MyCERT) 's general incident classification statistics in 2021 [4]. Additionally, 319 identity theft cases were reported in Malaysia in 2021.

The third issue is that there is a need to adopt the most effective approach to increase awareness of cyberattacks. A recent study by Masakazu and Megumi [5] demonstrates that the mobile gamification approach is suitable for various age groups. This is important because it will help increase and sustain the motivation to learn. Mobile gamification is appealing to people of all generations, making it an effective way to increase and maintain their motivation to learn [5]. Recent studies have emphasized the growing role of gamification in strengthening cybersecurity awareness and behavior. Mason *et al.,* [11] evaluated the GICAST training program, which employs game-based learning to teach cybersecurity to non-IT students, finding that emotional factors such as Fear of Missing Out (FoMO) can predict risky online behavior while fostering improved security attitudes and actions. Similarly, Matovu *et al.,* [13] examined non-digital serious games in smaller institutions and demonstrated that tailored gameplay significantly enhanced students' understanding of common cyberattacks, particularly phishing and malware. Extending this approach, Urhuogo and Addo [12] proposed a comprehensive gamification model that integrates engagement, simulation, continuous learning, and analytics to embed cybersecurity best practices within organizational culture and strengthen awareness initiatives. While Yigit *et al,.* [14] demonstrated that integrating gamified learning, behavioral reinforcement, and digital twin simulations significantly enhances cybersecurity training effectiveness by improving engagement, situational awareness, and real-world threat response.

Recent innovations, such as SWINDLERT, have demonstrated the pedagogical impact of game-based interactivity in promoting cybercrime awareness by Pitchay *et al*., [15]. Therefore, Cyberpoly

is proposed as a suitable approach for enhancing the learning experience through cybersecurity edugames. According to Grabosky [6], one of the most effective techniques for preventing and controlling cybercrime is raising public awareness of threats. Hence, by considering current user behaviour, mobile gamification as an edugame will bring users' excitement while playing the game and educating society at the same time, which will assist netizens in better understanding cyberattacks in a fun way. The following section will describe the methodology, results and conclude the contribution of this study.

2. Methodology

This study adopted a DevSecOps methodology to develop Cyberpoly, a gamified mobile application designed to enhance cybersecurity awareness and promote a culture of security. Unlike traditional Agile, DevSecOps embeds security at every stage of the development pipeline, ensuring both cultural and pedagogical integration as well as secure mobile application design and deployment (Prates and Pereira [16]; Feio *et al.,* [17]).

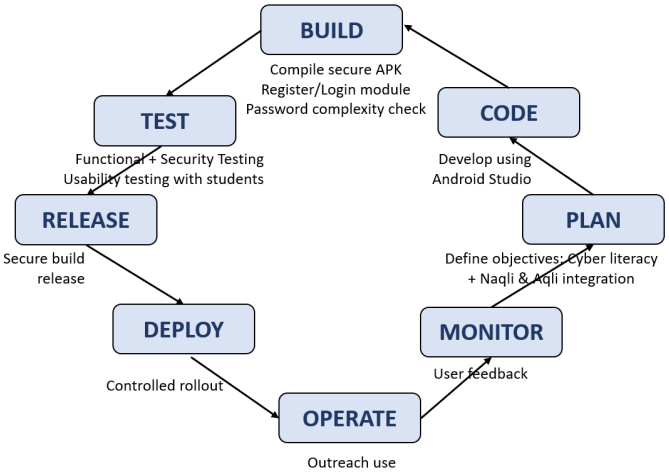

Fig. 1. DevSecOps phases for Cyberpoly development.

The eight phases as shown in Figure 1, which are plan, code, build, test, release, deploy, operate, and monitor, illustrate how cultural values (Figures 2 and 3), security features (register/login with password complexity), and technical tools (Android Studio, SQLite) were integrated to ensure a secure and pedagogically effective gamified platform.

2.1 Planning Phase

The planning phase focused on defining the project's objectives and scope. The primary aim was to reduce the number of cybercrime victims by enhancing cyber literacy among digital citizens. A secondary, yet equally significant, goal was to integrate Naqli (revealed knowledge) and Aqli (rational knowledge), thereby embedding Islamic ethical values into cybersecurity education. This included Arabic terms such as *Tawakkal* (trust in God), *Ta'alim* (obligation to learn), *Iktikaf* (self-reflection), and *Muhasabah* (self-accountability). Figure 2 illustrates the board game concept of the early vision, where players earn virtual money through quizzes and expend or gain resources based on their decision-making. This served as the conceptual foundation for linking cybersecurity knowledge to everyday digital risks, framed within an ethical context. These elements were identified through

preliminary needs analysis, which confirmed a gap in culturally contextualised cybersecurity awareness tools.

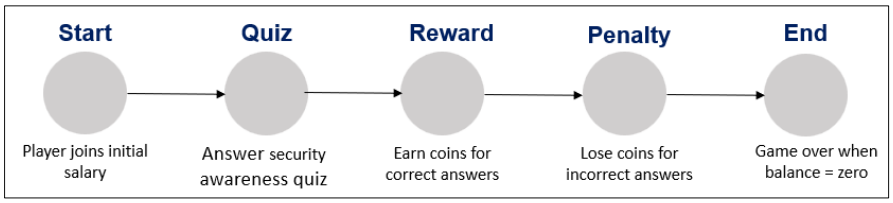

Fig. 2. Board game concept (Planning phase - Linear)

Figure 2 illustrates a schematic linear flow of Cyberpoly's gameplay, where players answer quizzes to earn coins (cyber resilience), risk losing coins (penalties), and end the game when their balance reaches zero.

2.2 Code Phase

In this phase, conceptual designs were translated into executable logic. Ethical triggers, such as Ta'lim (the obligation of continuous learning) and Tawakkal (trust in God's plan), were incorporated into the gameboard mechanics. In this phase, the Cyberpoly use case focuses on iterative feature integration and enhancement of functionality as shown in Figure 3. Core modules, including user registration, login authentication, tutorial access, and dual gameplay modes (Quiz-Based Game and INAQ Board Game), were continuously refined through version-controlled updates to ensure stable, secure, and user-centred application performance.

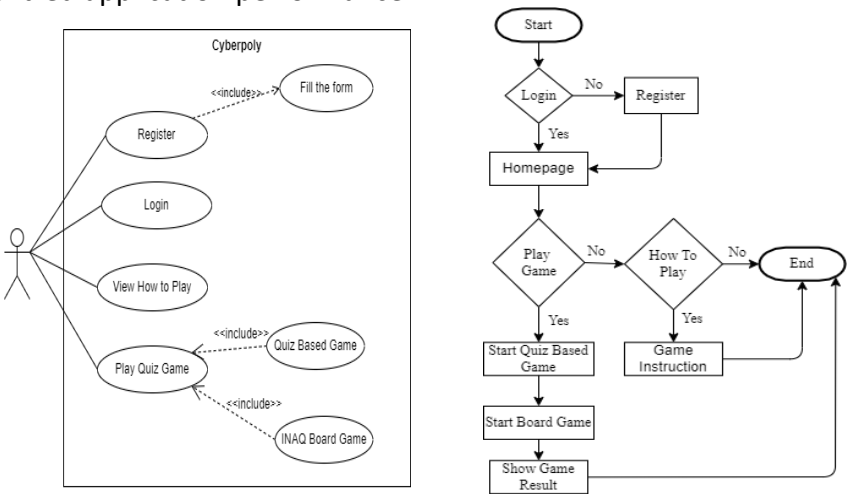

Fig. 3. Use case and flowchart of the Cyberpoly application

The flowchart in Figure 3 illustrates Cyberpoly's sequential logic, beginning with user registration or login and progressing through the homepage to either viewing instructions or initiating gameplay. Users can engage in two modes—Quiz-Based Game or INAQ Board Game—before viewing results. This flow aligns with the prior use case, confirming coherent functional integration and seamless user interaction throughout the development cycle. Coding development was employed in Android Studio, while SQLite served as the lightweight database to manage user progress, in-game currency, and quiz data.

2.3 Build Phase

In this phase, the conceptual framework of Cyberpoly was developed as a digital board game that rewards players with virtual currency earned from security awareness quizzes. This game mechanic simulates real-world decision-making: correct responses build cyber resilience, while poor choices result in financial penalties, leading to the depletion of a player's balance. The game design also embedded *iNaq* elements as ethical reminders; for instance, landing on a *Ta'alim* square reinforces the responsibility of learning, while *Tawakkal* squares reflect the balance between faith and rational actions. Storyboards and mock-ups were created to visualise the user journey, ensuring seamless integration of pedagogical and ethical components.

Application builds were automated to compile secure Android packages (.apk). This phase ensured dependencies and libraries were integrated without vulnerabilities. Security elements were emphasized from the start, including a register/login module with a password complexity checker, ensuring stronger protection against weak credential attacks before deployment.

The design phase translated conceptual objectives into interactive learning mechanics. In this stage, illustrated in Figure 4 (Ta'alim and Tawakkal Concept), specific elements of the board were incorporated as educational triggers. For instance, Ta'alim squares emphasize the importance of continuous learning obligations, while Tawakkal squares underscore the significance of relying on God's plan, along with the inherent unpredictability of gains or losses in cyber decision-making. These features were thoughtfully storyboarded and integrated to sustain engagement, align with Bloom's Taxonomy, and provide culturally relevant reinforcement.

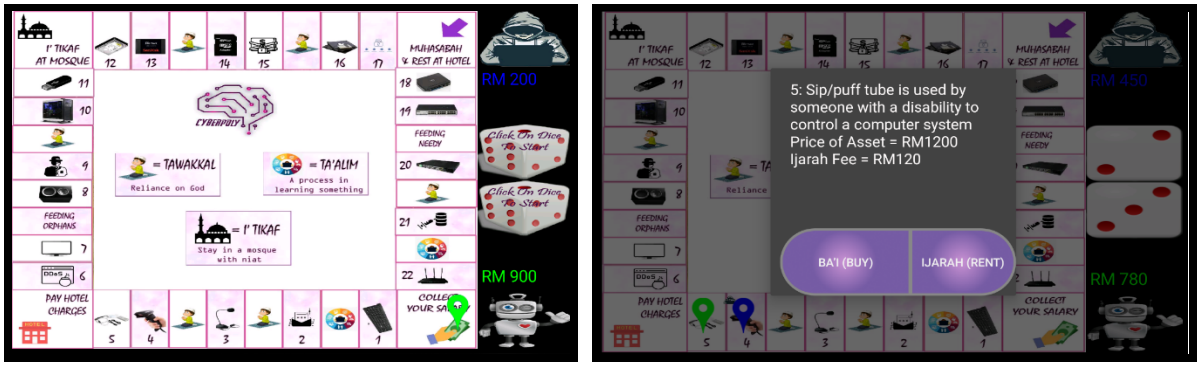

Fig. 4. Ta'alim and Tawakkal Concept in user interface layout

2.4 Test Phase

During the testing phase, functional verification ensured that Cyberpoly operated according to predefined specifications. Functional testing ensured smooth navigation, reward mechanics, and ethical triggers operated as designed. Security authentication testing validated the password complexity indicator, secure data handling in SQLite, and resilience against input-based threats. A total of 20 functional and 4 security authentication test cases were executed to assess performance, usability, and data protection. Complementing the structured testing, an online survey comprising 16 functionality-based questions was administered to student participants from the Universiti Sains Islam Malaysia (USIM), representing diverse academic backgrounds. The results confirmed that the application met its functional objectives, demonstrating reliability, security compliance, and a positive user experience.

Usability testing with secondary and university students confirmed motivational appeal and cultural authenticity. Feedback at this stage led to refinements in interface design and adjustment of in-game financial penalties, ensuring fairness and sustained engagement.

2.5 Release Phase

Once validated, stable builds were packaged for release. Security scans were performed prior to release to identify vulnerabilities, ensuring that no insecure APIs or misconfigurations were present. This phase reflects security by design, ensuring safe delivery of mobile builds. The deployment strategy emphasised accessibility, including offline usability for rural or bandwidth-limited contexts. Integration workshops introduced players to the game while highlighting its educational intent. The culturally embedded components (e.g., Muhasabah moments) were explained as reflective practices to connect digital choices with ethical living.

2.6 Deploy Phase

The application was deployed in controlled environments (universities and secondary schools). Offline accessibility features were prioritized to reach rural contexts. Deployment workshops highlighted not only the educational mechanics but also reflective practices such as Muhasabah, encouraging ethical digital citizenship. The iterative nature of DevSecOps was exemplified through user acceptance testing and structured user feedback, ensuring continuous refinement, enhanced security, and sustained alignment with stakeholder requirements.

2.7 Operate Phase

During operation, Cyberpoly was used as a teaching and awareness tool in the outreach programs. The integration of Naqli and Aqli values promoted lifelong learning and sustained engagement beyond initial deployment. Instructors and facilitators ensured continued alignment of gameplay with learning objectives.

2.8 Monitor Phase

Continuous monitoring involved user acceptance evaluations and the collection of iterative feedback. Surveys showed that 96.8% of users found Cyberpoly practical and easy to use, while most strongly agreed it improved awareness of cyber threats. Monitoring also included tracking quiz performance data from SQLite, allowing for the refinement of question difficulty and player progression.

The adoption of DevSecOps ensured Cyberpoly was not only pedagogically effective but also technically secure. Figure 1 employs DevSecOps as the methodology development for Cyberpoly application depicts the eight phases which are plan, code, build, test, release, deploy, operate, and monitor with cultural-pedagogical integration (Figures 2 and 3) embedded into Plan and Code phases, while security elements (register/login, password complexity, SQLite validation) are highlighted in build and test phases. This comprehensive approach demonstrates how security, ethics, and gamification can be tightly interwoven, resulting in a scalable and culturally contextualized cybersecurity awareness platform.

3. Results

A total of 210 respondents participated in the preliminary survey. Table 1 summarizes the demographic and digital behavior of respondents. Gender distribution showed 120 females (57.1%) and 90 males (42.9%). A chi-square analysis ($\chi^2 = 1.79$, $p > 0.05$) confirmed no significant gender bias, indicating balanced representation. The age distribution revealed that 58.7% of the participants were aged 18–25, and 41.3% were aged 13–17. A chi-square test ($\chi^2 = 9.84$, $p < 0.01$) indicated a significant difference in Internet engagement between age groups, with older students reporting higher daily use. Internet and social media activity revealed 84.8% daily usage, and 98.6% of respondents reported having at least one social media account. A one-sample t-test ($t(209) = 14.75$, $p < 0.001$) confirmed that mean daily usage significantly exceeded the hypothesised average of 4 hours/day, supporting the relevance of cybersecurity awareness initiatives.

3.1 Findings Analysis

The findings of the preliminary survey are summarised in Table 1-3.

Table 1
Preliminary survey statistical summary

Variable	N	Percentage (%)	Statistical Test
Gender (Female)	120	57.1	Chi-square = 1.79, p > 0.05
Gender (Male)	90	42.9	Chi-square = 1.79, p > 0.05
Age 18-25	123	58.7	Chi-square = 9.84, p < 0.01
Age 13-17	87	41.3	Chi-square = 9.84, p < 0.01
Daily Internet Use	178	84.8	One-sample t-test: t(209) = 14.75, p < 0.001
Social Media Account	207	98.6	Descriptive frequency

The chi-square test, as shown in equation (1), was applied to categorical data (gender, age group, and daily Internet use) to determine whether the observed frequencies significantly deviated from the expected distributions.

$$\chi^2 = \sum \frac{(O_i - E_i)^2}{E_i} \tag{1}$$

where O_i= observed frequency, E_i= expected frequency under the null hypothesis and the sum is taken over all categories. A larger χ^2 value indicates greater deviation from the expected distribution. In this study:

- **Gender ($\chi^2 = 1.79$, $p > 0.05$):** Not significant, suggesting proportional representation of male and female respondents.
- **Age group ($\chi^2 = 9.84$, $p < 0.01$):** Significant, indicating higher internet activity among 18–25-year-olds compared to 13–17-year-olds.

Table 1 confirms that respondents are digitally active across all genders and age groups, with nearly universal use of social media. The statistical findings demonstrate that older students are disproportionately more exposed online, supporting the need for targeted gamified interventions like Cyberpoly to promote cybersecurity awareness.

Table 2
Multi-Domain cybersecurity awareness analysis

No	Domain	Analytical Dimension	Core Findings
1	Self-Perception of Cybersecurity Skills	Confidence, awareness, and self-efficacy in managing cyber threats	Respondents demonstrated moderate confidence in identifying threats but limited practical readiness, indicating a gap between perception and performance in cybersecurity competence.
2	Password and Access Security Awareness	Password hygiene, authentication methods, and vulnerability awareness	Awareness of secure authentication was evident, but weak password reuse and limited adoption of multi-factor authentication remain prevalent.
3	Social Network Security Awareness	Privacy settings, phishing recognition, and responsible sharing behavior	High awareness of the importance of privacy, contrasted with inconsistent threat recognition, highlights behavioural gaps in applying secure online practices.
4	Online Gaming Awareness	Scam recognition, in-game data protection, and safe digital behavior	Awareness was lowest in this domain, as respondents demonstrated poor recognition of gaming-related threats, such as scams and phishing, revealing an overlooked risk environment.
5	Knowledge of Cyberattack Types	Familiarity with malware, phishing, ransomware, and social engineering attacks	Participants demonstrated a limited ability to identify and classify diverse cyberattacks, underscoring the need for more structured and experiential cybersecurity education.

Table 3
Statistical Summary of cybersecurity awareness domains

Domain	Mean Awareness Score (M)	Standard Deviation (SD)	Awareness Level	Ranking	Interpretation
1 – Self-Perception of Cybersecurity Skills	3.82	0.67	Moderate–High	2	Participants perceived themselves as relatively competent, although their skill execution lagged behind their perceived awareness.
2 – Password & Access Security	3.95	0.54	High	1	Highest mean awareness; however, behavioural inconsistency (weak passwords, poor MFA adoption) remained prevalent.
3 – Social Network Security	3.68	0.72	Moderate	3	Awareness of privacy principles was evident; however, the practical application of phishing recognition and privacy-setting tools was inconsistent.
4 – Online Gaming Security	3.21	0.81	Low–Moderate	5	Lowest awareness; users underestimated threats in recreational contexts, revealing a neglected aspect of risk perception.
5 – Knowledge of Cyberattack Types	3.47	0.76	Moderate	4	Partial familiarity with malware and phishing, but limited understanding of ransomware and social engineering tactics.

The analysis of Table 2 reveals that while participants exhibit moderate conceptual knowledge and self-confidence in cybersecurity, their practical preparedness and behavioral application remain limited. Awareness is highest in password security but weak in consistent protective behavior, especially regarding password reuse and multi-factor authentication. Privacy awareness is strong;

however, users often underestimate social engineering threats, and online gaming emerges as a critical vulnerability with minimal risk recognition. The findings indicate a fragmented state of cybersecurity literacy, where respondents demonstrate robust theoretical knowledge but lack practical application. This emphasizes the critical role of Cyberpoly's gamified and ethical approach in converting theoretical knowledge into consistent, secure digital practices.

Mean awareness scores were derived from 5-point Likert-scale items (1 = Strongly Disagree to 5 = Strongly Agree). Ranking was determined by descending mean values. Quantitative findings across Table 3 highlight distinct awareness gradients among the five cybersecurity domains. The highest mean score in password and access security (M = 3.95, SD = 0.54) suggests participants possess conceptual understanding of secure authentication practices, albeit not consistently applied. Self-perception of cybersecurity skills (M = 3.82) ranked second, indicating confidence in digital safety but insufficient depth in threat mitigation—reflecting the overconfidence phenomenon reported in prior security-behaviour research.

Mid-tier scores in social network security (M = 3.68) and knowledge of cyberattack types (M = 3.47) highlight partial literacy but persistent behavioural and conceptual gaps. The lowest awareness was recorded in online gaming security (M = 3.21, SD = 0.81), reaffirming that entertainment platforms constitute emerging threat vectors frequently overlooked in conventional cybersecurity training. Statistically, the domain variance (SD = 0.54–0.81) indicates heterogeneous literacy levels across topics, underscoring the necessity for differentiated and contextualized interventions. These findings validate Cyberpoly's gamified and ethically anchored design, which targets both cognitive and behavioural dimensions of cybersecurity learning to transform fragmented awareness into sustained, security-conscious behaviour.

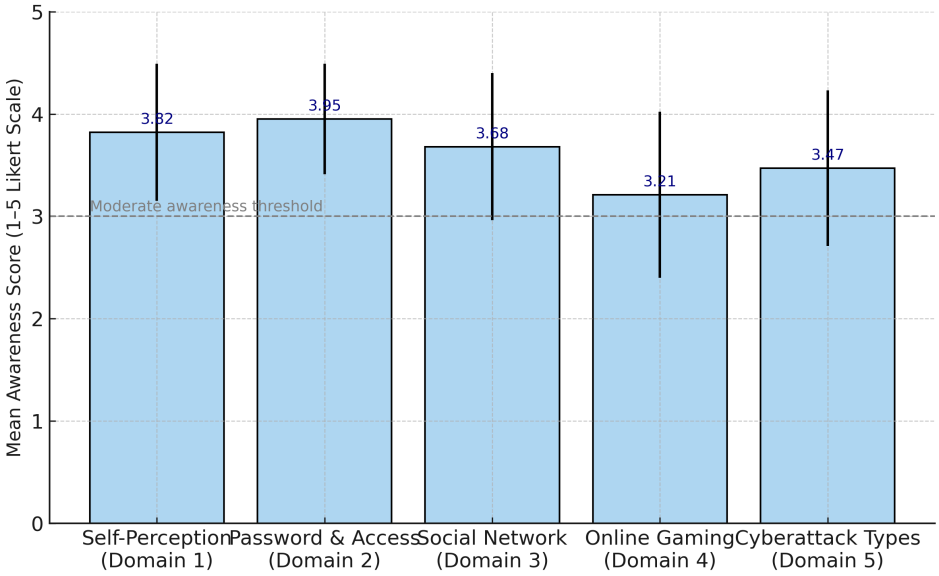

Fig. 3. Mean cybersecurity awareness scores across domains

This bar chart in Figure 3 illustrates the comparative mean awareness scores (1–5 Likert scale) across five cybersecurity domains, highlighting that password & access security achieved the highest awareness (M = 3.95), while online gaming security had the lowest (M = 3.21).

3.2 Discussion

The analysis shows that Cyberpoly successfully met its development objectives, demonstrating strong functionality and high user acceptance at a statistically significant level. End-user testing revealed a 98.4% satisfaction rate regarding functionality, with 100% of users agreeing on the reliability of its security authentication features. This highlights the system's operational integrity and its adherence to secure design principles. Additionally, respondents strongly agreed that Cyberpoly enhances cybersecurity awareness through its interactive and gamified learning approach. This confirms the platform's educational value in transforming complex cybersecurity concepts into practical knowledge. The alignment between engagement and understanding demonstrates Cyberpoly's effectiveness as a digital learning tool. Overall, these findings position Cyberpoly as a scalable and relevant model for cyber literacy education, capable of supporting institutional training, community awareness, and youth empowerment initiatives aimed at cultivating resilient and security-conscious digital citizens.

4. Conclusions

This study presents Cyberpoly, a gamified mobile application developed to enhance cybersecurity awareness among secondary and university students. Based on the DevSecOps methodology, Cyberpoly integrates security considerations throughout the software development lifecycle, including planning and monitoring. By incorporating both Naqli (informed) and Aqli (rational) knowledge, the app promotes cultural and ethical learning. It also embeds Islamic values such as Ta'alim (continuous learning) and Tawakkal (trust in God’s plan), making it a tool for both digital literacy and ethical digital citizenship. This approach emphasizes the importance of ethics in digital environments and aligns technology with cultural and moral values.

The preliminary survey of 210 students revealed high levels of digital engagement, with 84.8% reporting daily Internet use and nearly all respondents maintaining social media accounts. Statistical analyses confirmed balanced gender representation and significant differences in online behavior across age groups, underscoring the urgency of cybersecurity awareness programs for digitally active populations. Acceptance testing further showed that 98.4% of users perceived Cyberpoly as practical, smooth, and effective in increasing awareness of cyber threats. These findings validate the game’s capacity to combine motivation through gamification with secure design practices and culturally relevant educational content.

By aligning security-by-design principles with ethical reinforcement and user-centred gamification, Cyberpoly offers a novel model for cybersecurity education. It demonstrates how DevSecOps can be applied beyond conventional software engineering, ensuring both robust technical safeguards and pedagogical effectiveness. The results suggest that Cyberpoly can serve as a scalable, adaptable framework for building cyber-resilient communities, particularly among youth and student populations at high risk of cyber victimization. Future work will extend evaluation to larger, more diverse cohorts and integrate advanced analytics to monitor long-term behavioral change, thereby strengthening its contribution to national digital resilience and the global agenda of sustainable cyber-literacy.

Acknowledgement
This research was under the Research Grant Scheme (PPP1/BM/FST/USIM/13723), Universiti Sains Islam Malaysia (USIM).

References

[1] Malaysian Communications and Multimedia Commission (MCMC). Internet Users Survey 2020. The Internet Users Survey, 76. 2020. https://doi.org/ISSN1823-2523

[2] Kohli, S., V. Fabius, and S. M. Veranen. 2020. "How COVID-19 Is Changing Consumer Behavior—Now and Forever." McKinsey & Company, 1–3.

[3] Almarabeh, H. "The Impact of Cyber Threats on Social Networking Sites." *International Journal of Advanced Research in Computer Science* 10, no. 2 (2019): 1–9.

[4] Malaysia Computer Emergency Response Team (MyCERT). 2021. "Reported Incidents Based on General Incident Classification Statistics in 2021." Accessed September 30, 2025. https://www.mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-4d11-8169-66677d694932&id=77be547e-7a17-444b-9698-8c267427936c

[5] Masakazu, and Megumi. 2019. "A Challenge of Developing Serious Games to Raise the Awareness of Cybersecurity Issues." In Proceedings of the DiGRA International Conference: Game, Play and the Emerging Ludo-Mix

[6] Masakazu, and Megumi. "A Challenge of Developing Serious Games to Raise the Awareness of Cybersecurity Issues." In Proceedings of DiGRA International Conference: Game, Play and the Emerging Ludo-Mix, 2019.

[6] Grabosky, Peter. 2016. Cybercrime. New York: Oxford University Press.

[7] Chang, L. Y. C., and N. Coppel. 2020. "Building Cyber Security Awareness in a Developing Country: Lessons from Myanmar." Computers & Security 97: 101959.

[8] Cybersecurity ASEAN. 2020. "Fraud Continues to Be the Main Cause of Cybersecurity Incidents in Malaysia." Accessed September 30, 2025. https://cybersecurityasean.com/daily-news/fraud-continues-be-main-cause-cybersecurity-incidents-malaysia

[9] Malaysia Computer Emergency Response Team (MyCERT). Report Incidents Based on General Incident Classification Statistics 2023. August 10, 2024. https://www.mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-4d11-8169-66677d694932&id=2862eb40-2bc0-4b4e-90ed-07d4eef73b7b

[10] Malaysia Computer Emergency Response Team (MyCERT). Report Incidents Based on General Incident Classification Statistics 2024. August 10, 2024. https://www.mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-4d11-8169-66677d694932&id=23627097-41f2-4a21-8541-00a2b5c3352c

[11] Mason, Oliver J., Siobhan Collman, Stella Kazamia, and Ioana Boureanu. 2024. "Preparing UK Students for the Workplace: The Acceptability of a Gamified Cybersecurity Training." Journal of Cybersecurity Education, Research and Practice 2023 (1)

[12] Idierukevbe-Grand, I. U., and A. Addo. 2024. "Bridging the Cybersecurity Skills Gap: A Gamification Model." Journal of Business Studies Quarterly 14 (1). ISSN 2152-1034

[13] Matovu, Richard; Joshua C. Nwokeji; Terry Holmes; and Md Tajmilur Rahman. "Teaching and Learning Cybersecurity Awareness with Gamification in Smaller Universities and Colleges." In 2022 IEEE Frontiers in Education Conference (FIE), 1–9. IEEE, 2022. https://doi.org/10.1109/FIE56618.2022.9962519

[14] Yigit, Y., K. Kioskli, L. Bishop, N. Chouliaras, L. Maglaras, and H. Janicke. 2024. "Enhancing Cybersecurity Training Efficacy: A Comprehensive Analysis of Gamified Learning, Behavioral Strategies and Digital Twins." In Proceedings of the IEEE 25th International Symposium on a World of Wireless, Mobile and Multimedia Networks, 24–32.

[15] A.P. Sakinah, A. H. Azni, Farida Ridzuan, Najwa Hayaati Mohd Alwi, and Muhammad Syahmi Imran. 2025. "SWINDLERT©: Development of Augmented Reality Game-Based Interactivity for Enhancing Cybercrime Awareness." Journal of Computing Research and Innovation 10 (1): 77–88. https://doi.org/10.24191/jcrinn.v10i1.497

[16] Prates, Luís, and Rúben Pereira. 2024. "DevSecOps Practices and Tools." International Journal of Information Security. https://doi.org/10.1007/s10207-024-00914-z

[17] Feio, Miguel, et al. 2024. "An Empirical Study of DevSecOps Focused on Continuous Security." In SysSec / EuroSPW 2024