Journal of Advanced Research in Applied Sciences and Engineering Technology

Journal homepage:
https://semarakilmu.com.my/journals/index.php/applied_sciences_eng_tech/index
ISSN: 2462-1943

Inculcating Cybersecurity Awareness Among School Students through the Application of Courseware

Khairol Ezedy Abdul Rahman[1,*], Yusri Abdullah[1], Sumayyah Dzulkifly[2], Muhammad Modi Lakulu[2], Mohd Sidek Mohd Yunus[3], Wan Norhafiz Ashman Noruddin[4]

[1] Department of Creative Multimedia, Faculty of Art, Sustainability and Creative Industry, Universiti Pendidikan Sultan Idris, 35900 Tanjong Malim, Perak, Malaysia
[2] Department of Computer Science and Digital Technology, Faculty of Computing and Meta Technology, Universiti Pendidikan Sultan Idris, 35900 Tanjong Malim, Perak, Malaysia
[3] Faculty of Defence Science and Technology, National Defence University of Malaysia, Kem Sungai Besi, 57000 Kuala Lumpur, Malaysia
[4] Faculty of Business & Law, De Montfort University Kazakhstan, Amaty City, Medeu District, Al-Farabi Ave, 050044 Almaty, Republic of Kazakhstan

ABSTRACT

Malaysians have been exposed to the internet from a young age, and the COVID-19 pandemic in 2020 further increased internet access and gadget possession among school children due to remote learning. However, this technological progress has also brought about an increased risk of cybersecurity threats. To address this, a cybersecurity awareness courseware was developed to prepare students to utilize cyber infrastructure safely. The research paper focuses on cybersecurity awareness among secondary school students in Malaysia. With technology integration in education expanding, there was a pressing need to equip young learners with essential cybersecurity knowledge and skills. The study has been aimed at developing an interactive courseware to foster a proactive cybersecurity mindset, measuring its effectiveness using data-driven analyses while considering the country's cultural and educational context. The courseware was a web application with tailor-made modules covering topics like Wangiri, phishing, email scammer, social media scammer, and malware. It was designed in collaboration with Cybersecurity Malaysia, the authority for enhancing cybersecurity in the country. The courseware underwent a test run in a selected school, evaluating its success based on participant quiz scores. its development employed the ADDIE method, ensuring a systematic approach. The application of the courseware is expected to help increase cybersecurity awareness among school students while exposing them to cyber threats, potentially reducing the cyber-crime rate in Malaysia. The courseware has since shown promise as a potential addition to the Malaysian school curriculum as a dedicated cybersecurity module.

Keywords:
Cybersecurity; courseware awareness; cybersecurity threats; cybersecurity knowledge

[*] *Corresponding author.*
E-mail address: khairolezedy@fskik.upsi.edu.my

https://doi.org/10.37934/araset.58.1.175189

1. Introduction

Malaysian youth have grown up with widespread exposure to the Internet, starting from a tender age. The outbreak of the COVID-19 pandemic in early 2020 necessitated remote learning, which led to a surge in internet access and gadget ownership among school children. A 2020 survey by the Malaysian Communications and Multimedia Commission (MCMC) found that 89% of respondents were addicted to the Internet [1]. While this technological advancement has its merits, it also brings forth heightened risks and threats concerning cybersecurity. This research paper focuses on the pressing issue of cybersecurity awareness among secondary school students in Malaysia. As technology continues to permeate education, there is an increasing urgency to equip young learners with the necessary knowledge and skills to navigate the digital world securely. According to The Star [2] in 2019, three out of ten Malaysian youths are victims of cyberbullying that affects their education and social life, with the majority experiencing them through private messaging applications. The Star also added findings from the United Nations Children's Fund (UNICEF), that in Malaysia, out of the more than 5,000 respondents, 457 or 9% admitted they had used digital platforms to harass or bully others. The survey also found that 63% of the Malaysians, who took part in the poll, were not aware of cyberbullying helpline services. These findings have become an emergency call for responsible Malaysians to lead the younger generation to increase their cybersecurity awareness while embracing the cyber world. Prof Dr. Mohamad Fauzan Noordin, head of the Cybersecurity Cluster for Malaysian Crime Prevention Foundation in his statement to Bernama [3] stated that netizens must be aware of the risks of using the internet especially when sharing their personal information since it would be resourced by cybercriminals to be used against them for illicit gains.

The study was aimed at developing and implementing interactive and engaging courseware that fosters a proactive cybersecurity mindset among students. The effectiveness of the courseware in achieving its objectives was measured through data-driven analyses, taking into account Malaysia's cultural and educational context. The courseware was designed as a web application featuring various cybersecurity awareness modules tailored for school students. A selected school was chosen to conduct a test run of the courseware, and its success rate was evaluated based on the quiz scores of the participants. The courseware's development utilized the ADDIE method, a five-stage educational technology development approach involving Analysis, Design, Development, Implementation, and Evaluation tasks. In conclusion, safeguarding Malaysian students from cyber threats necessitates the development and implementation of interactive cybersecurity awareness courseware. By empowering the youth with essential knowledge and skills, we can create a generation that is well-equipped to protect themselves and others in the digital realm. This initiative not only contributes to a safer online environment for students but also bolsters the overall cybersecurity landscape in Malaysia.

Courseware is considered one of the learning methods of Open Educational Resource (OER) which was defined as technology-enabled, open provision of educational resources for consultation, use, and adaptation by a community of users for non-commercial purposes [4]. OER includes learning objects such as lecture materials, references and readings, simulations, experiments, and demonstrations, as well as syllabi, curricula, and teachers' guides [5]. The adoption of several interactive elements in courseware is a feature that makes it gain in popularity as a method of learning among students. It can also be used as a guided self-learning method for students where the equipped guided interface will help students to understand the learning module and content easily without the direct involvement of the instructor or teacher. Theoretical content adapted using electronic documents, podcasts, or videos; can be delivered to students using standard courseware [6]. Moreover, the flexibility that comes with courseware is another preference for students where

students would initiate their lesson anytime and anywhere as long as they are accessible to the required technology.

Along with courseware and OER gaining in popularity, the dependence on technology has also increased. This trend has also exposed the cybersecurity threat arising among students. The technology that students possess can serve a variety of purposes outside of education, especially for teenagers who tend to share their personal information online. Even worse, in some cases, the cyber world becomes their alternate reality through various applications and the variety of social media. Based on the Royal Malaysian Police (PDRM) statistics [7], over the past two years, almost 80% of rape cases reported to them involved friendships in the virtual world, and this is becoming more acute and alarming as more and more sexual predators use false identities on the Internet when hunting for victims. Children, especially school students who easily have access to gadgets and the internet are the easiest targets since they lack exposure to cyber threats faced in the cyberworld. As found by NACSA, 50% of the children in Malaysia were interacting on social media without parental supervision, and 94% of Malaysian children were exposed to internet pornography [10]. These alarming findings illustrate the seriousness of betrayal of trust and unethical conduct among school children. School children themselves need to be educated about cyber ethics and the impact of misconduct and unethical behaviour while embracing the cyber world. There should be no hesitation. This issue has to be contained as early as in the school years so that it does not have a major impact on school children [8] in the hope that cyber threats will not become a discipline issue among them.

Many countries such as the United States and Australia have initiated the cybersecurity awareness module for public schools by including the cybersecurity curriculum for school children as early as five years old up to 16 years old teenagers [9]. Through that curriculum, five-year-old kids would be taught not to share information with strangers such as their birth date or full names, and to "consult parents or guardians before entering personal information online". In Malaysia, The Ministry of Education (MOE) in collaboration with Cybersecurity Malaysia (CSM) plans to introduce a National Cybersecurity Awareness Module to 300 primary and secondary schools nationwide [3]. Most of the cybersecurity awareness campaigns for school children require involvement and cooperation from parents. This approach is necessary and extremely helpful for parents who also need to be responsible but have limitations in delivering cybersecurity awareness to their children. The cybersecurity awareness courseware would promote a comprehensive cybersecurity awareness program as one of the methods of delivery [25]. The courseware adopted the ADDIE model as the development model. The ADDIE model stands for Analysis, Design, Development, Implementation, and Evaluation and is structured as a sequential task in educational technology development [12]. It was developed for the U.S. Army by the Centre for Educational Technology at Florida State University. ADDIE was later implemented across all branches of the U.S. Armed Forces. Educators, instructional designers, and training developers find this approach very useful because having stages clearly defined facilitates the implementation of effective training tools. As for this research, the ADDIE model is referred to as an effective courseware development model for cybersecurity awareness modules for schools in Malaysia.

Cybersecurity education has emerged as a critical aspect of preparing individuals, especially young users, to navigate the digital landscape securely and responsibly. In this increasingly interconnected world, the prevalence of cyber threats demands a proactive approach to fostering cybersecurity awareness among school students. This section presents an extensive and comprehensive review of existing literature related to cybersecurity education and awareness among school students in Malaysia. The importance of cybersecurity education has gained significant attention in recent years, as cyber threats continue to evolve and expand in complexity. Scholars have emphasized that cybersecurity education is not limited to learning technical skills alone but also

includes imparting knowledge on risk awareness, privacy protection, and responsible digital behaviour [13]. Early exposure to cybersecurity concepts and best practices is essential, as young users are particularly vulnerable to cyber-attacks due to their limited experience in the digital realm. Researchers [14,15] highlighted the positive impact of cybersecurity education on individuals' cyber awareness and behaviour. Participants who received cybersecurity education during their formative years displayed a higher level of awareness and were less likely to fall victim to cyber-attacks. This reinforces the significance of introducing cybersecurity education in schools as part of a holistic approach to developing digital literacy and responsible online practices.

Incorporating cybersecurity topics into school curricula has been recognized as an effective strategy to reach a wide audience of young users. By integrating cybersecurity lessons into existing subjects like computer science, mathematics, and ethics, students can develop a well-rounded understanding of digital safety and the ethical use of technology [16]. This multidisciplinary approach not only strengthens students' technical skills but also instils critical thinking and decision-making abilities necessary to navigate the digital landscape effectively. Malaysia has witnessed a concerning rise in cyber incidents targeting young individuals, raising alarm bells about the need for improved cybersecurity awareness among school students. The Cybersecurity Malaysia Annual Report (2021). revealed that a significant percentage of cyber-attacks in the country targeted school students. These attacks ranged from phishing attempts aimed at stealing personal information to cyberbullying and harassment on social media platforms.

Malaysia Cybersecurity Strategy 2020-2024 states that the government has taken steps to address cybersecurity concerns through initiatives like the National Cybersecurity Policy (NCSP) and the CyberSAFE Program, the effectiveness of these programs in enhancing cybersecurity awareness among school students remains a subject of inquiry. Understanding the current state of cybersecurity awareness among students is crucial in designing effective and targeted educational interventions. Despite the importance of cybersecurity education, several challenges exist when delivering comprehensive and impactful programs to school students in Malaysia. Cyber threats are continually evolving, and new attack vectors emerge regularly. This dynamic nature of cyber threats presents a challenge to traditional teaching methods that may struggle to keep pace with the rapidly changing landscape [17]. Educational content must remain current and relevant to address the latest cybersecurity risks and provide students with up-to-date knowledge and skills. The digital divide in Malaysia poses a significant obstacle to the widespread implementation of cybersecurity education. Not all schools have equal access to digital resources and technology, particularly in rural and remote areas [18]. This disparity limits the reach of cybersecurity educational initiatives and can exacerbate the vulnerability of students in underserved regions. Cybersecurity education should not solely focus on technical aspects but also on the ethical and behavioural dimensions of online interactions. While technical knowledge is essential, instilling ethical values and responsible digital citizenship is equally critical [19]. Encouraging students to be ethical digital citizens can contribute to a safer and more respectful online environment, reducing instances of cyberbullying and other harmful online behaviours.

Interactive learning experiences provide students with practical application opportunities to reinforce their understanding of cybersecurity concepts. Simulated cyber-attack scenarios and role-playing activities enable students to immerse themselves in real-world situations, allowing them to develop critical thinking and problem-solving skills. Virtual labs and interactive quizzes offer hands-on experiences that bridge the gap between theory and practice, empowering students to apply their knowledge in authentic settings [21]. The active engagement afforded by interactive learning methods enhances students' retention of information and equips them with practical skills to safeguard themselves in the digital realm [24].

Therefore, the courseware approach for the cybersecurity awareness module is an appropriate tool to inculcate cybersecurity awareness for school students. Cybersecurity awareness should be groomed by the school students themselves to avoid the misuse of cyber facilities and unethical conduct in the cyber world. Among all those cybersecurity campaigns and awareness programs, the cybersecurity courseware would become an essential tool to inculcate cybersecurity awareness in school students since school students could make a self-study effort with minimum required supervision from schoolteachers.

2. Methodology

By Creswell's approach to sampling in research methodology, the selection of the sample population is a critical element in study design. Assessing heterogeneity is an essential step, particularly when examining a group of 23 schools. The degree of heterogeneity among these schools can significantly impact the representativeness and generalizability of the study findings. If the schools within the sample exhibit substantial similarities in terms of demographics, size, curriculum, and other pertinent factors, selecting one school as a representative might be appropriate. In such cases, this chosen school can effectively stand for the entire group due to the minimal variation observed across the sample.

Conversely, when there is notable variability among the schools in the sample, whether it be in demographics, size, curriculum, or other relevant factors, it becomes less likely for a single school to accurately represent the entirety of the group. In these situations, a more comprehensive approach to sampling and representation may be necessary to ensure a comprehensive and accurate reflection of the diverse characteristics present within the population of schools under study.

Qualitative research methods were used in the cybersecurity courseware that involved collecting and analysing non-numerical data to gain insights, understanding, and context regarding various aspects of cybersecurity. These methods are crucial for understanding human behaviours, attitudes, motivations, and perceptions related to cybersecurity. Utilizing open-ended questions in the quiz to gather qualitative data on cybersecurity-related topics participants could provide detailed responses, allowing for a deeper understanding of their thoughts and experiences. Besides, the quiz researcher would be able to conduct interviews with the students after they have all finished their session with the courseware. The purpose is to find in-depth information about their experiences, opinions, challenges, and perceptions related to cybersecurity courseware.

As mentioned earlier, the ADDIE model was used to build the courseware. Below is the structure based on the ADDIE model.

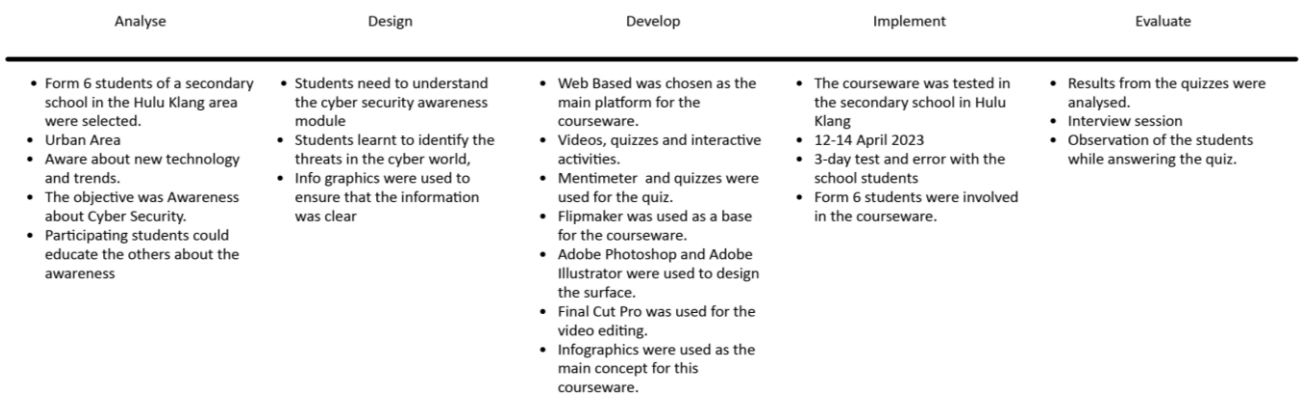

Fig. 1. ADDIE model structure for the courseware

2.1 Scope

The cybersecurity awareness courseware is a collection of cybersecurity awareness materials that were provided and suggested by multiple cybersecurity authorities in Malaysia such as CSM, NACSA, PDRM, and Malaysian Communication and Multimedia Commission or MCMC *Malaysia Cybersecurity Strategy 2020-2024.* As a result, the 2023 National Anti-Scam Tour in conjunction with the celebration of Safer Internet Day (SID) 2023 was officiated by the Minister of Communications and Digital, YB Fahmi Fadzil at CelcomDigi Tower, Petaling Jaya on 18 February 2023. The tour aimed to provide education and awareness to users about methods of recognizing scam calls, procedures, and the latest scam modus operandi as sharing tips and guidance to avoid becoming victims of scams or cyber threats.

The envisioned web-based interface for secondary school students integrated essential features to optimize learning progression. It systematically organizes educational materials, simplifying navigation through the curriculum. This would allow students to track their progress visually, clearly indicating completed and pending topics. Regular quizzes and assessments would be seamlessly integrated into the interface, serving as a gauge for understanding and progress. Immediate feedback and correct answers to these quizzes would facilitate comprehension. Furthermore, the platform offers performance analyses over time, providing insightful metrics for students to self-assess and identify areas for improvement. To enhance engagement, interactive elements such as drag-and-drop exercises, multiple-choice questions as we as engaging multimedia-like videos and interactive diagrams are embedded. A robust search functionality and filters would enable students to quickly locate specific materials or subjects. Additionally, students could offer feedback on materials and quizzes, contributing to continuous platform improvement. With a responsive design, the interface ensures accessibility across various devices, promoting seamless learning experiences while upholding security and privacy measures in compliance with regulations being of paramount consideration.

Furthermore, in the realm of cybersecurity awareness research, qualitative methodologies centre around interviews and quizzes as primary tools to delve into individuals' perceptions, knowledge, and behaviours regarding cybersecurity. Interviews are pivotal in qualitative research, providing a platform for open-ended discussions with participants. Cybersecurity-focused interviews allow researchers to probe participants about their thoughts, experiences, and understanding of cybersecurity threats, best practices, and their overall digital behaviour. These discussions elicit a qualitative understanding of how individuals perceive cybersecurity risks; what actions they take to mitigate these risks and what challenges they face. Through narratives and personal anecdotes, interviews can uncover the psychology behind security decisions and the factors influencing individuals' cybersecurity awareness.

Quizzes, although typically associated with quantitative assessment, can also be adapted qualitatively. Instead of focusing solely on scores, open-ended questions within a quiz format can be incorporated, allowing participants to explain their choices and thought processes when answering cybersecurity-related questions. These qualitative insights provide a deeper understanding of the reasoning, misconceptions, or uncertainties that participants might have regarding specific cybersecurity concepts. Additionally, quizzes can serve as interactive tools during interviews, prompting participants to actively engage with cybersecurity scenarios and share their responses, fostering a dialogue and enriching qualitative data. By combining insightful interviews and interactive quizzes, researchers can explore the nuances of cybersecurity awareness, gaining qualitative insights into individuals' knowledge gaps, attitudes, decision-making, and areas that require targeted educational efforts. This holistic understanding is instrumental in tailoring cybersecurity awareness

initiatives to effectively address the specific needs and perceptions of the audience, ultimately enhancing overall cybersecurity resilience.

2.2 Limitation

As mentioned in the scope, the ADDIE (Analysis, Design, Development, Implementation, and Evaluation) model is a widely used instructional design framework for creating effective educational courses, including those in the field of cybersecurity. However, it is important to recognize certain limitations when applying the ADDIE model to cybersecurity courseware development.

One limitation is the potential for inflexibility within the ADDIE model. The linear nature of the ADDIE phases may not align well with the dynamic and evolving nature of cybersecurity. In cybersecurity, new threats, technologies, and best practices constantly emerge, requiring rapid updates and adjustments to course content and structure. The rigid sequence of the ADDIE model may hinder the ability to adapt quickly to these changes, potentially leading to outdated or less effective courseware.

Additionally, the ADDIE model may face challenges in adequately addressing the real-time, hands-on nature of cybersecurity training. Cybersecurity skills are often best developed through practical, interactive experiences such as simulations, labs, and live exercises. The ADDIE model's emphasis on systematic planning and design may not fully integrate or prioritize these crucial experimental components, limiting the development of practical skills in a cybersecurity context.

Moreover, the evaluation phase of the ADDIE model may not fully encompass the comprehensive assessment of cybersecurity courseware. Evaluating the effectiveness of cybersecurity training involves not only assessing knowledge retention but also measuring applied skills, incident response capabilities, and the ability to defend against real-time threats. The traditional ADDIE evaluation framework may need augmentation to encompass these multifaceted aspects adequately.

In summary, while the ADDIE model is a valuable tool for instructional design, its inherent structure and rigidity can pose challenges when applied to the dynamic and practical realm of cybersecurity education. Flexibility, real-time practical experiences, and a more comprehensive evaluation approach are crucial considerations for addressing the limitations and enhancing the effectiveness of cybersecurity courseware developed using the ADDIE model.

This extensive research project is carefully intended to develop in three different and precisely prepared phases. Each phase is meticulously intended to build on the one before it, resulting in a progressive and unified investigative journey that attempts to get to the heart of the matter. This method provides for a methodical investigation of the research issue, resulting in a detailed and informative study. We want to offer useful insights and breakthroughs to the current body of knowledge in the subject by carefully executing these three phases, increasing our understanding and paving the road for relevant implications and applications.

3. Results

Concerned over the cybersecurity issues on children, the National Cybersecurity Agency (NACSA) took the initiative of producing a cyber-parenting handbook [22] in the hope that cybersecurity awareness among children could be conveyed through parent guidance and surveillance. Although the role of parents is crucial in this problem, some constraints such as career, responsibilities in society, and educating skills make cybersecurity awareness difficult to deliver to children through the role of one party alone. Even a cybersecurity expert parent might face some difficulty in delivering their expertise well to their children even though they are in the cybersecurity industry. On the other

hand, Malaysian schools have the experience and dedication to educating and mind-shaping youngsters with a structured curriculum [11]. This advantage can be utilized to inculcate cybersecurity awareness practices among school children. Together with the parent's responsibility, the cybersecurity practice among school children could be used in grooming in many ways. Even though there are possibilities that the school teachers' knowledge and expertise in cybersecurity can be questioned, it can be overcome with the help of structured module cybersecurity courseware. The planned courseware will contain all suitable materials for cybersecurity awareness that will be properly tailored for Malaysian school students. It is also planned to be equipped with self-study guidance to enable self-study skills with minimal supervision of school teachers [23].

The charts below show the main content structure inside the courseware. The research will only focus on this content because of the secondary school level.

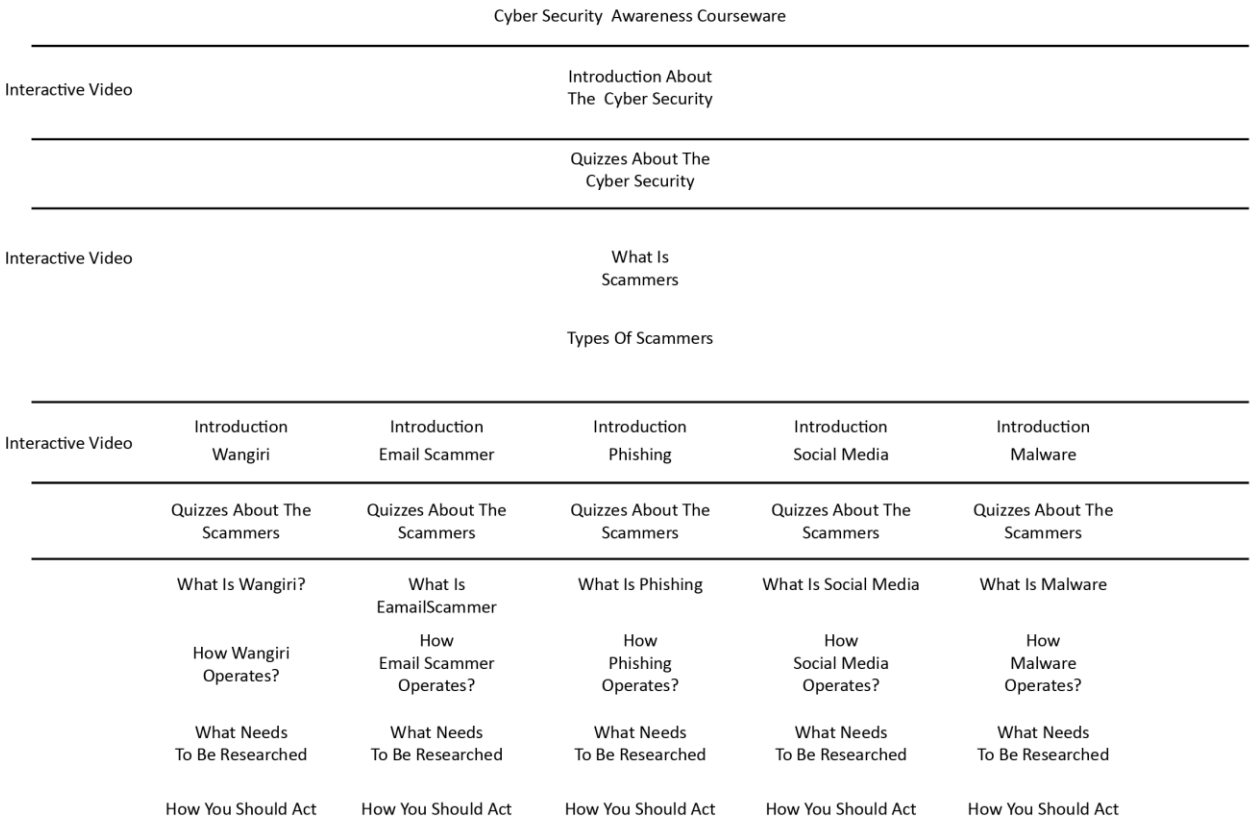

Fig. 2. Content structure in cybersecurity courseware

The insights derived from this research offered profound implications for cybersecurity education among school students in Malaysia. This section delves into the nuanced analysis of the data, exploring potential strategies to address the challenges encountered during the implementation of an advanced courseware model. Undoubtedly, a cybersecurity awareness module tailored for school children in Malaysia holds paramount significance, shaping their digital behaviour, guarding them against cyber threats, and nurturing a secure digital environment for the nation as a whole. This study was meticulously conducted in a secondary school in Hulu Klang, Selangor, employing a simple yet effective sampling technique to gather responses from a sample size of 162 students. The respondents comprised 78 males and 84 females. There were 73 students aged between 17-18 and the other 89 students between 19-20 years old. Most of the students (comprising 126 students) were not aware of the cybersecurity awareness campaign, while 36 students were aware of it.

Fig. 3. Snap screen cover cybersecurity courseware

The importance of a cybersecurity awareness module for school children cannot be overstated, particularly in the digital era where a multitude of online threats abound. This study illuminates the efficacy of utilizing infographics to simplify complex cybersecurity concepts, enhancing students' understanding and engagement with this critical subject matter. One prevalent scam that students should be vigilant about is the "Wangiri" or "one-ring" scam, a deceptive ploy where scammers make short phone calls to numerous numbers, encouraging callbacks. Students need to be aware that returning these calls can lead to exorbitant charges on their phone bills. Thus, cybersecurity education equips students with the knowledge to protect themselves from such scams, promoting online safety. Scammers capitalize on premium rate numbers, leaving unsuspecting victims burdened with unauthorized call charges. The research involving 162 students yielded encouraging results, with 147 students demonstrating a good understanding of handling calls from unknown international numbers. This high level of awareness showcases commendable caution and vigilance among students in today's digital landscape where scams and fraudulent activities proliferate. However, it is imperative to address the concerns of the 15 students who expressed uncertainty about the appropriate actions in such scenarios.

Email scammers engage in phishing, posing as reputable entities to deceive recipients into divulging sensitive information. These scams, occurring through various communication channels, underline the necessity of educating students on recognizing and combating them. Out of the 162 students surveyed, it is reassuring that 119 students exhibit a good understanding of how to recognize and handle email scams. These students display awareness of the potential risks associated with unsolicited emails, showcasing their ability to protect themselves. However, 42 students might benefit from additional clarity and guidance on this subject.

Phishing is a deceptive and fraudulent technique employed by malicious actors to trick individuals into revealing sensitive information, such as login credentials, financial data, or personal information, by posing as trustworthy entities. These attempts occur through various channels like emails, text messages, phone calls, or fake websites. Among the 162 students surveyed, a substantial number—141 students—demonstrated a commendable understanding of what phishing entails and how to identify it. Phishing represents a digital ruse where individuals impersonate trustworthy entities, coercing recipients into divulging sensitive information through lures of urgency or enticing promises. The danger lies in the attempt to create a sense of urgency, pressuring recipients to act hastily. It's

essential to educate all students comprehensively, as evidenced by 12 students providing incorrect answers and 9 expressing uncertainty about handling phishing attempts.

Similarly, the study sheds light on social media scams, illustrating the urgent need for enhanced understanding and awareness. Only 112 students out of the 162 surveyed displayed a solid understanding of social media scammers and their operations. Social media scammers employ deceitful tactics on platforms to deceive users, exploiting trust and widespread usage for personal gain or malicious intent. The presence of 50 students providing incorrect answers emphasizes the critical necessity for education and awareness about social media scams, urging immediate attention and targeted educational efforts to bridge this knowledge gap. To mitigate risks, individuals should exercise caution and scepticism online, refraining from sharing personal information and engaging with suspicious links or unverified profiles. Educating students and the wider community about the red flags associated with social media scams is crucial, fostering a culture of awareness and promoting safe online practices.

Fig. 4. Snap screen inside cybersecurity courseware

Furthermore, the research highlights the need for a greater understanding of malware and its potential threats. Only 132 students out of 162 demonstrated a clear understanding of this topic. A malware scammer is an individual or a group that deploys malicious software, known as malware, with the intent to harm users' devices, steal personal data, or compromise their security. Various forms of malware, such as viruses, spyware, ransomware, or trojan horses, often disguise themselves as legitimate software or files. The concerning aspect is that 21 students provided incorrect answers about malware, and 9 students expressed uncertainty in handling malware-related situations. This underscores a critical gap in awareness and education about cybersecurity threats like malware and the essential precautions required to stay safe. Malware can have severe consequences, including identity theft, financial loss, or device damage. It's crucial to educate students and the broader community about recognizing suspicious signs, avoiding downloads from untrusted sources, regularly updating security software, and not clicking on unfamiliar links or email attachments. Additionally, emphasizing the importance of regularly backing up data and reporting any suspicious activities can enhance protection against malware. Empowering students with knowledge on how to recognize, prevent, and respond to malware attacks is paramount. This includes fostering a culture of reporting potential threats and seeking assistance from trusted sources. With a collective effort to enhance

awareness and understanding, we can fortify our defences against malware and create a safer digital environment for all.

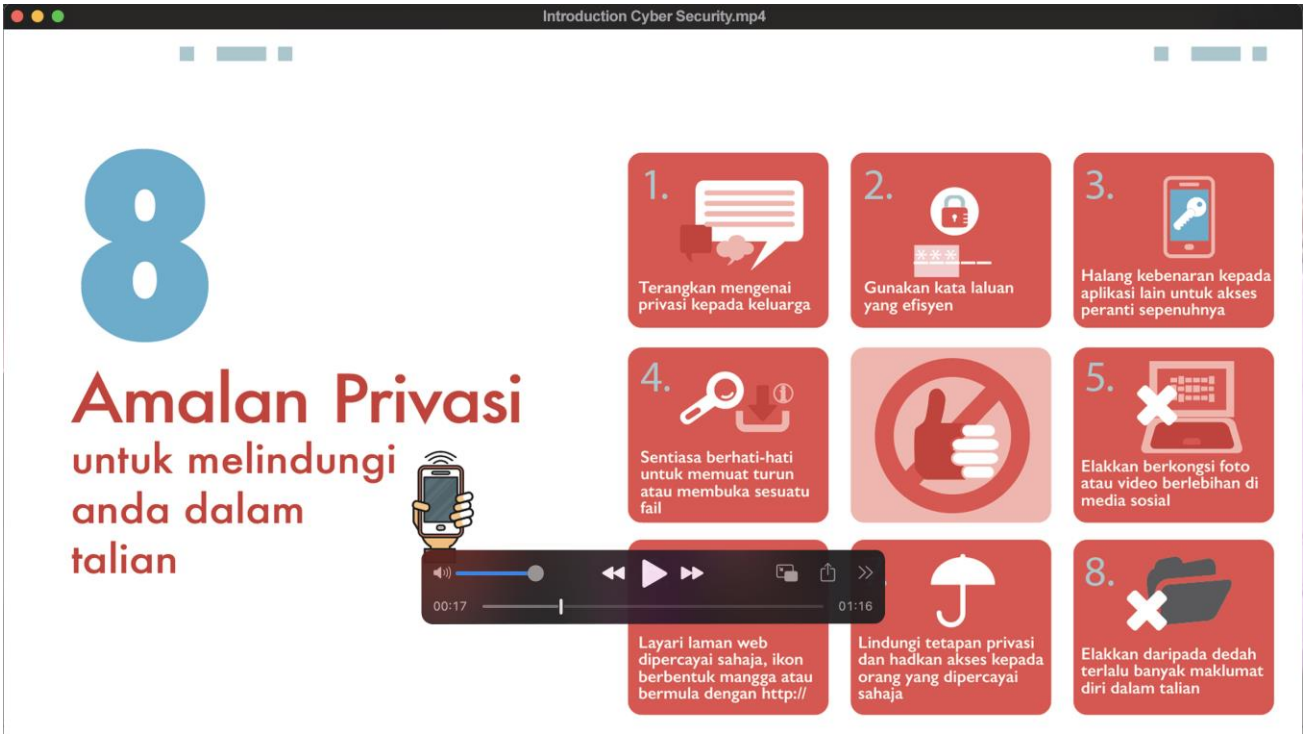

Fig. 5. Snap screen video cybersecurity courseware

During the interview, there were two questions asked of the students. Below are the questions and the answers given.

3.1 Why a Cybersecurity Awareness Module is Extremely Essential for School Children?

More than half of the students (138 respondents) did not understand the cybersecurity awareness content while only 24 students understood the content from the cybersecurity awareness campaigns that they watched in the media. There were three reasons why the students did not understand the cybersecurity awareness courseware. It was too complicated with too much information about cybersecurity. Most of the students skipped the information about the awareness when the graphics were too dull and uninteresting.

After the courseware session with the students, the researchers found that 92 out of 162 students were able to understand cybersecurity awareness while using the internet. Most of them agreed that by enhancing the graphics in the courseware they were more focussed on the content. When using infographics as the main mode of information, the students could understand more about the content. Infographics played a crucial role in the courseware for several reasons. They are effective tools for presenting information in a visually appealing and engaging manner, making complex concepts easier to understand. As visual representation, infographics use a combination of images, icons, charts, and text to present information in a concise and visually appealing way. Visuals can enhance learning by providing a clear representation of concepts, making it easier for learners to process and retain information. Normally infographics simplify complex concepts and course materials often contain complex information that may be challenging for learners to grasp. Infographics break down these complex ideas into smaller, digestible chunks, making it easier for students to understand the content. Visuals are known to enhance memory retention and recall.

Infographics create a memorable learning experience, helping learners recall information more effectively during exams or real-world applications. Data and information are well organized. This is because infographics allow course designers to organize information in a structured and logical manner. By using visual hierarchy and layout, important points can be emphasized, and connections between different ideas can be illustrated clearly. In courses that involve data analysis or statistics, infographics can effectively present data in a visually appealing way, making trends and patterns more evident and easier to comprehend [15].

3.2 How was the School Students' Acceptance of the Cybersecurity Awareness Courseware?

Cybersecurity education has evolved as a vital pillar of knowledge in today's digital environment. The recently implemented revolutionary cybersecurity courseware has received great appreciation for its novel approach to engaging and informing students. This courseware goes beyond standard approaches by engaging students in interactive activities that build better knowledge and respect for the challenges of cybersecurity.

The courseware's interactive design, which has struck a deep chord with students, is fundamental to its success. Many people have cited this feature as being crucial in piquing their interest and improving their understanding of cybersecurity principles. The courseware demystifies complex topics through immersive learning experiences, making them more approachable and relevant. Students not only internalize academic information but also develop the practical abilities required for real-world application as a result of this strategy. The use of practical activities and simulations improves the courseware's efficacy even more. Students have commended these hands-on components for bridging the theoretical and practical divide. Participants receive essential experience in applying theoretical principles to real-life settings by participating in simulated cyber threat scenarios. This active learning not only broadens their awareness but also gives them renewed confidence in their capacity to mitigate possible cyber hazards.

Among the 162 students in the cohort, 135 indicated substantial gains in their understanding of cybersecurity topics after engaging with the courseware. Notably, a significant majority of these students successfully turned their knowledge into practical abilities, applying essential insights to real-world circumstances. This practical knowledge not only improves individual cyber resilience but also allows students to have an impact outside of the classroom.

The good impact of the cybersecurity courseware on participants' families is a stunning testimonial to its transforming impact. Students have taken on the role of cybersecurity champions inside their own houses, armed with increased information. They have bridged the cybersecurity gap for their family members through patient advice and open communication, establishing a culture of alertness and secure internet practices. As a result, their loved ones are protected from potential cyber-attacks. The influence of the courseware extends beyond individual lives, influencing the digital behaviours of entire communities. The growth of a feeling of personal responsibility and a communal commitment to ensuring a safer digital environment is at the base of this ripple effect. As more people take on the role of cybersecurity advocates in their social networks, the combined impact of their actions enhances the collective cyber defence.

Finally, the development of new and engaging cybersecurity courseware signals a watershed moment in cybersecurity education. Its emphasis on interactive learning, practical application, and the development of cybersecurity champions within families and communities demonstrates its enormous influence. The courseware builds the groundwork for a safer digital world by providing students with the skills to integrate theoretical knowledge into actionable insights. As these young

cybersecurity experts continue to advocate for online safety, their efforts will strengthen the digital landscape for future generations.

4. Conclusions

In conclusion, this research emphasizes the urgency of inculcating cybersecurity awareness among school students in Malaysia. The data analysis underscores the importance of early education to equip students with the knowledge and skills to navigate the digital landscape safely and responsibly. The application of an advanced courseware model, enriched with gamification and interactive elements, demonstrated its efficacy in enhancing students' understanding of cybersecurity issues and fostering ethical online behaviour.

Addressing challenges such as the digital divide and providing adequate teacher training will be crucial to the sustainable implementation of the courseware on a national scale. The long-term impact of the program will be evaluated through follow-up surveys, providing valuable insights for future improvements and iterations. Overall, by empowering the younger generation with cybersecurity awareness, Malaysia can take a proactive stance against cyber threats, creating a safer and more secure digital future for its citizens. Introducing cybersecurity concepts to secondary school children in Malaysia is of paramount importance, given the high prevalence of internet usage among this age group. Malaysian secondary school children are active users of digital technologies, making them vulnerable to various cybersecurity threats and risks. In today's digital age, these students, being part of the digital native generation, are growing up with technology as an integral part of their lives. Incorporating a dedicated cybersecurity awareness module into their curriculum is essential to ensure safe and responsible internet usage. This is particularly crucial as secondary school students often spend a considerable amount of time online and may exhibit careless or reckless behaviour in using computers and digital devices.

Research indicates that, despite the many benefits of the internet, there are notable negative aspects related to its use. Protecting personal information is a significant concern, and it is vital to educate secondary school children about the importance of safeguarding their data to mitigate risks such as identity theft, phishing, and other cybercrimes. Studies have shown that secondary school children in Malaysia, ranging from 12 to 19 years old, tend to overshare information online and lack awareness of how to protect sensitive data. Cyberbullying is a prevalent issue affecting youth in Malaysia, including those in secondary schools. According to the United Nations Children’s Fund (UNICEF), cyberbullying is a significant concern in Malaysia, underscoring the urgency of integrating cybersecurity education into the curriculum. Educating secondary school children about cybersecurity empowers them to recognize and report cyberbullying incidents, thereby fostering a safer online environment. Incorporating parents into the cybersecurity education of secondary school children is equally vital. Well-informed children can effectively share their knowledge with their parents, enabling families to collectively understand potential online threats and risks. This collaborative approach ensures a safer digital environment for the entire family and promotes responsible digital citizenship.

As cyber threats continue to evolve, early education on cybersecurity equips secondary school children with the necessary skills and knowledge to protect themselves and their communities from cyber-crimes effectively. Integrating responsible digital citizenship with cybersecurity awareness fosters a positive online community, encouraging ethical online behaviour among secondary school children in Malaysia. Ultimately, this comprehensive approach to education empowers Malaysian secondary school children to navigate the digital world securely and contribute positively to the online society.

Acknowledgment

This research was funded by a Skim Geran Galakan Penyelidikan Universiti Pendidikan Sultan Idris (GGPU) 2021 (Inculcating Cybersecurity Awareness Among School Students Through the Application of Courseware 2021-0103-107-01)

References

[1] Zulkifli, Zahidah, Nurul Nuha Abdul Molok, Nurul Hayani Abd Rahim, and Shuhaili Talib. "Cyber security awareness among secondary school students in Malaysia." *Journal of information systems and digital technologies* 2, no. 2 (2020): 28-41. https://doi.org/10.31436/jisdt.v2i2.151

[2] The Star. "Three in 10 are bullied online." (2019). https://www.thestar.com.my/news/nation/2019/09/06/three-in-10-bullied-online

[3] Bernama. "Cybersecurity Awareness Module to be introduced in 300 schools." (2020). http://youth.bernama.com/v2/news.php?id=1813305&c=7

[4] UNESCO. "UNESCO Promotes New Initiative for Free Educational Resources on the Internet." (2002). http://www.unesco.org/education/news_en/080702_free_edu_ress.shtml

[5] Jalil, Masita, Noraida Hj Ali, Farizah Yunus, Fakhrul Adli Mohd Zaki, Lee Hwee Hsiung, and Mohammed Amin Almaayah. "Cybersecurity Awareness among Secondary School Students Post Covid-19 Pandemic." *Journal of Advanced Research in Applied Sciences and Engineering Technology* 37, no. 1 (2024): 115-127. https://doi.org/10.37934/araset.37.1.115127

[6] Urquiza-Fuentes, Jaime. "Increasing students' responsibility and learning outcomes using partial flipped classroom in a language processors course." *IEEE Access* 8 (2020): 211211-211223. https://doi.org/10.1109/ACCESS.2020.3039628

[7] Talib, Y.Y.A. "Keselamatan di alam maya." (2017). https://www.hmetro.com.my/hati/2017/12/295907/keselamatan-di-alam-maya

[8] Rahman, Nurul Amirah Abdul, Izzah Hanis Sairi, Nurul Akma M. Zizi, and Fariza Khalid. "The importance of cybersecurity education in school." *International Journal of Information and Education Technology* 10, no. 5 (2020): 378-382. https://doi.org/10.18178/ijiet.2020.10.5.1393

[9] Dzafri, D. "5-year-old kids in Australia will soon have cybersecurity in their school curriculum." (2021). https://soyacincau.com/2021/05/01/5-year-old-kids-in-australia-will-soon-have-cybersecurity-in-their-school-curriculum/

[10] NACSA. "Cyber Parenting Guidebook." (2018). https://www.nacsa.gov.my/doc/keibubapaansiber.pdf?t=1623836800652118839

[11] Rahman, R. "Carut, adab dan dilema sang guru." (2021). https://www.sinarharian.com.my/article/128200/SUARA-SINAR/Lidah-Pengarang/Carut-adab-dan-dilema-sang-guru

[12] Kurt, Serhat. "ADDIE model: Instructional design." *Educational Technology* 29 (2017).

[13] Al Shamsi, Arwa A. "Effectiveness of cyber security awareness program for young children: A case study in UAE." *Int. J. Inf. Technol. Lang. Stud* 3, no. 2 (2019): 8-29.

[14] Venter, Isabella M., Rénette J. Blignaut, Karen Renaud, and M. Anja Venter. "Cyber security education is as essential as "the three R's"." *Heliyon* 5, no. 12 (2019). https://doi.org/10.1016/j.heliyon.2019.e02855

[15] Cain, Ashley A., Morgan E. Edwards, and Jeremiah D. Still. "An exploratory study of cyber hygiene behaviors and knowledge." *Journal of information security and applications* 42 (2018): 36-45. https://doi.org/10.1016/j.jisa.2018.08.002

[16] Yamin, Muhammad Mudassar, and Basel Katt. "Cyber security skill set analysis for common curricula development." In *Proceedings of the 14th International Conference on Availability, Reliability and Security*, pp. 1-8. 2019. https://doi.org/10.1145/3339252.3340527

[17] Onyema, E. M., A. E. Dinar, S. Ghouali, B. Merabet, R. Merzougui, and M. Feham. "Cyber threats, attack strategy, and ethical hacking in telecommunications systems." In *Security and privacy in cyberspace*, pp. 25-45. Singapore: Springer Nature Singapore, 2022. https://doi.org/10.1007/978-981-19-1960-2_2

[18] Noor, Marhaini Mohd, Mohamed Aiman Shah Hj Johan Shah, and Nur Syahzanani Hani Mohd Zamri. "User Acceptance Of Cyber Security Application (Our Cyberhero) Among Secondary School Students, Teachers And Local Communities In Coastal Terengganu District: A Preliminary Study For Maritime Education." *Journal of Maritime Logistics* (2022): 79-89. https://doi.org/10.46754/jml.2022.12.006

[19] Kshetri, Naresh. "The Global Rise of Online Devices, Cyber Crime and Cyber Defense: Enhancing Ethical Actions, Counter Measures, Cyber Strategy, and Approaches." PhD diss., University of Missouri-Saint Louis, 2022.

[20] Zadeja, Imelda, and Jozef Bushati. "Gamification and serious games methodologies in education." In *International Symposium on Graphic Engineering and Design*, pp. 599-605. 2017.
[21] Jalil, Masita, Noraida Hj Ali, Farizah Yunus, Fakhrul Adli Mohd Zaki, Lee Hwee Hsiung, and Mohammed Amin Almaayah. "Cybersecurity Awareness among Secondary School Students Post Covid-19 Pandemic." *Journal of Advanced Research in Applied Sciences and Engineering Technology* 37, no. 1 (2024): 115-127. https://doi.org/10.37934/araset.37.1.115127
[22] Yuliana, Yuliana. "The importance of cybersecurity awareness for children." *Lampung Journal of International Law* 4, no. 1 (2022): 41-48. https://doi.org/10.25041/lajil.v4i1.2526
[23] Zulkifli, Faiz, and Rozaimah Zainal Abidin. "Identity in the Digital Age: An Investigation of Malaysian Perspectives on Technology and Privacy." *Journal of Advanced Research in Applied Sciences and Engineering Technology* 43, no. 2 (2025): 1-20. https://doi.org/10.37934/araset.43.2.120
[24] Azam, Nurul Alieyah, Alya Geogiana Buja, Nor Masri Sahri, Rabiah Ahmad, Nur Fadly Habidin, Shekh Faisal Abdul Latip, Mohamad Yusof Darus, Mohd Shahril Hussin, and Saharudin Saat. "A Light Review on Cyber Security Awareness Models for the Elderly." *Journal of Advanced Research in Applied Sciences and Engineering Technology* 44, no. 1 (2025): 31-45. https://doi.org/10.37934/araset.44.1.3145
[25] Zulkifli, Faiz, and Rozaimah Zainal Abidin. "Identity in the Digital Age: An Investigation of Malaysian Perspectives on Technology and Privacy." *Journal of Advanced Research in Applied Sciences and Engineering Technology* 43, no. 2 (2025): 1-20. https://doi.org/10.37934/araset.43.2.120