SMART CTZEN: A DIGITAL STORYTELLING APP TO EMPOWER YOUTH'S AWARENESS IN CYBER SAFETY AND SECURITY

NURUL NUHA ABDUL MOLOK [1*], NURIDAH BINTI SAPEE[1], ANIS ASILA OTHMAN[1]

[1]Department of Information Systems, Kulliyyah of Information and Communication Technology, International Islamic University Malaysia

**Corresponding author: nurulnuha@iium.edu.my*

ABSTRACT: The impact of the COVID-19 epidemic on Malaysian educational institutions highlights the rise in cybercrime cases among students. Studies indicate that university students are the top users of the Internet with high daily internet usage, yet, this group of users are not only the victims but also the perpetrators of cyber threats and crimes. Despite being the top Internet users, youth aged 18-25 have been found to have limited understanding of cyber threats, making them more susceptible to such threats, or to become an accidental outlaw. Therefore, this study aims to uncover the types of threats that are prevalent among university students and ways to address these threats. This study found that majority of undergraduate students experienced cyberbullying, gaming addiction, depression and anxiety due to cyber threats, online sexual harassment and online financial scams. In order to address this contemporary phenomenon, this study proposes a digital storytelling application which aims to educate youth about strategies to recognize cyber threats, respond to these threats appropriately, and make informed decisions about their cyber behaviour. It also proposes that being vigilant about these strategies are in line with Islamic teachings and principles. This will equip them with the necessary knowledge and skills to protect themselves, their finances, and their safety, security and privacy in the cyber space, so that they are able to contribute to a safer digital community.

KEY WORDS: *Youth, Cyber safety, Cyber security, Cyberbullying, Internet addiction, Digital storytelling*

1. INTRODUCTION

Malaysia and countries around the world have been hit by the COVID-19 outbreak which made many governments impose lockdowns, urging everyone to stay at home and work remotely to stop the virus from spreading. This includes educational institutions, which encountered many difficulties in teaching and learning. All institutions around the world were forced to shut down their physical campuses and focused on online learning. Despite the benefits of online learning, studies have found issues among students which include being attached to electronic gadgets for activities other than online learning (Abdul Molok & Zulkilfli, 2021; Abdul Molok, Abdul Hakim & Jamaludin, 2023). Although the lockdowns are no longer being imposed in Malaysia and globally, the users of the Internet are getting accustomed to the technology, making Internet use is still prevalent today, especially among today's youth. This widespread use has not only increased

productivity issues among students but also caused the rise of cybercrime cases in which they are both victims and perpetrators of such crimes.

Malaysian Communications and Multimedia Commission (MCMC) reported that the percentage of Internet users in Malaysia increased from 88.7% from the total Malaysian population in 2020 to 92.7% in 2022 (MCMC, 2022). This was mainly due to nationwide lockdowns which had a "direct impact to remote work and remote education within the reach of many" (MCMC, 2022, p.16). It further reports that majority of the Internet users in Malaysia are within the age of early 20s, which is the age of university students. Furthermore, 16.1% of Internet users under the age of 20 spent more than 18 hours a day while 15.3% came from users in their 20s (MCMC, 2022). These results indicate that students in tertiary education or higher learning institutions are the top Internet users in Malaysia with the highest number of users and the highest time spent on the Internet came from this age group. Unfortunately, this age group was found to be the most vulnerable to cyber threats and most prone to cyber-attacks (Fatokun, Hamid, Norman & Fatokun, 2019; (Muniandy, Muniandy & Samsudin, 2017; New Straits Times, 2022b). Among the reasons are unfamiliarity to cyber threats, password sharing practice and susceptibility to phishing. Similarly, Shaikh, Rehman and Amin (2020) agree that university students are amongst the most frequent users of the Internet. Such exposure to the Internet exposes them to sexual and violent content, cyberbullying, fake content, religious extremism, drugs and expressing political opinions online. Hence, it is not surprising that Malaysia ranked the second in Asia for cyberbullying among youth (The Star, 2022).

Other than that, Zhou and Xing (2021) report that college students are susceptible to online games addiction which is damaging to their studies and deteriorating their physical and mental health. Such addiction is due to lack of self-control, and lack of communication, care and attention among family members. In their study, they found that online game addicts had lower impulse control, unhealthy habits, difficulty to resist temptation, and difficulty to focus on work or study. Interestingly, Abdul Molok & Zulkifli (2021) point out a Malaysian university student being an accidental outlaw when he posted a sensitive remark on his Facebook status.

Realizing the continuous online danger that youth are facing, Fatokun et al. (2019) and Shaikh et al. (2020) suggest that students in tertiary education need to be taught about cyber security in order to be familiar with cyber threats and learn about ways to address those threats.

Following this stance, this project developed a digital storytelling application (a multimedia application that uses interactive elements to tell stories or present ideas) to provide interactive and graphical presentation of cyber safety and security storytelling using videos, images and audio files to educate university students about top cyber threats to this age group and how to address such threats. The application is not only intended to educate youth about cyber safety and security but also to empower them to combat cyber threats so that they can empower their peers to do the same. It starts with the introduction to the current phenomenon, and subsequently provides the review of literature on top cyber threats that are predominant among university students. Then, this study presents the review of existing system applications to uncover important features that can be adopted and

adapted in our application. Afterwards, research methodology and the results of a survey on university students will be provided to understand their demographics, how they used the Internet, cyber threats that they experienced, their security practices and what kind of features that they wished to see a digital storytelling application. Finally, it provides the conclusion and recommendations of the study.

2. REVIEW OF LITERATURE

Reviews on academic literature was carried out to understand about cyber threats that are prevalent among students in the tertiary education and what can these students do to address such threats.

2.1. Cyber safety and security

The definitions of cyber safety and cyber security are being defined in our earlier works in Abdul Molok et al. (2023), Abdul Molok, Zulkifli & Wahiddin (2022) and Abdul Molok & Zulkifli (2021). Similarly, in this study, cyber safety and security comprised of two distinct terminologies: cyber safety and cyber security. Although sometimes cyber safety is being used interchangeably with cyber security, it has actually a different definition to the latter. Cyber safety is defined as the protection of people's privacy, physical, mental and emotional wellbeing, through safe and responsible use of Information and Communication Technology. Cyber security refers to the protection of ICT infrastructure which includes data/information, hardware, software, and networks in order to preserve the confidentiality, integrity and availability of information and information processing facilities. The subsections below present the threats coming from both cyber safety and security.

2.2. Cyber threats

Acknowledging the Internet User Survey results by MCMC (2022), this study focuses on cyber threats that are related to the top users of the Internet in Malaysia which are tertiary education students, particularly university students in Malaysia. As mentioned in the Introduction section, Fatokun et al. (2019) cover the following cyber issues among university students: being unfamiliar with cyber threats, password sharing and phishing (sending fraud messages claiming from reputable organizations to induce individuals to reveal personal information and security credentials). Shaikh et al. (2020) assert cyberbullying, exposure to sexual and violent content, creating or disseminating fake content, and expressing political opinions and religious extremism online. On the other hand, Zhou and Xing (2021) cover online gaming addiction as a problematic concern among college students, while United Nations list cyberbullying, sexual exploitation and abuse, and human trafficking as the risks of the Internet for young people (United Nations, 2023). Another threat worth mentioning and it is becoming more rampant among Malaysian university students are online scams (Muniandy et al., 2017; New Straits Times, 2022a; New Straits Times, 2022b; The Sun, 2019). Muniandy et al. (2017) posit security threats that are common among university students as online scams, phishing, social engineering, malware and weak password usage.

The following cyber threats are in line with the above academic literature couple with top threats that we found in our study:

2.2.1. Gaming Addiction

The Internet has transformed traditional physical and board games to online games which involve massive, multiplayer, online role-playing games (MMORPG), first-person shooter (FPS), real-time strategy (RTS) games, and Multiplayer Online Battle Arena (MOBA) (Li, Zhang, Wu, Zhou, Dong & Zhang, 2023). There are positive effects on players such as increasing users' scores in mathematics and science (Abdul Molok & Zulkifli, 2021) and for psychological and interpersonal relationships growth, to reduce depression and stress, promoting academic performance, and enhance mental skills (Li et al., 2023). However, uncontrolled use of online games may expose users to pornographic content and conversation (sexting), the risk of cyberbullying, increase aggression and reduce prosocial behavior, hearing impairment, neck and back pain, repetitive stress injury, vision problem and technostress (Abdul Molok & Zulkifli, 2021 & Li et al., 2023). In addition to these effects, Zakaria & Adnan (2022) state the effects of mobile gaming addiction to youth's physical health are it causes abnormal body posture, obesity, visual impairment, migraines, and musculoskeletal pain and discomfort. They also include that mobile gaming among youth disturbs sleep quality, affects relationships, causes uncontrolled spending, promotes anti-social behavior and lack of interpersonal experience (Zakaria & Adnan, 2022). The top mental health issues are depression, Internet addiction, anxiety, impulsiveness, and attention-deficit hyperactivity disorder (Darvesh et al., 2020). Due to these effects of uncontrolled online gaming behavior to physical and mental health, the World Health Organization (WHO) has declared internet gaming disorder as an official medical condition (WHO, 2023).

This study does not prohibit online gaming since there are positive impacts to users when they play these games but it actually aims to promote the safe use and self-control in online gaming. If the user, especially among the university students, are aware of both positive and negative impacts of online games and they can implement self-regulation while playing these games, the impacts to cyber safety and security can be minimized.

2.2.2. Cyberbullying

Cyberbullying refers to "the use of ICT to support deliberate, repeated, and hostile behavior by an individual or group that is intended to harm or defame others" or in simpler term, "an electronic form of peer harassment" (Shaikh et al., 2020, p. 148032). According to Shaikh et al. (2020), cyberbullying is more dominant in literature that focuses on school children and most literature overlooks cyberbullying issues faced by university students. This study agrees with Shaikh et al. (2020) since United Nations Children's Fund (UNICEF) report that "Malaysia ranks second in Asia in 2020 for cyberbullying among youths" (The Star, 2022, p.1). In accordance to United Nations' definition, youth refer to "persons between 15 to 24 years" (United Nations, 2023), in which the common age range of university students is between 18 to 24 years. Similar to Zhou and Xing (2021)'s statement about lack of care and attention by family members influence online gaming addiction, The Star (2022) also reports that cyberbullying perpetrators experienced loneliness and lack of affection by family members.

Online chat groups are common platforms for cyberbullying which can influence the victim's mental health (The Star, 2023). It further reveals that a victim who was cyberbullied since her college years is still traumatic about body shaming and racial

slurs coming from a chat group of course mates. Surprisingly, it reports that bullies may not even realize that they are hurting one's feelings and not aware that their online posts may have impacts on victims. However, some bullies do have the intentions to hurt or humiliate the victim.

This study posits that university students need to understand about cyberbullying and the impacts of it to others. A comment may be funny to some students, but it can also be devastating to others.

2.2.3. Online Scams

Online scams is a type of cybercrime that uses misleading or fraudulent strategies through the Internet to deceive victims out of money or property. Some examples of online scams are phishing, phone scams or Macau scams, love scams, sales scams, investment scams, fake loans and SMS scams (New Straits Times, 2022b). It is reported that scammers target youth, especially university students who are seen as victims with low awareness on cybercrime (Muniandy et al., 2017; New Straits Times, 2022a, 2022b, The Sun; 2019). New Straits Times (2022a, 2022b) and The Sun (2019) report that the syndicates behind these fraudulent activities are using and targeting youth especially university students to be their account mules. Mule accounts are "bank accounts that the owners allow others to control by handing over their bank card's pin numbers or the online banking password. Criminals use these accounts to receive money from their scams" (New Straits Times, 2022a, p.1). Account holders are being offered up to RM900 per day or to RM3000 per month to "rent out" their accounts which are being used by scammers to launder illegal funds.

This study suggests that university students need to be aware that renting out their bank accounts is an offense and their accounts will be frozen or closed. Further, their names will be blacklisted from opening other bank accounts which will result to difficulty in finding jobs since Ministry of Human Resources requires salary payments via bank accounts as mandated by Employment Act (CentralHR, 2023).

3. REVIEW OF EXISTING APPLICATIONS

This study aims to empower tertiary education students to be vigilant about cyber threats that can happen to them and their peers, how to address these threats and to assess their knowledge, through a digital storytelling application. Review of existing system applications that are similar to this aim was done to study important features that can be adopted and adapted in our application. Five existing applications that have similar purposes to this study were chosen, and the summary of each application is as follows:

3.1. Targeted Attack: The Game

This educational game application was developed by Trendmicro which illustrates the reality of a cyber targeted attack on a commercial organization. It tests the user ability to make the right choices, keep the project on time and on budget, and protect the organization from an attack. It also contains assessment and a story plot (Trendmicro, 2015).

3.2. Cybersecurity Lab

Similar to the above, Cybersecurity Lab is an educational games developed by Nova Labs. User of the game will defend a company that is targeted by

sophisticated cyber attacks by strengthening cyber defences by completing a series of cyber challenges (Nova Labs, 2023).

3.3. Cybersecurity Trivia Twirl

This educational game was developed by Center for Development of Security Excellence (CSDE), Defense Counterintelligence and Security Agency of the U.S. When a user clicks on the spin wheel button, a category will be chosen and questions about that category will be asked in that category, for e.g. Password. If the answer is wrong, the user will be provided with the right answer. The score of the quiz can be shared on social media (CSDE, n.d.).

3.4. The Missing Link

This is also an education game that was developed by Division of Information Technology, Texas A&M University. The game tests the user's knowledge on cybersecurity and teach useful teach for staying safe online (Texas, n.d.).

3.5. Cyber Generation

This is the only digital storytelling application about cybersecurity that could be found. It was developed by Bachelor of Information Technology students in 2021. The application educates children about cyber safety and security. It consists of videos, animation and audio and contains 6 modules about cyber threats to children and what can children do about the threats. It also contains quizzes to test the user's knowledge after watching each module (Tuan Abdullah, 2021).

Table 1: Comparison of Existing Applications

App	Assessment	Interactive Design	Story Plots	Background Music
Targeted Attack: The Game	✓	×	✓	×
Cybersecurity Lab	✓	×	✓	×
Cybersecurity Trivia Twirl	✓	×	×	×
The Missing Link	✓	✓	×	×
Cyber Generation	✓	✓	✓	✓

Table 1 compares these five existing applications in terms of assessments that are provided to users, interactive design, story plots and background music. Out of five applications, only Cybersecurity Trivia Twirl is suitable for our target users which are tertiary education students. Among these applications, only Cyber Generation is a digital storytelling application, therefore its features would be adopted and adapted, suitable to the target users. Nevertheless, features such as providing assessments or quizzes, interactive design, story plots and background music will be adopted in our digital storytelling application, called SmartCTzen.

4. METHODOLOGY

4.1. User Requirements

In order to understand the actual cyber threats that tertiary education students are currently facing, an online survey which consists of 15 questions, using a Google form was carried out. 105 university students in Malaysia between 18-25 years responded to the survey. The survey was meant to understand their demographics, how they used the Internet, the types of cyber threats that they experienced, their security practices and what kind of features that they wished to see in a digital storytelling application.

4.2. Digital Storytelling Design and Production

This study follows the definition of digital storytelling as "one of the innovative pedagogical approaches that can engage students in deep and meaningful learning… the use of multimedia tools including graphics, audio, video, and animation to tell a story" (Smeda Dakich & Sharda, 2014, p.1). The development of the application started with the story plots of different types of cyber threats. Each story consists of the details of each cyber threat, how to recognize the threat and what are the controls to be implemented to address the threat. The controls include cyber safety and security controls coming from credible sources such as Cybersecurity Malaysia, as well as controls from the Islamic perspectives. Islam is the religion of peace, therefore, as a Muslim, the believers must be aware that no harm can be done to anyone, whether physically or mentally, face-to-face or online. Each story serves as one lesson, for each type of cyber threat and its controls, or ways to combat it.

After the story plot for each threat are designed, the main and supporting characters of the stories were designed. Our main characters are a male student and a female student, and the supporting characters are the hackers or cybercriminals.

Next, the storyboard for each cyber threat was developed. The storyboards include narratives and drawings of each scene which were based on the review of literature and existing similar applications, as well as our findings from the survey.

The final module of our digital storytelling is an assessment module to test the understanding of the user after they have watched the story for each cyber threat in terms of quiz questions.

The influence of storytelling as a tool used in pedagogy (the method and practice of teaching) is widely used since the beginning of humanity, and then digital storytelling became popular during the e-learning era (Smeda et al., 2014). Hence, we believe that through interactive stories, driven by quality audio, videos and graphics, university students can learn about cyber safety and security better since they can do this at their own time, and educators can use our digital storytelling application to teach in class.

5. FINDINGS

As mentioned in the methodology section, a survey was conducted to understand about the respondents' demographics, how they used the Internet, actual cyber threats that university students had experienced, their security practices and what kind of features that they wished to see a digital storytelling application that can be used by them to learn about cyber safety and security.

5.1. Demographics

The survey was conducted online, using Google form and it was distributed to university students mainly at the International Islamic University Malaysia (IIUM) but we asked them to distribute the survey to their friends from other universities. We managed to get 105 respondents with age range from 18 to 25 years coming from IIUM (62%), MARA University of Technology (UiTM - 9.5%), National University of Malaysia (UKM – 3.8%), Putra University of Malaysia (UPM – 3%), Tun Hussein Onn University of Malaysia (UTHM – 2%), University of Malaysia (UM – 2%), Islamic Science University Malaysia (USIM - 1%), Northern University of Malaysia (UUM – 1%), UniKL (1%), UNITEN (1%), MMU (1%), UNITAR (1%), Polytechnics (2%), University of Technology Malaysia (UTM – 1%) and Others (not specified - 9.5%).

5.2. Internet Use

Majority of the respondents were using smartphones (96.2%) and laptops (96.2%) to use the Internet. 34.3% of them were using tablets and iPads. In term of social media, majority were Whatsapp users (98.1%), followed by Telegram (93.2%), Instagram (90.3%), TikTok (69%) and Twitter (69%). More than half of the respondents use social media for more than 5 hours per day (62.1%).

5.3. Security Behavior

When asked about disclosure of any personal information about themselves, it was found that most of the respondents admitted they shared personal information online. The top three types of information they shared were photos (71.8%), email addresses (59.2%), and real names (56.3%). 83.8% of respondents had never posted bad comments on social media about friends or strangers, and 16.2% admitted that they had. It is a relief to know that 92.2% of university students installed anti-malware (malicious software) solutions on their laptops, however only 21.4% installed anti-malware on their smartphones. 54.3% of them enabled personal firewall and kept their anti-malware up-to-date, but 39% were unsure whether they should. Fortunately, most of them did not divulge their password to anyone, although 47.6% admitted to using the same password across multiple user accounts. Furthermore, 44.8% scanned for malware when downloading a file or opening an email attachment.

5.4. Cyber Threats

In terms of cyberbullying, 14.3% of the university students confessed that they had been a victim of cyberbullying, however, 81.6% would tell others if they had been cyberbullied. Interestingly, 43.7% admitted that they had gaming addiction, 41.7% had experienced depression or anxiety due to Internet use, and 23.3% experienced online sexual harassment.

6. SMART CTZEN

While existing studies in cyber safety and security focus more on school students, this study focuses on tertiary education students since they are the top Internet users in Malaysia and studies show that these types of students are most vulnerable to cyber threats and attacks.

Based on literature review, reviews of existing similar applications, findings from our survey on 105 university students as shown above, this study recommends the use of digital storytelling application to educate tertiary education students about

top cyber threats and how to address them using the concept of edutainment (education-entertainment). Our digital storytelling application is called Smart Ctzen, targeted to. We used the word "smart" since it relates to a person's capacity to think intelligently in difficult situations (Cambridge Dictionary, 2023). The term "CTzen" is derived from the term "digital citizen" which means someone who is skilled in using the internet in order to communicate with others, …and who understands how to do this in a safe and responsible way" (Cambridge Dictionary, 2023, p.1).

The objectives of the project are:

- To develop a digital storytelling application for university students to understand about cyber safety and security
- To promote cyber ethics, safety and security among university students
- To promote self-empowerment among university students in cyber safety and security and at the same time be able to empower their peers.

The navigational flow of the application is shown in Fig.1 below which includes the main menu (homepage), introduction to Smart Ctzen, Stories or Lessons, and Quiz questions with the right answers and conclusions.

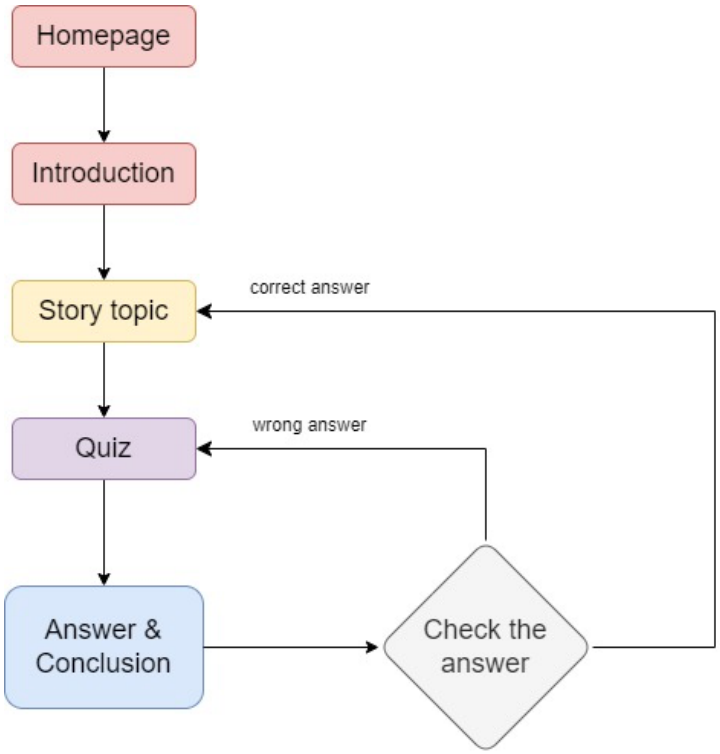

Fig. 1. Smart Ctzen Navigational Flow

In the content production process, characters and backgrounds were drawn using Adobe Illustrator and Photoshop. After this process, developers used Adobe After Effects to make videos, and the platform to publish the final product was Unity. In a nutshell, it includes video animation, voiceover, and quiz questions for each lesson. Fig.2 shows the screenshot of the main menu or homepage of the application.

Fig. 2. Smart Ctzen Navigational Flow

The stories of lessons in the Smart Ctzen application are cyberbullying, gaming addiction, online scams, phishing, online sexual harassment and password management. Password management was included as the final lesson because based on our research and of others, university students have issues in managing passwords, for example, using the same passwords for all accounts and share password with others. The screenshot of the lessons is shown in Fig.3:

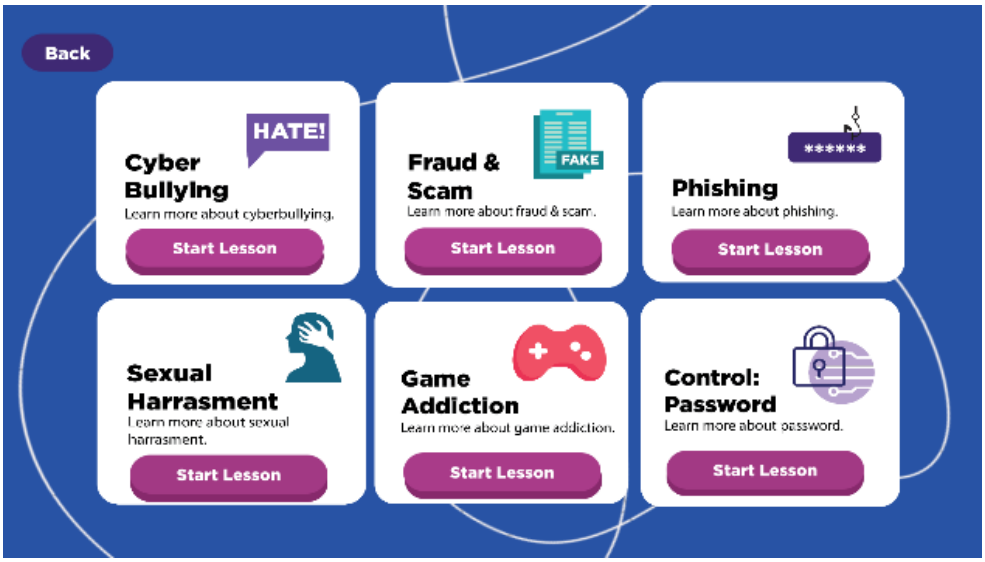

Fig. 3. Lessons in Smart Ctzen digital storytelling application

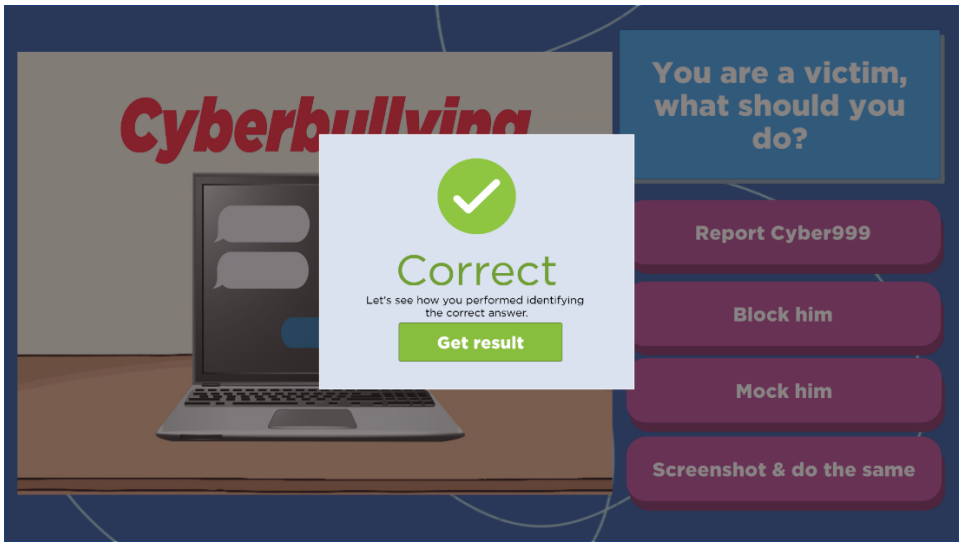

Fig. 4. Example of a quiz question with the right answer

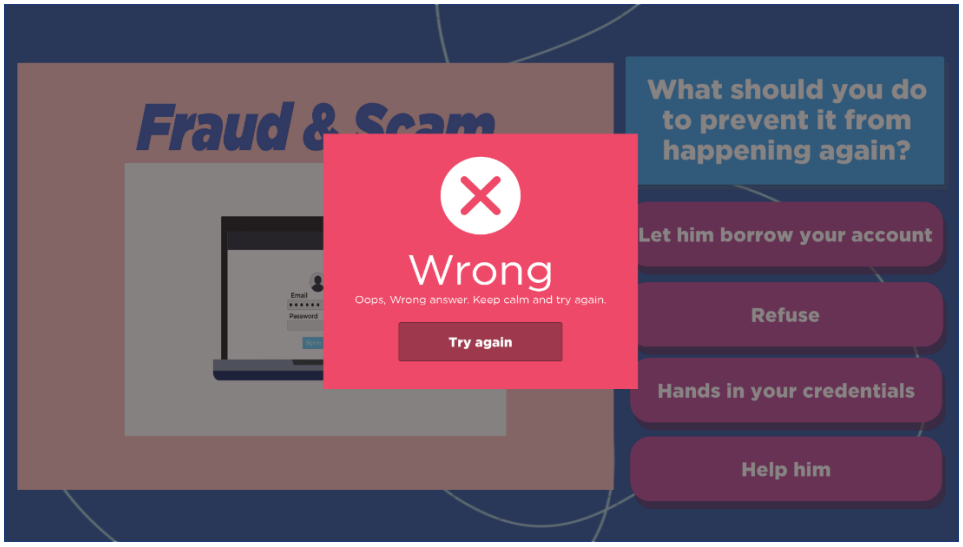

Fig. 5. Example of a quiz question with the wrong answer

Due to the limitation of the pages of this article, not all lessons and features of Smart CTzen are provided with the screenshots. Each lesson is presented using video animation and original voiceover of one of the developers. It is imperative to note that, the developed application provide different types of stories or lessons that were presented based on findings from the literature review (as shown in Section 2), review of existing applications (Section 3) and findings from the survey of 105 respondents (Section 5).

7. CONCLUSION

This study covers the research and development in the area of cyber safety and security. It includes the academic contributions in terms of fulfilling the gap of limited studies on cyber threats to tertiary education students as most studies cover primary and secondary school students. It presents the top cyber threats to university students based on literature and our own survey on 105 students from

numerous universities in Malaysia and incorporate these threats into stories or lessons in our digital storytelling application called Smart CTzen. This application does not only include the lessons about the cyber threats but also include how targeted users can address these threats. It is proposed to be a self-empowerment tool for tertiary educations students to empower themselves and their peers to combat today threats in the interconnected world. It is hoped that with this application, the number of students who become a victim will be minimized and at the same time reduce the cases of students who become the perpetrator of cyber threats, attacks and crimes.

ACKNOWLEDGEMENT

This study is based on Final Year Project (FYP) under the multimedia category for the Bachelor of Information Technology program, Faculty of ICT, International Islamic University Malaysia.

REFERENCES

Abdul Rahman, N. S., Sahabudin, N. A., Eh Phon, D. N., Ab Razak, M. F. & Mat Raffei, A. F. (2023), Factors affecting cyberbullying behaviours among university students: A review, *IEEE 8th International Conference On Software Engineering and Computer Systems (ICSECS)*, Penang, Malaysia, 342-346, doi: 10.1109/ICSECS58457.2023.10256292.

Abdul Molok, N.N. & Zulkifli, Z. (2021). Parents' roles in mitigating cyber threats to children in the new norm. Persidangan Kependudukan Kebangsaan (PERKKS 21).

Abdul Molok, N.N., Zulkifli, Z. & Wahiddin, M.R. (2022). Pendekar Siber: Empowering young people to combat cyber threats. International Conference on Cyber Resilience (ICCR), Dubai, United Arab Emirates, 2022, pp. 01-04, doi: 10.1109/ICCR56254.2022.9995935.

Abdul Molok, N.N., Abdul Hakim N.A. & Jamaludin, N.S. (2023). SmartParents: Empowering parents to protect children from cyber threats. International Journal on Perceptive and Cognitive Computing (IJPCC), 9(2), 73-79.

Cambridge Dictionary (2023). Smart. Retrieved from https://dictionary.cambridge.org/dictionary/english/smart

CentralHR (2023). Pay Employee Salaries Via Bank Accounts: MOHR. Retrieved from https://www.centralhr.my/payment-of-wages-malaysia/

CSDE (Center for Development of Security Excellence). n.d. Cybersecurity trivia twirl. Retrieved from https://securityawareness.usalearning.gov/cdse/multimedia/games/cybertrivia/index.html#

Darvesh, N. Radhakrishnan, A., Lachance, C.C., Nincic, V., Sharpe, J.P., Ghassemi, M., Straus, S.E., & Tricco, A.C. (2020). Exploring the prevalence of gaming disorder and Internet gaming disorder: A rapid scoping review. Systematic Reviews, 9(68). https://doi.org/10.1186/s13643-020-01329-2

Li, F., Zhang, D., Wu, S., Zhou, R., Dong, C. & Zhang, J. (2023). Positive effects of online games on the growth of college students: A qualitative study from China. Frontiers in Psychology 14:1008211, 1-10. doi: 10.3389/fpsyg.2023.1008211

MCMC (Malaysian Communications and Multimedia Commission). 2022. Internet User Survey. Retrieved from https://www.mcmc.gov.my/skmmgovmy/media/General/IUS-2022.pdf

Muniandy, L., Muniandy, B. & Samsudin, Z. (2017). Cyber security behaviour among higher education students in Malaysia. Journal of Information Assurance & Cyber security, 2017, 1-13. doi: 10.5171/2017.800299

New Straits Times. (2022a). Update laws to fight cyber criminals, government urged. Business Times. Retrieved from https://www.nst.com.my/news/crime-courts/2022/08/825848/update-laws-fight-cyber-criminals-government-urged

New Straits Times. (2022b). Online scam cases increasing in Malaysia. Business Times. Retrieved from https://www.nst.com.my/news/nation/2022/09/834531/online-scam-cases-increasing-malaysia

Nova Labs. (2023). Cybersecurity Lab. Retrieved from https://www.pbs.org/wgbh/nova/labs/lab/cyber/

Smeda, N., Dakich, E. & Sharda, N. The effectiveness of digital storytelling in the classrooms: a comprehensive study. Smart Learn. Environ. 1, 6 (2014). https://doi.org/10.1186/s40561-014-0006-3

The Star. (2022). Malaysia is 2nd in Asia for youth cyberbullying. Retrieved from https://www.thestar.com.my/news/nation/2022/01/14/malaysia-is-2nd-in-asia-for-youth-cyberbullying

The Star. (2023). Cyberbullying leaves mental scars that never go away. Retrieved from https://www.thestar.com.my/metro/metro-news/2023/07/01/cyberbullying-leaves-mental-scars-that-never-go-away

The Sun. (2019). Macau Scams target IPT students to provide 'mule account'. Retrieved from https://www.thesundaily.my/local/macau-scam-targets-ipts-students-to-provide-mule-accounts-LN681519

Trendmicro (2015). Targeted Attack: The Game. Retrieved from http://targetedattacks.trendmicro.com/about-the-game.html

Texas A&M University (n.d.) The missing link. Retrieved from https://it.tamu.edu/missinglink/about/#howtoplay

Tuan Abdullah, T.A.B. (2021). Cyber Generation: A digital storytelling of digital citizenship for children. Retrieved from https://www.youtube.com/watch?v=8-qB4D86FTo

United Nations. (2023). Global Issues: Youth. Retrieved from https://www.un.org/en/global-issues/youth

WHO (World Health Organization). (2023). Gaming Disorder. Retrieved from https://www.who.int/standards/classifications/frequently-asked-questions/gaming-disorder

Zakaria, A.S. & Adnan, W.H. (2022). Youth Awareness: A Survey on Mobile Gaming Addiction Concerning Physical Health Performance on Young Adults in Malaysia. Journal of Media and Information Warfare, 15(1), 85-98.

Zhou, X.H. and Xing, J. (2021). The Relationship between College Students' Online Game Addiction, Family Function and Self-Control. Health, 13, 910-919. https://doi.org/10.4236/health.2021.139070

Zulkifli, Z., Abdul Molok, N.N., Abdul Rahim, N.H. & Talib, S. (2020). Cyber security awareness among secondary schools in Malaysia. Journal of Information Systems and Digital Technologies, 2(2), 28-41.