International Journal of Data Science and Advanced Analytics (ISSN: 2563-4429)

Mobile Application for Cybersecurity Education and Awareness since COVID-19 Pandemic

Tang Shi Yin[1], Dr. Intan Farahana Kamsin[2], Zety Marlia Zainal Abidin[3], Hemalata Vasudavan[4]

[1'2]Asia Pacific University of Technology and Innovation, Technology Park Malaysia, Bukit Jalil, Kuala Lumpur, Malaysia.

[1]tp062489@mail.apu.edu.my, [2]intan.farahana@staffemail.apu.edu.my, [3]zety@staffemail.apu.edu.my, [4]hemalata@staffemail.apu.edu.my

***Abstract* – Many schools, businesses and even governments have shifted to digital platforms and digital solutions since the COVID-19 pandemic. However, public awareness of cybersecurity and cyberattacks remains low. As the public rapidly instals remote systems and networks to enable online learning and remote working, cybercriminals are utilising a rising number of security breaches to steal data and make profits. In this paper, an effective method is proposed to educate users in the field of cybersecurity through mobile applications for their benefits. This study will adopt the stratified sampling method, and quantitative research of questionnaire will be the data collection method. The public will be the target user, with 120 respondents involve. In conclusion, this research paper would examine how to benefits users with knowledges about cybersecurity through mobile applications. The future recommendation for this proposed system is to provide an interface for users to ask questions and discuss their troubles with cybersecurity experts.**

***Index Terms* – COVID-19, Cyberattack, Cybersecurity Education, Mobile Application**

1. Introduction

Coronavirus disease 2019 (COVID-19) is an airborne contagious disease that has afflicted millions of people worldwide and continues to claim thousands of lives every day [19]. With regard to the COVID-19 pandemic's infectious impact, economies are starting to implement various actions to reduce infections due to national lockdowns with restrict movement and inactivating economic activity to those who provide important services [16]. Therefore, the use of online technologies such as cloud computing, Internet of Things (IoT), high-speed data networks, and software applications has greatly expanded. Many people and businesses rely on technology to continue their lives and businesses [10]. Businesses are speeding up their digital transformations, and cybersecurity has become a big problem. The use of technology brings more problems and threats in cybersecurity. Organizations will have to deal with increasing security demands as the likelihood of cyberattacks rises [6]. The increase and growth of cyberattacks shows a lack of awareness. Therefore, it is necessary to be aware of these cyberattacks and privacy concerns that can lead to negative outcomes in order to prevent or avoid them.

This proposed solution is a new perspective and approach that can help educate people on cybersecurity through the use of mobile applications. This will increase awareness of cyberattacks while getting the latest information on cyber security. This study explains research into mobile applications that can collect cybersecurity information and then provide that information to users, and even provide them with training. Therefore, it is more convenient, time-saving and useful for the users.

2. Literature Review

2.1 Domain

2.1.1 Cybersecurity education and cyberattack awareness

The practise of securing digital devices and data is known as cybersecurity. According to Cybersecurity and Infrastructure Security Agency, cybersecurity is defined as the art of protecting data, devices, and networks against unauthorised access, as well as the practise of assuring information confidentiality and integrity [3]. It provides understanding on how to secure digital assets from attacks and how devices interact in the digital age [4]. Many protections, such as firewalls, access controls, and antivirus can be used to secure resources, but the human factor is always present in cybersecurity. Most cyberattacks and threats are carried out due to human behaviours and attitudes. The increase in remote working and learning requires greater attention to cybersecurity due to greater cyber risks [2]. A SonicWall report found that the rate of cyberattacks has risen by 232% in 2021 since 2019 [17] and Google blocks around 100 million phishing emails every day [9]. Not only that, the pandemic has provided opportunities for cybercriminals to carry out ransomware attacks, DoS attack, malware and more. According to a global study of IT security specialists, data exfiltration and leakage have accounted for the majority of cyberattacks since the COVID-19 epidemic. Phishing emails are also becoming more common and following by takeover of account as in Figure 1.

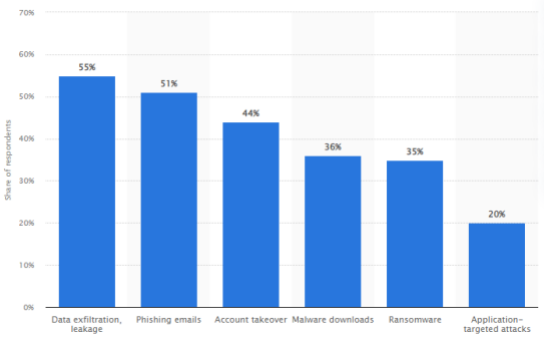

Figure 1: Types of Cyberattack against Number of Victims [18]

Although cybersecurity is one of the most serious focus points facing organizations today, public awareness and understanding on it are still low. Despite the fact that nearly most of the people has heard about cybersecurity, people's behaviours do not reflect their awareness. Cyberattacks on assets can be caused by a lack of cybersecurity understanding and a disregard for recommended procedures [2]. Based on Cybersecurity and Infrastructure Security Agency, it is found that cybersecurity is critical since it protects all types of data. Therefore, in this research, cybersecurity education and public awareness of cyberattacks will be focused.

2.1.2 Mobile application

A mobile application, usually referred to as an app, is software that runs on mobile devices. Mobile applications are regularly used to offer services that are comparable to those available on a computer. These applications behave similarly to small software with limited capability in order to deliver the greatest user experience and services. According to an eMarketer report, the amount of time spent on mobile applications on devices has climbed dramatically in recent years. While, the amount of time spent on mobile devices using the browser was not significantly different as shown in Figure 2.

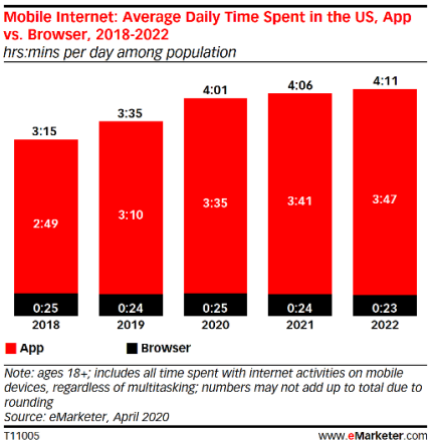

Figure 2: Average Daily Time Spent on Apps VS Browser [20]

The pandemic of COVID-19 has altered how people connect, conduct business, and consume media. However, as individuals utilise their phones for many purposes, the mobile app business has seen significant growth. In the third quarter of 2020, Google Play witnessed 28.3 billion new application instals, up 31% from 21.6 billion at the same time of 2019 can be seen in Figure 3.

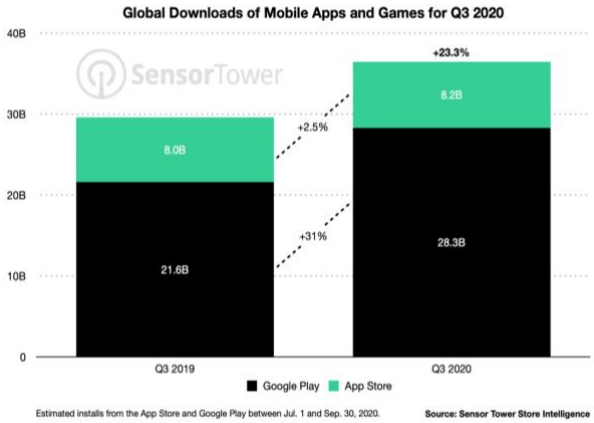

Figure 3: Global Downloads of Mobile Apps and Games [15]

The social platforms shown in Figures 4 and 5 can greatly influence the public due to large number of users [15]. When it comes to global events like cybersecurity, mobile applications seem to play a critical role in spreading global or local awareness. Therefore, in this research, the use of mobile applications created for the public will be the proposed solution.

Figure 4: TikTok

Figure 5: Facebook

2.1.3 Cybersecurity education and awareness on mobile applications

The internet is no longer a remote medium since it has gotten integrated into our daily lives. Many of these opportunities are available through game-based learning. For example, gradually improve skills by immersing individuals in real-life simulations. It is more enjoyable and learnable through play than it is through theory or other sources. Games with a purpose other than pure amusement are referred to as game-based cybersecurity education. It allows people to practise in a secure and enjoyable environment and thus, develop their cybersecurity skills and

prevent cyberattack [5]. Not only that, students also able to practice their cybersecurity skills and learn about cybersecurity education through the game-based cybersecurity learning mobile applications as shown in Figure 6.

Figure 6: Cybersecurity Learning Game-Based Application [7]

Besides, there is also cybersecurity learning mobile application with theory and latest information. However, there are not many journals articles on cybersecurity education covering both practical and theoretical aspects. Therefore, it can be concluded that an effective method to increase knowledge and awareness in a practical and theoretical way of cybersecurity through mobile applications should be created as proposed in this research.

2.2 Similar System

2.2.1 Learn Cybersecurity

Learn Cybersecurity is a mobile application that provides knowledge in the field of cybersecurity. The application includes explanations of security concepts, quizzes, technical questions, and latest information features. Users will be able to gain knowledge about cybersecurity in a theoretical way. However, the "entertainment" section is not for users to practice, but it is a suggestion of movies related to cybersecurity knowledge.

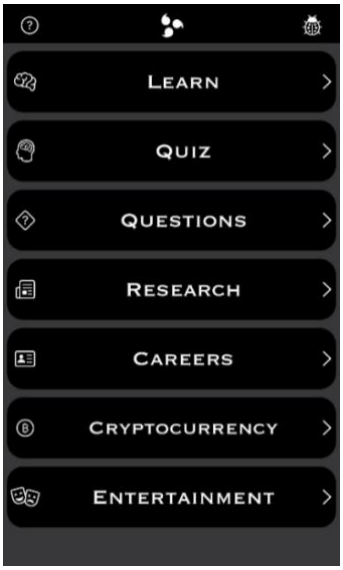

Figure 7: Learn Cybersecurity Functions

2.2.2 The Defence Works

The Defence Works is a game-based cybersecurity learning application. Through the app, users can virtually experience a scenario as such in Figure 8 and choose the solution. When the user chooses correctly, they will get scores. As shown in Figure 9, the higher the score, the higher the level of users.

Figure 8: The Defence Works Scenario

Figure 9: The Defence Works Level

2.3 Comparison Table

Similar Systems / Features/Components	Learn Cybersecurity	The Defence Works
Cybersecurity Education	✓	✓
Cyberattack Awareness	✓	✓
Quizzes	✓	✗
Latest news/information	✓	✗
Workshops details	✓	✗
Training/Entertainment	✗	✓
Mobile Application	Smartphones	Smartphones
Costs	Free	Free

Table 1: Similar System Comparison Table

Table 1 shows systems with similar characteristics and components to the system proposed in this research. Features considered are cybersecurity education, awareness, practical skills, quizzes and workshops. Furthermore, it must also be a mobile application and users can download it for free.

2.4 Conclusion

In short, not all similar systems above have the features mentioned in Table 1. Therefore, a mobile application will be created to allow users to get more information. Despite the fact that several applications have been developed to solve these issues, there are still gaps. Most applications do not have both theoretical and practical components, instead, they only have one, either theoretical or practical component. The system will need to have the features to educate and aware users with cybersecurity concepts, even provide the user with practical trainings. Therefore, study on another approach to educate users with the help of mobile applications to increase their level of understanding and awareness on cybersecurity would be highly beneficial to the public.

3. Problem Statement

For a long time, awareness of cybersecurity among people including organizations was very low [13]. During the COVID-19 pandemic, the ranks of Internet users have grown rapidly. Not only students using the internet and mobile technology for online learning [1], but employees are also similarly mandated to practice working remotely using modern technologies too [11]. The COVID-19 pandemic has boosted the speed of digitization, resulting in new highs in cybercrime and a significant rise in cyberattacks [12]. Cyberattacks such as malware, DDoS attacks and malicious websites threaten general public physically and mentally [8]. There are many applications for the public to learn cybersecurity techniques and skills, and there are even game-based apps. However, these applications are more inclined to allow the public to learn in practical ways, rather than knowledge-based ones, such as explanations and illustrations. Not only that, but the applications also lack with the latest news about cyberattacks [14]. Throughout the pandemic, despite the resources available, insufficient attention has been paid to cybersecurity and cyberattacks. As a result, researching another approach of providing cybersecurity education and awareness through mobile applications will be beneficial to the general population.

4. Aim and Objectives

Aim:

This research aims to raise awareness of cyberattacks and provide cybersecurity education through mobile applications since the COVID-19 pandemic.

Objectives:

i. To support users with cybersecurity education
ii. To collect information on the latest cyberattacks
iii. To provide updates on cybersecurity trends or notifications of any cybersecurity-related workshops

5. Research Significance

The findings of this research will severally contribute to the cybersecurity knowledge of public through mobile application. Users not only be able to practically learn the techniques and skills, but they can also access to the cybersecurity education, and even obtain the latest trends and incidents happened about cyberattacks daily. Armed with this information, they can understand the modus operandi of cybercriminals thereby protect themselves and their assets from cybercriminals. Besides, this study will provide researchers with some insight into the potential of using mobile application to help increase the cybersecurity education and awareness among public. Thus, a mobile application with these functionalities can benefit the application's users.

6. Research Methodology

6.1 Target users

The target users in this research paper are general public. Regardless of gender or age, the public will be involved as everyone should be aware of cybersecurity.

6.2 Sampling method

The sampling method will be stratified sampling. The public is divided into several different subgroups or known as strata based on their characteristics such as gender and age group. The male will be divided into each age group from the 10th to the 40th generation, the same will be divided for the female. Each stratum will select 15 respondents to participate in the questionnaire. A total of 120 respondents were involved, including 60 male respondents and 60 female respondents.

6.3 Data collection method

To effectively carry out this research paper, a quantitative approach has been conducted to determine the usefulness of mobile applications in the field of cybersecurity. It will involve a short survey that include cybersecurity related questions such as the public's own level of understanding of cybersecurity and their awareness on cyberattacks. This paper chooses questionnaire as the survey method because the number of confirmed cases in the pandemic is still above a certain level. Therefore, online meetings or face-to-face interviews are still difficult to be held. As a result, using a quantitative approach, it is preferable to utilise a questionnaire as it saves more time and is easier to disseminate among the population. In the questionnaire, it will consist of 6 multiple choice questions and 4 Likert scales ranging from 1 to 5 questions. In order to conduct the research more efficiently, Google Forms will be used as the platform for the questionnaire, and the URL link will be spread to the public through any platform. The

questionnaire will be clearly remarks in the Google Forms on no participant's details will be collected as it is confidential. A conclusion can be drawn from the results of questionnaire to summarize the level of cybersecurity education of public. In the end, the effectiveness of proposed solution can be determined from the data collected.

7. Overview of Proposed System

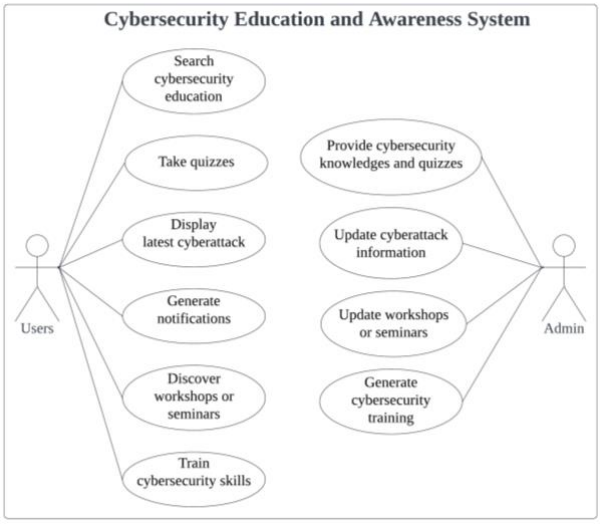

Figure 10: Use case diagram of the Cybersecurity Education and Awareness System

Figure 10 shows the use case diagram for the Cybersecurity Education and Awareness System. In this system, users can search for cybersecurity education. They will be able to gain knowledge about attacks, including how it happens, and through what techniques it happens, etc. After users have mastered this knowledge, they can test their understanding of the topic with a quiz provided. If the user answers some of the questions incorrectly, the correct answers and explanations will be given. Admins are responsible for providing education, including knowledge and quizzes.

Next, users will be able to keep up to date with the latest news and trends in cyberattacks. Only any cyberattack incidents officially announced by the organization will be processed and released by the admin in a timely manner so that users do not receive incorrect information. By understanding the latest trends in cyberattacks, they will understand the modus operandi of cybercriminals to protect their assets from attack. Not only that, but users can set up to get notified via their mobile devices if any latest news is released.

Moreover, users can discover and participate in any workshop or seminar in the field of cybersecurity through this system. The administrator will be in charge of keeping the details of workshops or seminars up to date. Lastly, users can practical their cybersecurity skills to avoid being attacked by cybercriminals, as admins will generate training for them.

8. Conclusion

By implementing the mobile application, the system can provide users with useful cybersecurity information. Users have been educated through the information, quizzes, latest news, and training provided in the applications. Thus, users can protect themselves from cybercriminals and avoid being attack from any method or technique as there is an increase in cyberattacks post COVID-19 pandemic. Therefore, the cybersecurity education will be slowly improved and cyberattack awareness will increase if the users utilise this mobile application.

References

[1] Adedoyin, O. B., & Soykan, E. (2020). Covid-19 pandemic and online learning: the challenges and opportunities. *Interactive Learning Environments*, 1–13. https://doi.org/10.1080/10494820.2020.1813180

[2] Chigada, J., & Madzinga, R. (2021). Cyberattacks and threats during COVID-19: A systematic literature review. *SA Journal of Information Management*, *23*(1). https://doi.org/10.4102/sajim.v23i1.1277

[3] CISA. (2019, November 14). *What is Cybersecurity? | CISA*. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/uscert/ncas/tips/ST04-001

[4] Hancock, M. (2021). The Influence of Cybersecurity on Modern Society. *The History, Development and Importance of Cybersecurity in a Modern World*. https://easychair.org/publications/preprint/PvXC

[5] Hendrix, M., Al-Sherbaz, A., & Bloom, V. (2016). Game Based Cyber Security Training: are Serious Games suitable for cyber security training? *International Journal of Serious Games*, *3*(1). https://doi.org/10.17083/ijsg.v3i1.107

[6] Humayun, M., Niazi, M., Jhanjhi, N., Alshayeb, M., & Mahmood, S. (2020). Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. *Arabian Journal for Science and Engineering*, *45*(4), 3171–3189. https://doi.org/10.1007/s13369-019-04319-2

[7] Jin, G., Tu, M., Kim, T. H., Heffron, J., & White, J. (2018). Evaluation of Game-Based Learning in Cybersecurity Education for High School Students. *Journal of Education and Learning (EduLearn)*, *12*(1), 150–158. https://doi.org/10.11591/edulearn.v12i1.7736

[8] Khan, N. A., Brohi, S. N., & Zaman, N. (2020). Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic. -. https://doi.org/10.36227/techrxiv.12278792

[9] Kumaran, N., & Lugani, S. (n.d.). *Protecting against cyber threats during COVID-19 and beyond*. Google Cloud Blog. https://cloud.google.com/blog/products/identity-

security/protecting-against-cyber-threats-during-covid-19-and-beyond

[10] McClain, C., Vogels, E. A., Perrin, A., Sechopoulos, S., & Rainie, L. (2022, April 28). *The Internet and the Pandemic*. Pew Research Center: Internet, Science & Tech. https://www.pewresearch.org/internet/2021/09/01/the-internet-and-the-pandemic/

[11] Nagel, L. (2020). The influence of the COVID-19 pandemic on the digital transformation of work. *International Journal of Sociology and Social Policy*, *40*(9/10), 861–875. https://doi.org/10.1108/ijssp-07-2020-0323

[12] Pranggono, B., & Arabo, A. (2020). COVID-19 pandemic cybersecurity issues. *Internet Technology Letters*, *4*(2). https://doi.org/10.1002/itl2.247

[13] Ponsard, C., Grandclaudon, J., & Bal, S. (2019). Survey and Lessons Learned on Raising SME Awareness about Cybersecurity. *Proceedings of the 5th International Conference on Information Systems Security and Privacy*. https://doi.org/10.5220/0007574305580563

[14] Roepke, R., & Schroeder, U. (2019). The Problem with Teaching Defence against the Dark Arts: A Review of Game-based Learning Applications and Serious Games for Cyber Security Education. *Proceedings of the 11th International Conference on Computer Supported Education*. https://doi.org/10.5220/0007706100580066

[15] Sensor Tower. (2020, October). *Global App Revenue Grew 32% Year-Over-Year in Q3 2020 to More than $29 Billion*. https://sensortower.com/blog/app-revenue-and-downloads-q3-2020

[16] Shrestha, A., Shrestha, U., Sharma, R., Bhattarai, S., Tran, H., & Rupakheti, M. (2020). Lockdown caused by COVID-19 pandemic. *Reduces Air Pollution in Cities Worldwide*. https://doi.org/10.31223/osf.io/edt4j

[17] SonicWall. (2022, February 16). *2022 SonicWall Cyber Threat Report | Threat Intelligence*. https://www.sonicwall.com/2022-cyber-threat-report/

[18] Statista. (2021, August 18). *Increases in cyber attacks according to IT professionals in 2021, by type*. https://www.statista.com/statistics/1258261/covid-19-increase-in-cyber-attacks/

[19] World Health Organization (WHO). (2020, January 31). *Statement on the second meeting of the International Health Regulations (2005) Emergency Committee regarding the outbreak of novel coronavirus (2019-nCoV)*. https://www.who.int/news/item/30-01-2020-statement-on-the-second-meeting-of-the-international-health-regulations-(2005)-emergency-committee-regarding-the-outbreak-of-novel-coronavirus-(2019-ncov)

[20] Wurmser, Y. (2020, July 9). *The Majority of Americans' Mobile Time Spent Takes Place in Apps*. Insider Intelligence. https://www.emarketer.com/content/the-majority-of-americans-mobile-time-spent-takes-place-in-apps