Vol. 4 Special Issue. 1
International Journal of Data Science and Advanced Analytics (ISSN: 2563-4429)

Cybersecurity Education Through Mobile Application to Prevent Cyber Attacks During Covid-19

Chan Xin Ying[1], Intan Farahana Binti Kamsin[2], Salmiah Amin[3], Nur Khairunnisha Zainal[4]
[1'2'3'4]Asia Pacific University of Technology and Innovation, Technology Park Malaysia, Bukit Jalil, Kuala Lumpur, Malaysia.
[1]chan-xy@hotmail.com, [2]intan.farahana@staffemail.apu.edu.my, [3]salmiah@staffemail.apu.edu.my, [4]khairunnisha.zainal@staffemail.apu.edu.my

***Abstract* – Since Covid-19 pandemic, population in all the world have change their lifestyle in order to suppress the virus transmission. The popularised of digital technology give a great opportunity to the cybercrimes to conduct their cyberattack activities. Since the pandemic, the cybercrimes have manipulated the victims as the source of financial income. The main aim of this research is to develop mobile application to educate people on cybersecurity and prevent them from being attacked. 400 of Malaysian who are not adequate the cybersecurity knowledge is involved in the questionnaire survey. The proposed system has implemented stratified sampling method which falls under probability sampling. In the questionnaire, clear instructions will be given with either ranking questions or rating questions. As a consequence, the proposed mobile application is important to the Malaysian in order to reduce the cyberattack occurred in any individuals. By using the mobile application, the public may increase the cybersecurity awareness as well as having precaution on getting cyberattacks. The future recommendations can more focus on the functionality of the mobile application and related topic on the cybersecurity education.**

***Index Terms* – Cybersecurity education, mobile applications, cyber attack.**

1. Introduction

Since December 2019, the novel Coronavirus infection (COVID-19) is a new pandemic that affected people in the whole world. Starting from March 18th in 2020, the government of Malaysia has enforced a Movement Control Order (MCO) in order to slow down the transmission rate of "severe acute respiratory syndrome coronavirus 2" (SARS-CoV-2), the virus of COVID-19. MCO is referred as "lockdowns", which all the Malaysian has movement restriction, as well as mandated the shutdown of business and education institution [2]. Within the new announcement, all the daily activities are affected since everyone is in prohibition of movement, which means that all the gathering activities is not allowed. In order to maintain the business and education, everything is transformed into digital which the tasks are conducted in online platform. Work from home (WFH) and e-learning is becoming a new norm due to the impact of Covid-19 [10]. Reference [33] stated the internet traffic in Malaysia countrywide has increased 23.5 percent in the first week of MCO. It has a further increase of 8.6 percent which is a total of 32.1 % in second week of MCO. As the Internet users has increased significantly, cybercrime also rise since the beginning of the pandemic [37]. Based on the study, the cyber criminals may conduct different types of cyber-attacks due to the insufficient knowledge of users [26]. During the pandemic, cyber criminals have more focus on the attack related to the pandemic such as sharing unproven news on social media, sending phishing emails, and hacking the vulnerability on the old software [39]. The goal of the attacks is to misguide the victims, in order to earn money by stealing and selling a person's confidential information.

2. Research Background / Literature Review

2.1. Cyberattack

Cyberattack can be defined as an unauthorised individual with spiteful intent who launch the attack on data, hardware, software, or network in computer system [14]. The action may achieve the goals include financial gain, entertainment, or revenge by destroy, disrupt, degrade, disable, or maliciously control the computer infrastructure [4]. The typical types of cyberattacks are phishing, scam, malware, intrusion, ransomware and etc.

Based on the incident report from Malaysia Computer Emergency Response Team (MyCERT) in March 2020, the rate of cybercrimes has increased 43%. All the top three incident reported in March 2020 have increase from 10% to 115% compared to previous month, which are fraud has increase 10% (798 incidents), intrusion has increase 34% (125 incidents), and cyber harassment has increase the highest 115% (58 incidents) [36]. Reference [43] has mentioned about the total of cyberattack has reached a maximum of 10790 in 2020 which has broken the record from 2015. Due to the Covid-19 pandemic, it is an expected result as the cases of cyberattack is continuing increased [46]. The new norm include work from home, e-learning and online shopping have significant increased. This has provided an environment to the cybercrime for ongoing or enlarging their cyberattack activities [16].

In order to fit into the new massive cyber environment, cyber defense as the flip side of cyberattacks should be practiced consistently. Awareness among the public should be concerned so they can take action to mitigate and prevent themselves as a victim of cyber-attack effectively. The rate of cyberattack will be reduced simultaneously as the online vulnerability and weakness of the Internet is diminished.

2.2. Cybersecurity Education

The definition of cybersecurity is highly inconstant as it is widely used in different industry and comes out with a subjective definition. The terms of cybersecurity can be discussed by separating the two domains, "cyber" and "security" [12]. Cyber as a prefix of cyberspace refers to "electronic communication networks and virtual reality" [38]. Reference [40] has clarified the meaning of cyber as "the electronic world created by interconnected networks of information technology and the information on those networks." For the term "security", it is hard to be defined in general sense as the terms takes on meaning based on a person's perspective. Still, the main idea of security is being free from danger or threat [38]. Reference [5] also mentioned that the term security should be included the understanding of threats, referent object, causes and impact of the danger. From reviewing a broad range of definitions of cybersecurity, it can be concluded as cybersecurity is the collection of resources in order to protect or defend the cyberspace from being cyberattack by unauthorised [9][22][30][24]. Professor Drever has mentioned "Education is a process in which and by which knowledge, character and behaviour of the young are shaped and moulded." [27]. Thompson also stated that education may influence a person's view, habits, behaviour, thought and attitude [27].

Reference [41] shows the cybersecurity awareness among the Internet user in Malaysia is in a low or moderate level. For instance, Cyber Crime and Multimedia PDRM Investigation Division has reported of the statistical figure about cyber-love scams as known as African Scam has taken the attention from everyone [1]. Marimuthu also mentioned that Malaysian has lost more than RM4.9 million due to fraudulent purchase of goods in housing, tourism and automobile sector online. From the two example cases, it is crucial to implement of cybersecurity education among the public [35]. However, most of the cybersecurity education is more focus on higher education and for intermediate level as it has a certain difficulty on the courses [6][3]. Most of the teaching method that implement in cybersecurity education is more on conference and workshop which is not beginner friendly [42]. A person's age also will affect his or her education progress in cybersecurity sector [13].

As the Internet has totally impacted everyone's life especially in Covid-19 pandemic, cybersecurity education play an important role as the conveyed cybersecurity knowledge will change a person's practices in order to protect themselves from being cyberattack. Cybersecurity education should popularize on different category but not just focus on tertiary education. Besides, the education method should be more interactive so the publics may gain the difficult knowledge in a motivated environment.

2.3. Mobile Application

A mobile application is a set of programs that run on a hand holdable mobile gadgets and perform certain task based on the responses from user. It has used in a vast range of functionalities, including communication, entertainment, business, learning etc. Compared to computer application, it is much more convenience as mobile apps is ease of use and assessable in anywhere, anyplace, anytime [21]. Mobile apps also provide a higher quality with a lower price or free of charge to the consumers. User friendly and attractiveness is the main element that the consumer will more prefer on mobile application compared to other platform like website or computer application. The mobile apps are available for update to enhance its features and reduce the error of the apps [11].

While everyone is adapting the new norm from Covid 19 pandemic, the consumers are more rely to mobile applications for their need no matter for any purposes. Reference [44] has stated that there are more than 31 billion new apps has been downloaded and the popularity of mobile application development has risen with a 366% in quarter one of 2020. Since the huge dependent on the mobile application, the education can be conduct through mobile application. Based on the research, learning via mobile application is effective for the learners as they may gain the critical knowledge in a short period with a personalized learning experience [15].

Since mobile application is more capable and usable, the proposed system is designed to implement an online learning mobile application. With the limitation of research has been conducted on mobile application with cybersecurity education, the proposed system will be developed on mobile application which focus on cybersecurity education in order to enhance the fundamentals of the learners in a more interesting and accessible way.

2.4. Similar System

Figure 1.0* - Screenshot of the *Anti-Phishing Phil, tutorial before the game starte.

Source: https://search.proquest.com/openview/17ed0ff94edfac5f8222f9d4b73f717a/1?pq-origsite=gscholar&cbl=18750

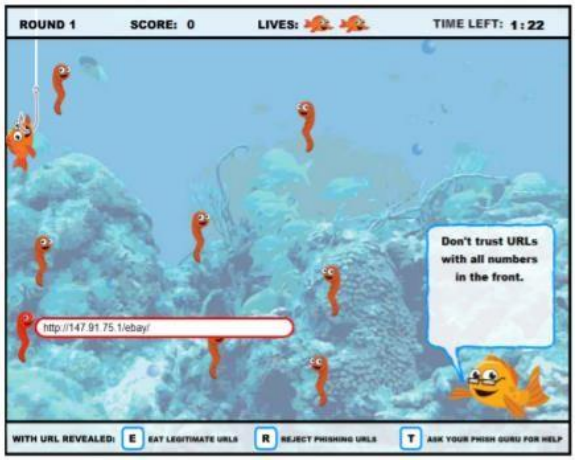

Figure 2.0 - Screenshot of the Anti-Phishing Phil, tips given by PhishGuru
Source: https://search.proquest.com/openview/17ed0ff94edfac5f8222f9d4b73f717a/1?pq-origsite=gscholar&cbl=18750

Considering of the Covid-19 pandemic, the Internet has been popularised and using of Internet has become a routine in the new norms. The fundamentals of cybersecurity education are crucial to protect the publics from being victims of the cyber-attacks [41]. Kumaraguru has developed an educational system which is called "Anti-Phishing Phil" [28]. It is a game-based system that only focus on the education of the phishing attack. Phishing attack is categorised as a kind of social engineering attack which manipulate the victims to share their information or sensitive data. The attack can be formed as the phishing criminals has masquerade as a trusted entity to lure the victims into opening the emails or ULRs. The phishing awareness among the public is crucial as phishing can be prevented by the end-users [20]. Anti-Phishing Phil system is built based on the learning science principles. Based on the learning science principles [8], the trainees have been motivated to learnt about phishing attack by an embedding training which is in more interesting ways. In this system, the learners have been taught to distinguish about the legal and fraudulent URLs. Users also have the opportunity to practice themselves in several times and a summary will list all the questions and answers when the round is over. In order to achieve the goal of the user have an ability to make more accurate on the online trust decision, Anti-Phishing Phil have provided an entertainment platform so the users can learn a more difficult anti-phishing approach. In this game, Phil as a young fish wish to eat the correct worms (legal links) and reject the fake worms (fraud links) as shown in Figure 1.0. Based on the Figure 2.0, PhishGuru as an experienced fish helps Phil to prevent from the fake worms by giving Phils some tips. Wombat Security Technologies is a company that provides the security awareness and training solution has modified and commercialized the Anti-Phishing Phil as their product [47].

Figure 3.0 - Screenshot of the video-based education on OnGuardOnline
Source: https://heinonline.org/HOL/LandingPage?handle=hein.journals/umkc75&div=13&id=&page=

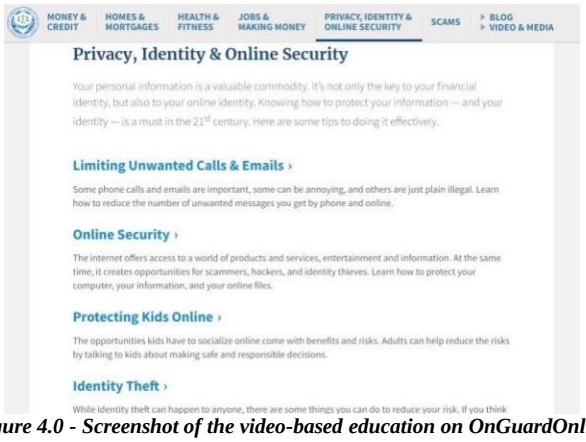

Figure 4.0 - Screenshot of the video-based education on OnGuardOnline
Source: https://heinonline.org/HOL/LandingPage?handle=hein.journals/umkc75&div=13&id=&page=

One of the independence agencies in United State, Federal Trade Commission has developed a website called OnGuardOnline [32][18]. The website is established to educate the consumers about the knowledge related to Internet safety and responsibility [31]. With this website, the users may prevent themselves as a victim of cyber-attack or Internet fraud without giving any charges. Based on Figure 3.0 and 4.0, OnGuardOnline offers two types of activity such as article and video, the consumers may learn the online security tips and resources based on their learning preference. Normally, the video is advised on the solutions to a person who are facing cyber-attacks and suggestions to the persons in order to protect themselves from being cyber-attacks. Users may figure out the level of proficient of themselves in cybersecurity by using the quizzes on the website. FTC teams also emphasized on the advance technology which the website information will be updated frequently. Besides, OnGuardOnline also offer the content which related to privacy, identity, and online security. The topic like precautions of social networking, online investing, on secure network devices physically and security action for housing network [17].

Table 1: Comparison Table of Anti-Phishing Phil & OnGuardOnline

	Anti-Phishing Phil	OnGuardOnline
Platform	System	Website
Education Method	Game-based	Video & Article
Accessibility	X	X
Intereactive Learning	✓	X
High of Cybersecurity Knowledge	X	✓

Based on Table 1, Anti-Phishing Phil and OnGuardOnline are compared as the similar system order to protect themselves from being cyber-attacks. Both systems have the strength and limitation respectively. In Anti-Phishing Phil, it provides a game-based education system which focus on anti-Phishing attack to the public like identify the fake links. The learners can learn in an interesting environment, but the public may have insufficient cyber-attacks knowledge as the system just only focus on the anti-phishing attack. In OnGuardOnline, it is more focus on the variety of cybersecurity resource in video and article based. However, the OnGuardOnline as well as Anti-Phishing Phil is not mobile-friendly which leads to the users are more difficult to open the video or article from the actual sized. The ways of learning in OnGuardOnline are more boring compared to Anti-Phishing Phil which provide an interactive game in learning process. Therefore, in the proposed system, it is planned to develop on mobile application as there is a little cybersecurity education system are proposed in mobile application. In order to educate people on cybersecurity and prevent them from being attacked, the cybersecurity knowledge is provided should be in a more interesting way so the publics may have a motivation on their self-learning path. The proposed mobile application is a game based as well as video, quizzes, article with the short explanation. Hence, the public have an option to choose their learning method in an entertainment method.

3. Problem Statement

Due to Covid 19 pandemic, the Internet users increases exponentially as work from home (WFH) and e-learning is the new normal for this situation [19]. Most of the sector such as education and business enterprise are going online brings the impact of cyberattacks incidents such as ransomware, phishing, malware has significantly growth [25][23]. The users believe that they are not the target of the cyber victims or doubt that cybercrime is the things. In contrast, the cyber-attack can cause an individual to loss a large amount of personal data which can affect the financial level for an individual [45]. The beginning of cyber incidents comes when one decides to neglect prevention and lack of knowledge in cybersecurity. Some of the common user's characteristic may bring an issues forwards cybercrime includes the gain profits from illegal ways, follow new trend of social media, ignore the update of software or operating system, and download the unknown files or browse through the phishing URLs [34][29][16][7].

4. Aim and Objectives

4.1. Aim

The main aim of this research is to develop mobile application to educate people on cybersecurity and prevent them from being attacked.

4.2. Objectives

4.2.1 To convey the knowledge of cyber threats to the users.

4.2.2 To educate the users about the data sensitivity and data protection.

4.2.3 To provide the information on how to avoid Phishing emails and malicious files.

5. Research Significant

The proposed research is significant as it is beneficial to society especially in this Covid 19 pandemic. While everyone is adapting to the culture of new normal like conduct the daily life in online platform no matter is working or learning, the Internet users are not aware on their online activities. Lack of knowledge in cyber security might cause an individual becomes the victims of cyber-attack. The proposed mobile application is specially designed for educating the public about the cybersecurity knowledge. By applying the approached system, the public will increase their awareness to prevent them from being cyber-attack. Internet users also may protect their data so the data will not be misused by someone for fraud. Consequentially, the rate of cyber-attack will be reduced spontaneously as the fundamentals concepts of cybersecurity among the public increased.

6. Methodology

In the proposed system, it is targeted on the Malaysian who are not familiar in cybersecurity knowledge. As the large portion population involved in the system, sampling method is used for generalising the behaviour of the entire group. A total of 400 people is participated in the sampling method which each 25 people is surveyed from 13 states and 3 federal territories, which are Johore, Malacca, Negeri Sembilan, Selangor, Pahang, Perak, Penang, Kedah, Kelantan, Terengganu, Perlis, Sabah, Sarawak, Labuan, Kuala Lumpur, and Putrajaya. With the random selection, probability sampling method is chosen as each population has an equal chance to be selected. Stratifies sampling which under complex probability sampling is applied to investigate the proposed mobile application. According to stratified sampling, the method is started with divide the population into different strata based on their similar characteristic which is age. In the population of lacked on cybersecurity education, people who are under the age of 18 and over the age of 18 is defined as two of the strata in stratified sampling. It is because the proposed system has conveyed the fundamentals in different kind of method like games, video, and articles. With the help of the method, the proposed system can have an idea of which part of educational approach should be more focus on. As the big number of people participated in the survey, the research is using questionnaires to get the data which fall under quantitative method. The questionnaire is planned to design with the clear instruction so the respondents may complete the questions with any assist from the researcher which called "self-administered". In these questions, closed questions will be listed by using ranking questions and rating questions. Ranking questions is requesting the respondent to

place the answer in a ranking order. It is used to understand the corresponding significant to the respondent. In rating question, Likert-style rating scale has requested the user to express opinion based on how strongly respondent agree or disagree with a question statement. It is used to collect the opinion data in order to measure the strength of the respondent opinions. There are some limitations by using questionnaire as the data collective method. First, the number of respondents will insufficient as poor responses will be faced since random people is requested to respond on the survey. With the insufficient responses, biases sample may occur which leads to fallacy of the data. Less enthusiasm has a possibility with not complete the form as lack of motivation. The problem can be minimised with getting a management support in order to having a higher response rate. Creating a huge mailing list and following up the procedure like send a reminder email to the respondent before the due date may increase the response rate also.

7. Overview of The Proposed System

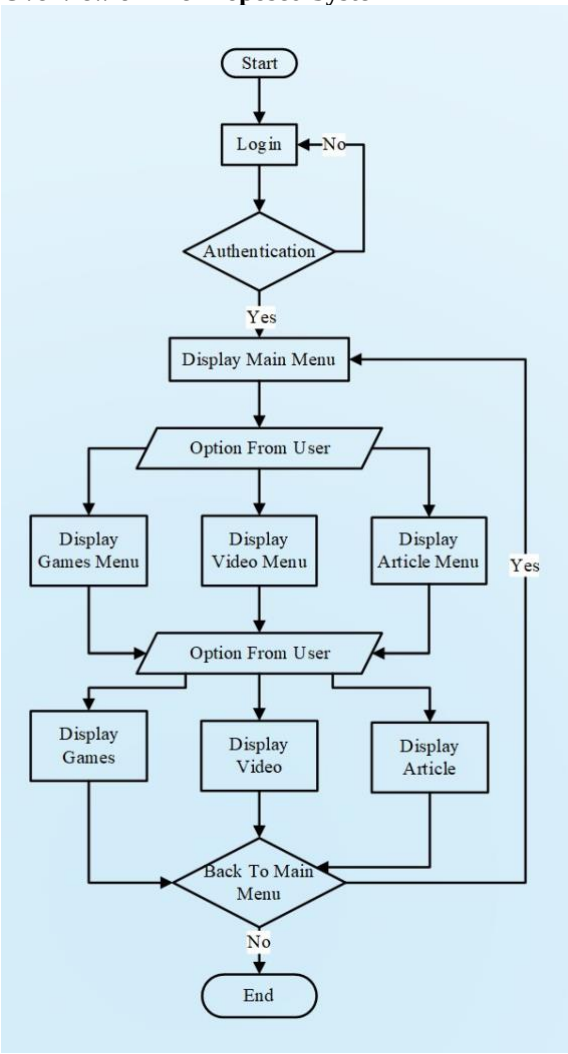

Figure 5.0 – Flowchart of Proposed System

Figure 9.1 is the flowchart which shows the main function of the proposed mobile application. In the proposed mobile application, the users have to login with their identity credentials such as username and password. In the authentication process, the user is with correct credentials may proceed to the main menu Graphic User Interface (GUI). If the user is failed to authenticate their credentials, the user will not be able to proceed with the main menu interface. In main menu, the user may choose their option regarding to the preferred education method which are game-based, video-based or article-based. In each method menu, the user may sort the cybersecurity education based on the category or time. In the last of system, the user has a right to back to the main menu or close the application. With the straightforward and interactive graphic user interface, the learners may learn the complicated cybersecurity education in a flexible, personalized, and high motivation environment.

8. Conclusion

Covid-19 pandemic has boost up the digital technology due to the new norms like social distancing and nationwide lockdowns. People and organisation in all over the world have affected their daily life as they have to adapt the new ways to study, work and life. In this case, cybersecurity education is crucial since thousands of people have adjust their lifestyle such as work from home (WFH) and e-learning. A person may lose their personal data as well as substantial financial loss due to the cyberattack from cybercriminals. In order to minimise the cyberattack in Malaysia, a mobile application is proposed with the goal of educate the public about the cybersecurity knowledge. The approach may benefit to the public who are not familiar in cybersecurity fundamentals. They will gain the cybersecurity knowledge to increase their awareness as well as prevent themselves from being a cyber victim. With the different range of age is involved in the mobile application, it is designed has adopt the user-friendly concept which are simple, clear and meaningful. The cybersecurity education is provided in several method like game-based, video-based, and article-based. Therefore, the public may gain the knowledge in a more interesting environment with high motivation level to keep their learning path. In future recommendations, the functionality of mobile application can be extended. More topic that related to cybersecurity education can be included in each teaching method.

References

[1] Annuar, S. S. (2018). 8,313 kes penipuan siber direkodkan. *Berita Harian*. https://www.bharian.com.my/berita/nasional/2018/10/483422/8313-kes-penipuan-siber-direkodkan

[2] Aziz, N. A., Othman, J., Lugova, H., & Suleiman, A. (2020). Malaysia's approach in handling COVID-19 onslaught: Report on the Movement Control Order (MCO) and targeted screening to reduce community infection rate and impact on public health and economy. *Journal of Infection and Public Health*, *13*(12), 1823–1829. https://doi.org/10.1016/j.jiph.2020.08.007

[3] Berger, H., & Jones, A. (2016). Cyber security & ethical hacking for SMEs. In *Proceedings of the The 11th International Knowledge Management in Organizations Conference on The changing face of Knowledge Management Impacting Society*, 1-6. https://dl.acm.org/doi/abs/10.1145/2925995.2926016

[4] Brar, H. S., & Kumar, G. (2018). Cybercrimes: A proposed taxonomy and challenges. *Journal of Computer Networks and Communications*, 11. https://doi:10.1155/2018/1798659

[5] Buzan, B., Wæver, O., & De Wilde, J. (1998). *Security: A New Framework for Analysis*. Boulder, CO: Lynne Rienner Publishers.

[6] Catota, F. E., Morgan, M. G., & Sicker, D. C. (2019). Cybersecurity education in a developing nation: the Ecuadorian environment. *Journal of Cybersecurity*, *5*(1). https://academic.oup.com/cybersecurity/article-pdf/doi/10.1093/cybsec/tyz001/28086821/tyz001.pdf

[7] Chigada, J., & Madzinga, R. (2021). Cyberattacks and threats during COVID-19: A systematic literature review. SA Journal of Information Management, 23(1). http://www.scielo.org.za/scielo.php?script=sci_arttext&pid=S1560-683X2021000100001

[8] Clark, R. C. (1989). *Developing Technical Training: A Structured Approach for the Development of Classroom and Computer-Based Instructional Materials*. Addison Wesley Publishing Company.

[9] CNSS. (2010). National Information Assurance Glossary. *Committee on National Security Systems (CNSS) Instruction, 4009*. http://www.ncix.gov/publications/policy/docs/CNSSI_4009.pdf

[10] Corpuz, J. C. G. (2021). Adapting to the culture of "new normal": an emerging response to COVID-19. *Journal of Public Health*, *43*(2), 344–345. https://doi.org/10.1093/pubmed/fdab057

[11] Corral, L., Janes, A., & Remencius, T. (2012). Potential advantages and disadvantages of multiplatform development frameworks–A vision on mobile environments. *Procedia Computer Science*, *10*, 1202-1207. https://doi:10.1016/j.procs.2012.06.173

[12] Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, *4*(10). https://www.timreview.ca/article/835

[13] Daengsi, T., Pornpongtechavanich, P., & Wuttidittachotti, P. (2021). Cybersecurity Awareness Enhancement: A Study of the Effects of Age and Gender of Thai Employees Associated with Phishing Attacks. *Education and Information Technologies*, 1-24. https://doi.org/10.1007/s10639-021-10806-7

[14] Denning, P. J., & Denning, D. E. (2010). Discussing cyber attack. Communications of the ACM, 53(9), 29-31. https://10.1145/1810891.1810904

[15] Drigas, A. S., & Angelidakis, P. (2017). Mobile Applications within Education: An Overview of Application Paradigms in Specific Categories. *International Journal of Interactive Mobile Technologies*, *11*(4). https://doi.org/10.3991/ijim.v11i4.6589

[16] Eian, I. C., Yong, L. K., Li, M. Y. X., Qi, Y. H., & Fatima, Z. (2020). Cyber attacks in the era of covid-19 and possible solution domains. https://www.preprints.org/manuscript/202009.0630

[17] Federal Trade Commission. (2007). Enhancing FTC Consumer Protection in Financial Dealings with Telemarketers and the Internet. *U.S. Government Printing Office*. https://books.google.com.my/books?id=YoiOgA3yXG0C&pg=PA26&dq=OnGuard+Online&hl=en&sa=X&ved=2ahUKEwjru_DKxczAhWir1YBHe8zB-cQ6AF6BAgKEAI#v=onepage&q=OnGuard%20Online&f=false

[18] Federal Trade Commission. (n.d.). *Consumer Information*. Retrieved January 25, 2022, from https://www.consumer.ftc.gov/

[19] Feldmann, A., Gasser, O., Lichtblau, F., Pujol, E., Poese, I., Dietzel, C., Wagner, D., Wichtlhuber, M., Tapiador, J., Vallina-Rodriguez, N., Hohlfeld, O., & Smaragdakis, G. (2020). The Lockdown Effect. *Proceedings of the ACM Internet Measurement Conference*, 1-18. https://dl.acm.org/doi/pdf/10.1145/3419394.3423658

[20] Hong, J. (2012). The state of phishing attacks. *Communications of the ACM*, *55*(1), 74-81. https://doi/abs/10.1145/2063176.2063197

[21] Islam, R., Islam, R., & Mazumder, T. (2010). Mobile application and its global impact. *International Journal of Engineering & Technology (IJEST)*, *10*(6), 72-78. https://doi=10.1.1.657.9773

[22] ITU. (2009). *Overview of Cybersecurity. Geneva: International Telecommunication Union (ITU).* http://www.itu.int/rec/T-REC-X.1205-200804-I/en

[23] Jayakumar, P., Brohi, S. N., & Zaman, N. (2020). *Top 7 lessons learned from COVID-19 pandemic.* https://www.researchgate.net/profile/Sarfraz-Brohi/publication/341254687_Top_7_Lessons_Learned_from_COVID-19_Pandemic/links/5ebacc87299bf1c09ab6c42a/Top-7-Lessons-Learned-from-COVID-19-Pandemic.pdf

[24] Kemmerer, R. A. (2003). Cybersecurity. *Proceedings of the 25th IEEE International Conference on Software Engineering*, 705-715. http://dx.doi.org/10.1109/ICSE.2003.1201257

[25] Khan, N. A., Brohi, S. N., & Zaman, N. (2020). *Ten deadly cyber security threats amid COVID-19 pandemic.* https://www.techrxiv.org/articles/preprint/Ten_Deadly_Cyber_Security_Threats_Amid_COVID-19_Pandemic/12278792/files/22624319.pdf

[26] Khweiled, R., Jazzar, M., & Eleyan, D. (2021). Cybercrimes during COVID -19 Pandemic. *International Journal of Information*

Engineering and Electronic Business, *13*(2), 1–10. https://doi.org/10.5815/ijieeb.2021.02.01

[27] Kumar, S., & Ahmad, S. (2008). Meaning, aims and process of education. *School of Open Learning*, 3-6.

[28] Kumaraguru, P. (2009). PhishGuru: A System for Educating Users about Semantic Attacks. *Carnegie Mellon University*, 1–199. https://search.proquest.com/openview/17ed0ff94edfac5f8222f9d4b73f717a/1?pq-origsite=gscholar&cbl=18750

[29] Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, 105. https://arxiv.org/pdf/2006.11929.pdf

[30] Lewis, J. A. (2006). Cybersecurity and critical infrastructure protection. *Center for Strategic and International Studies*. 1(12). http://csis.org/publication/cybersecurity-and-critical-infrastructure-protection

[31] LiteracyLink, P. B. S., & Education, H. A. (n.d.). *Free Online Resources*. https://media.gcflearnfree.org/content/56390951927fb614d0c2face_11_03_2015/free%20online%20resources%202017.pdf

[32] Majoras, D. P. (2006). Federal Trade Commission: Learning from History as We Confront Today's Consumer Challenges. *UMKC Law Review*, *75*, 115. https://heinonline.org/HOL/LandingPage?handle=hein.journals/umkc75&div=13&id=&page=

[33] Malaysian Communications And Multimedia Commission (MCMC) | Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM). (2020). *Media Statement: Changing Usage Patterns Influence Internet Speed In Malaysia | Malaysian Communications And Multimedia Commission (MCMC)*. https://www.mcmc.gov.my/en/media/press-releases/media-statement-changing-usage-patterns-influence

[34] Mandal, S., & Khan, D. A. (2020, September). A Study of security threats in cloud: Passive impact of COVID-19 pandemic. *International Conference on Smart Electronics and Communication (ICOSEC)*. 837-842. https://www.researchgate.net/profile/Sudakshina-Mandal/publication/343745876_A_Study_of_Security_Threats_in_Cloud_Passive_Impact_of_COVID-19_Pandemic/links/5f5b2238299bf1d43cf99ca9/A-Study-of-Security-Threats-in-Cloud-Passive-Impact-of-COVID-19-Pandemic.pdf

[35] Marimuthu, M. (2016). *Pembelian secara online catat kes penipuan paling tinggi pada 2015.* https://www.nccc.org.my/v2/index.php/home/1763-pembelian-secara-online-catat-kes-penipuan-paling-tinggi-pada-2015

[36] MyCERT (2020). *Reported Incidents based on General Incident Classification Statistics 2020.* https://www.mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-4d11-8169-66677d694932&id=2650ed29-88be-4cec-86cc-13f8e07ae228

[37] Naidoo, R. (2020). A multi-level influence model of COVID-19 themed cybercrime. *European Journal of Information Systems*, *29*(3), 306-321.

[38] Oxford University Press. (2014). Oxford Online Dictionary. http://www.oxforddictionaries.com/definition/english/Cybersecurity

[39] Pranggono, B., & Arabo, A. (2020). COVID-19 Pandemic Cybersecurity Issues. *Internet Technology Letters*, *4*(2), 1–6. https://doi.org/10.1002/itl2.247

[40] Public Safety Canada. (2010). *Canada's Cyber Security Strategy. Ottawa: Public Safety Canada, Government of Canada.* http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-eng.aspx

[41] Rahman, N. A. A., Sairi, I. H., Zizi, N. A. M., & Khalid, F. (2020). The Importance of Cybersecurity Education in School. *International Journal of Information and Education Technology*, *10*(5), 378–382. https://doi.org/10.18178/ijiet.2020.10.5.1393

[42] Schneider, F. B. (2013). Cybersecurity education in universities. *IEEE Security & Privacy*, *11*(4), 3-4. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6573305

[43] Singh, M. M., Frank, R., & Zainon, W. M. N. W. (2021). Cyber-criminology defense in pervasive environment: A study of cybercrimes In Malaysia. *Bulletin of Electrical Engineering and Informatics*, *10*(3), 1658-1668. https://beei.org/index.php/EEI/article/download/3028/2230

[44] Smartbear Company. (2020). *App Usage & Popularity Statistics During COVID-19*. https://www.bugsnag.com/covid-19-app-usage-error-data-report

[45] Spremić, M., & Šimunic, A. (2018). Cyber security challenges in digital economy. *In Proceedings of the World Congress on Engineering*, *1*, 1-6. http://www.iaeng.org/publication/WCE2018/WCE2018_pp341-346.pdf

[46] Tan, S. L., Vergara, R. G., Khan, N., & Khan, S. (2020). Cybersecurity and privacy impact on older persons amid COVID-19: A socio-legal study in Malaysia. *Asian Journal of Research in Education and Social Sciences*, *2*(2), 72-76. https://myjms.mohe.gov.my/index.php/ajress/article/download/9697/4601

[47] Wombat Security Technologies. (2008). *Why Wombat?* https://info.wombatsecurity.com/hubfs/WhyWombat_0116.pdf