An application to Raise Cyber Security Awareness Among Organization Employees

Hong Yen Wai[1], Intan Farahana Binti Kamsin[2], Zety Marlia Binti Zainal Abidin[3] and Hemalata A/P Vasudavan[4]
[1'2'3'4]Asia Pacific University of Technology and Innovation, Technology Park Malaysia, Bukit Jalil, Kuala Lumpur, Malaysia.
[1]ywhong0328@gmail.com, [2]intan.farahana@staffemail.apu.edu.my, [3]zety@staffemail.apu.edu.my, [4]hemalata@staffemail.apu.edu.my

***Abstract*— The cyber security attacks incidents have been growing rapidly all around the globe recently due to the growth of internet users, especially since the covid-19 pandemic started. This has caused financial and intellectual properties losses to many organizations. The aim of this research is to come up with an application which helps the organizations to combat cyber security incidents due to the lack of cyber security awareness of employees. A survey will be distributed to the target employees in the organizations selected using cluster sampling. The proposed application has included a few important features such as artificial intelligence, hands-on training with guidance, as well as the capability for the user to socialize within the application. Future recommendation of adding an admin panel to the application has also been covered.**

***Index Terms*— Cyber security awareness, Cyber security training, Employee cyber security awareness**

1. Introduction

Internet technology has been playing a dominant role in people's life since the world has slowly transformed into this digital era [1]. It serves billions of users worldwide across different sectors such as retails, education, and governance [1]. However, the number did not stop there. Since the start of the covid-19 pandemic globally, there are a noticeable increase in numbers of organization moving their businesses online, causing a surge in the ecommerce sector [2]. The people and organizations also begin to depend heavily on the digital technologies to get connected for their daily tasks [3]. Alongside with the growth of internet users, the cyber-attack incidents are incrementing as well, so does the victims of cyberattacks, which includes the healthcare sector especially during this pandemic time [4]. According to Symantec, 69% out of the 20000 people from a total of 24 countries has at least once been fall as a victim in cyber security incidents [5]. Thus, cyberattacks have to be prevented to protect the intellectual properties of the people and organizations.

2. Literature Review 2.1 Research Domains

2.1.1 Application

An application is a type of software that falls under the computer software category [6]. It can be written in different programming languages such as C++, Java, Python, and Go. It helps the user in performing a specific task with the help of computer system, in order to speed up the process compared to doing it manually [6].

Due to the current covid-19 pandemic, the education method and system during pre-pandemic is not quite relevant anymore, there are better ways to deliver knowledge in education system, such as online education which also known as e-learning [7]. The research has concluded that digitization of education is the number one priority for the post pandemic globally [8]. Hence, developing an application can help to fill the gap in this case as it could be accessible from any digital devices that has an Internet connection.

However, after further research on software application in the cyber security field, it is found that the traditional software algorithms which is used by majority of organizations nowadays seemed insufficient in fulfilling the needs of the industry [9]. The traditional systems are being built based on fixed rules and algorithms [10]. Which means that a database of the currently known issues will be needed to allow the system to carry out comparison. This is not appropriate as the system cannot figure out new potential vulnerabilities.

Thus, implementing machine learning in the application can help to overcome this issue, as the dynamic algorithm can recognize and analyze the traffics, patterns, and trends from the past experiences, and then perform prediction on the real-time behavior [10]. Apart from that, another technology is artificial intelligence [11]. It is an algorithm that mimics how the human thinking works, learn it, and then applies the solution on complex real-world problems when being implemented in a system [10]. According to the study, artificial intelligence has the capabilities in supporting both the defensive, as well as the offensive operations in cyber security field [12]. It can be backed by another study stating that integrating machine learning effectively can help in enhancing the effectiveness of the security countermeasures in an organization [13].

Therefore, this research will be proposing a software application, integrated with artificial intelligence and machine learning, with the goal of increasing the cyber security awareness in organizations' employees.

2.1.2 Cyber Security Awareness

Cyber security awareness is one of the most mentioned topics when it comes to preventing cyber-attacks. The cyber security awareness is often associated with a person's knowledge regarding the potential legal violation, as well as the risks in exposing the company to potential cyber security attacks [14]. Besides that, security awareness is also a descriptive phrase towards increasing the users' attention regarding the importance of information security [15]. It has been described as a primary defensing method of organizations in mitigating security breaches [16]. This can be backed by a study that targeted university students, indicating that the solution for mitigating cyber-attack risks can be prevented through the increase of cyber security awareness [17]. Apart from that, the author from another research agreed that the first step in coping the absence of general cyber-attacks understanding is by increasing the world-wide security awareness, starting from individual, way up to organization level [18].

However, the results of the research carried out by Enterprise Management Associates has shown that there are up to 56% of organization employees did not receive any form of security awareness training except for the information technology employees [19]. Moreover, the delivered content and quality for existing programs were not considered appropriate as well. This is further backed by another research where it showed that there is lack of email-based attacks training in a huge number of organizations [20]. Research on the cyber security awareness in the middle east also found that the people involved did not have the understanding, as well as the theoretical and practical knowledge that were required for their daily work activities [21].

Nonetheless, this issue can be overcome by conducting an awareness training program [21]. Education on security best practices needs to be included as part of the cyber security awareness training program to educate the employees [22]. Hence, this research aims to address the issues mentioned above by implementing a training application with the objective to raise the cyber security awareness of the organizations' employees.

2.1.3 Training Organization Employees in Raising Cyber Security Awareness

In this era where digital transformation is happening at a very fast pace compared to decades ago, organizations and ventures has begun to virtualize their businesses and services with the aim of reaching a wider audience. This eventually opens up endless of opportunities for the attackers to perform cyber-attacks [23]. However, due to the fact that the defensing technologies are getting better, the attackers now had decided to turn their head towards the weakest link in cyber defence, which is the human elements [24]. Hence, the significance of training organization employees to counter with the emerging cyber-attacks cannot be understated [24].

Nonetheless, there is a huge concern on the awareness programs provided are not working in a way it was expected to [20]. The study also doubted the effectiveness of current cyber awareness training offered in the organization as the reports for successful cyber-attacks were increasing day-by-day [25]. One of the possible reasons of why the organizations' training programs failed was because the employees have reached cyber security fatigue, and they do not have the motivation to participate in it [26]. The programs held were mainly focusing on the transfer of information such as security policies, virus and malwares prevention, as well as password management [27]. Although the knowledge being transferred were categorized as meaningful, but it failed to lead to behaviour changing such as raising the awareness [27]. This is backed by the research stated that there were no major improvements observed in reducing phishing scams when classroom training was implemented as the training option [28].

To overcome this matter, the results from the research shown that the hands-on experience are more preferred most of the time compared to the other options [29]. The researchers who performed research on the effectiveness of cyber security training in Japan also found that hands-on activities are much needed to ensure the effectiveness of the training program, so that the employees are able to deal with the daily real-life scenarios [30].

Thus, this research will be implementing practical training for organizations' employees, giving them the hands-on experience while guiding them the way it should be done, so that the skills are able to pick up by their muscle memory and then apply them on a daily operational basis.

2.2 Similar Systems

2.2.1 KnowBe4

KnowBe4 is a paid cyber security awareness training platform that was created to solve the current social engineering issues [31]. The platform mainly focusses on email phishing training, using the built-in automated phishing simulation program [32]. It also offers administration feature with the dashboard for generating reports so that the organization can visualize their phishing and training results at a glance.

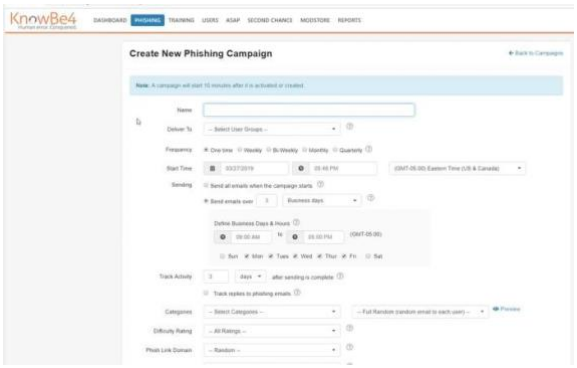

Figure 1 above shows an interface of KnowBe4's platform [31].

Figure 1 above shows the interface of KnowBe4's platform. Some of the settings that can be made were when will the campaign be taking place, the target users, and level of difficulty. Once they are all set, the campaign can be launched.

2.2.2 Infosec IQ

Infosec IQ is a paid security awareness training platform that integrated with the phishing simulation, to help in building the cyber awareness among organizations' employees [33]. One of the key features of Infosec IQ is it consist of the games which known as Choose Your Own Adventure, which gives the employees a gamification learning experience. Apart from that, the platform has a statistic dashboard which allows the admin to view the training and phishing results for further analysis.

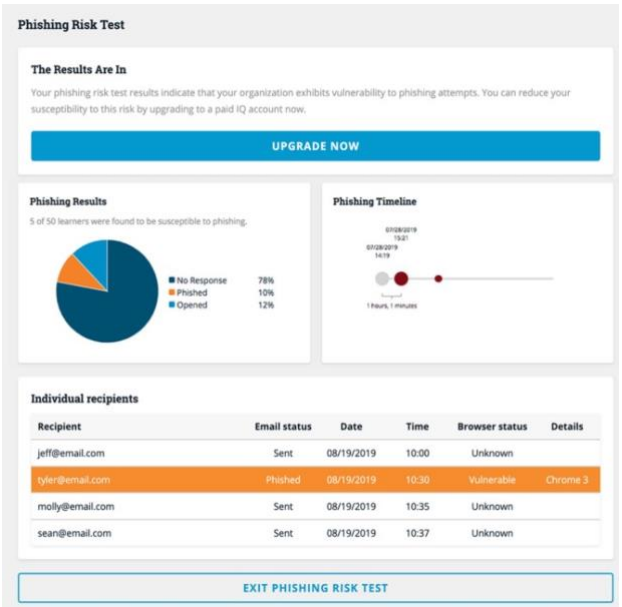

Figure 2 shows the interface of Infosec IQ [33].

Figure 2 above shows the interface of Infosec IQ platform where it can be viewed by the admin. It displays the results of the phishing campaign including detailed timeline, and who was the high-risk employee according to the status. It even let the admin to view who has opened the email and who did not open it.

2.2.3 Comparison Table

Features	KnowBe4	Infosec IQ	Proposed system
AI	✓	✗	✓
Email training	✓	✓	✓
Guide & tips	✗	✗	✓
Gamification	✓	✓	✗
Practical training	✗	✗	✓
Social	✗	✗	✓
Admin panel	✓	✓	✗
Pricing	Paid	Paid	Free

Table 1 shows the comparison table for different platforms.

The table 1 above shows the comparison table for each of the key features among the platforms. Each platform has its own pros and cons, and none of them carries every function stated.

Hence, the proposed system will be integrating most of the functions that were important from other similar systems as well as some of the great features which should be included, for instance, the artificial intelligence, pop-up guidance, practical hands-on training, socializing, which is the chat messages feature, and most importantly, making it free for download.

3. Problem Statement

The increasing of cyber-attacks has become an emerging threat that creates huge negative impacts to global organizations [34]. In fact, up to 95 percent of the total cyber incidents such as ransomware attacks, and data breaches, happened due to human factor [35]. The lack of cyber security skills among the employees has led to organization's significant financial and information losses [36]. Not to mention that it also caused reputational damage [37]. This is not saying that the employees do not have the knowledge at all, but the cyber security awareness is still way below sufficient despite that it is increasing [38]. According to Corradini, the factor of human beings is always considered as the weakest point in a security network [39]. Hence, it shows that the cyber security awareness among the employees plays a critical role in protecting the organizations from cyber-attacks [40].

4. Research Aims

The aim of this project is to propose an application for organizations' day-to-day internal use, which integrated with artificial intelligence, and practical security guidance.

5. Research Objectives

i. To create an application for organizations' private daily usage.

ii. To integrate artificial intelligence in the application to identify keywords, files, and links.

iii. To show pop-up guidance when files and links are being clicked.

6. Research Significance

The findings of this research will help to reduce the cyberattacks on organizations which related to human factors. The employees will be equipped with significantly better cyber security awareness, and cyber-attacks prevention skills, especially for the non-IT employees. Not to mention that these skills are implemented into their muscle memory and being applied on a daily basis. While towards the researchers, this research provides the insights of how training the employees in a different approach will benefit the organization compared to the traditional theoretical-based training. Thus, the research is crucial in assisting the cyber defense team for developing effective training courses in the future.

7. Methodology 7.1 Sampling method

The sampling method to be used in this research is cluster sampling. This method was chosen as it is more suitable and efficient for the quantitative research which will be carried out later on, where it will be involving specific type of employees from different organization across different geographical location [41].

By using cluster sampling method, the population will be divided according to the geographic locations, such as Bukit Jalil, Puchong, and Subang Jaya [42]. From each cluster, or area in this case, an equal number of organizations will be chosen randomly to represent the cluster.

7.2 Identify Respondents

The target respondents for the survey are the employees who are currently working for an organization. The daily activities of the targeted employees should involve the use of computers and emails, regardless the position titles.

This is due to the fact that the application is specially customized for employees used. Hence, they would be the best people where to get opinions, feedbacks, and suggestions from. This can help to improve the user experience of the application and increase the effectiveness of the cyber security awareness training program.

7.3 Data Collection Method

The data collection method to be used in this research is survey. Survey was chosen as it is more time saving and convenient compared to interview. It can help to reach wider audience as well because it can be distributed to the target respondents through the internet, which means that it is suitable for this research where it involved respondents from various geographical locations.

The survey will contain a total of 5 questions with 4 closedended questions where all 4 of them are using 5-point Likert scales. The fifth question will be an open-ended question. Before distributing to the selected organizations, a pilot test will be carried out on the employees in APU to ensure that the questions asked are suitable towards their level and easily understandable.

At the end of the survey, the collected data and relevant statistics would be put into a graph for further analysis purpose. The focus of the analysis will be mainly on evaluating the effectiveness of practical guidance training in raising the employees' cyber security awareness, and is the artificial intelligent technology implemented reliable, and lastly, how sustainable it is compared to the theoretical training methods.

8. Overview of the Proposed System

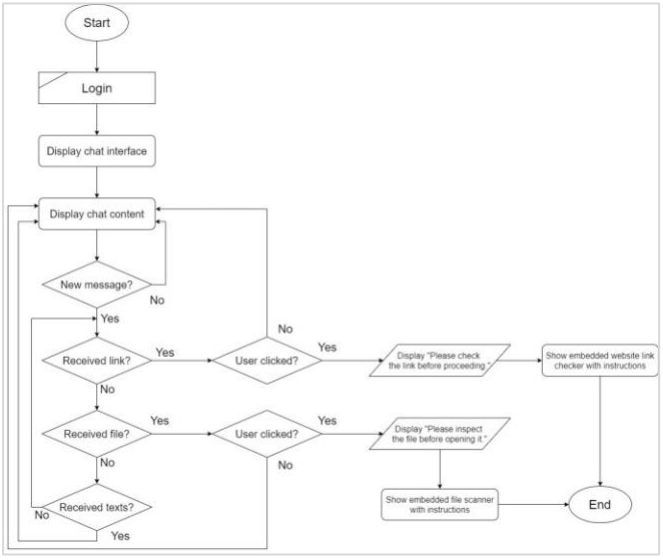

Figure 3 shows the flowchart of the proposed application.

Figure 3 above shows the flowchart for the proposed application. The registration and credential checking process will take place inside the Login function. After the user successfully login to her account, the chat interface will be displayed on screen. Then, the system retrieves and display the

previous chat histories, just like any chatting app on the market. If there are no new messages come in, the system remains in the background, constantly checking for new conversation. However, when there are new messages coming in, the system will verify the types of the message. The machine learning algorithm implemented will automatically identify whether the message consists of link, file, or normal texts. If it is a normal text, the texts are directly displayed to the user without any further action taken.

On the other hand, if the application detected link or file, it would then listen to the user's action on whether or not the link or file has been clicked. Once the user clicks on it, she will be prompt with the predefined messages for the link or file respectively. Next, the embedded window will pop-up depends on the item being clicked. If user clicked on link, then the popup will show the website redirection link checker which the user has to follow in order to open the link. Besides that, if the user clicked on a file, then the pop-up will show the file scanner which the user has to follow in order to open and view the content of the file.

9. Conclusion

In a nutshell, this research has showed how worldwide organization was impacted by the emerging cyber-attack threat incidents It also showed that one of the contributors towards these attacks was the lack of cyber security awareness among the employees.

The research also covered one of the possible reasons on why the traditional cyber security awareness training programs offered to the organization employees might not be effective enough stop the organization from cyber-attacks.

Hence, the author proposes an application with the key features to be included such as artificial intelligence, practical training program with guidance, as well as the ability for the users to socialize on the platform, hoping to fill the gaps of the traditional training programs offered by the current platforms.

One of the improvements that can be made to the system in the future is by adding an admin panel, where the dashboard will display the results and statistics of the program. This allows the organizations to better visualize and evaluate the outcomes difference of the employees, before and after the usage of the application.

References

[1] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments," *Energy Reports*, pp. 8176-8186, 2021.

[2] K. Sharma, " SURGE IN E-COMMERCE MARKET IN INDIA AFTER COVID-19 PANDEMIC," *Grand Academic Portal*, p. 57, 2020.

[3] I. Corradini, "The Digital Landscape," *Building a Cybersecurity Culture in Organizations*, pp. 1-22, 2020.

[4] M. Muthuppalaniappan and K. Stevenson, "Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health," *International Journal of Quality in Healthcare*, pp. 1-3, 2020.

[5] S. Nepal and J. Jang-Jaccard, "A survey of emerging threats in cybersecurity," *Journal of Computer and System Sciences*, pp. 973-993, 2014.

[6] S. Education, "Computer-Software," *SasakawaEducation*, pp. 1-7, - 2020.

[7] M. Constantinescu and V. Dumitrache, "THE IMPACT OF COVID 19 ON THE ROMANIAN MILITARY EDUCATION," *Conference proceedings of eLearning and Software for Education*, pp. 28-35, 2021.

[8] Alotaibi et al., "A survey of cyber-security awareness in Saudi Arabia," *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)*, p. 1, 2017.

[9] A. Okutan and C. Eyupoglu, "A Review on Artificial Intelligence and Cyber Security," *2021 6th International Conference on Computer Science and Engineering (UBMK)*, p. 1, 2021.

[10] K. Kumar and B. P. Pande, Cyber Security and Digital Forensics, Massachusetts: Scrivener Publishing LLC , 2022.

[11] C. V. Dalave and T. Dalave, "A REVIEW ON ARTIFICIAL INTELLIGENCE IN CYBER SECURITY," *International Research Journal of Modernization in Engineering Technology and Science*, pp. 33-35, 2022.

[12] A. Wenger, Cyber Security Politics Socio-Technological Transformations and Political Fragmentation, New York: Routledge, 2022.

[13] Suresh et al., "Chapter 10 - Contemporary survey on effectiveness of machine and deep learning techniques for cyber security," *Machine Learning for Biometrics*, pp. 177-200, 2022.

[14] Walterbusch et al., "Missing cloud security awareness: investigating risk exposure in shadow IT," *Journal of Enterprise Information Management*, pp. 644-665, 2017.

[15] I. Legard, "BUILDING AN EFFECTIVE INFORMATION SECURITY AWARENESS PROGRAM," *CEE e|Dem and e|Gov Days 2020*, pp. 189-200, 2020.

[16] Dahbur et al., "Assessment of Security Awareness: A Qualitative and Quantitative Study," *International Management Review* , p. 37, 2017.

[17] Garba et al., "A Study on Cybersecurity Awareness Among Students in Yobe State University, Nigeria: A Quantitative Approach," *Semantic Scholar*, pp. -, 2020.

[18] A. Bendovschi, "Cyber-Attacks – Trends, Patterns and Security Countermeasures," *Procedia Economics and Finance 28*, pp. 24-31, 2015.

[19] S. e. al., "An Effective Cybersecurity Training Model to Support an Organizational Awareness Program: The Cybersecurity Awareness TRAining Model (CATRAM). A Case Study in Canada," *Research Anthology on Artificial Intelligence Applications in Security*, p. 15, 2021.

[20] T. Caldwell, "Making security awareness training work," *Computer Fraud & Security*, pp. 8-14, 2016.

[21] S. Al-Janabi and I. Al-Shourbaji, "A Study of Cyber Security Awareness in Educational Environment in the Middle East," *Journal of Information & Knowledge Management*, p. 1, 2016.

[22] P. e. al., "Fortifying Corporate Human Wall: A Literature Review of Security Awareness and Training," *Information Technology Risk Management and Compliance in Modern Organizations*, p. 34, 2018.

[23] Sodagudi et al., "Novel Approaches to Identify and Prevent Cyber Attacks in Web," *2019 3rd International Conference on Computing Methodologies and Communication (ICCMC)*, pp. -, 2019.

[24] J. Abawajy, "User preference of cyber security awareness delivery methods," *Behavior & Information Technology*, pp. 237-248, 1 August 2014.

[25] Chowdhury et al., "Modeling effective cybersecurity training frameworks: A delphi method-based study," *Computers & Security*, pp. 1-15, 2022.

[26] W. He and Z. J. Zhang, "Enterprise cybersecurity training and awareness programs: Recommendations for success," *Journal of Organizational Computing and Electronic Commerce*, pp. 249-257, 2019.

[27] Khan et al., "Effectiveness of information security awareness methods based on psychological theories," *African Journal of Business Management*, pp. 1086210868, 2011.

[28] K. F. Tschakert and S. Ngamsuriyaroj, "Effectiveness of and user preferences for security awareness training methodologies," *Heliyon*, pp. 1-10, 2019.

[29] N. Chowdhury and V. Gkioulos, "Cyber security training for critical infrastructure protection: A literature review," *Computer Science Review*, pp. -, 2021.

[30] Beuran et al., "Towards Effective Cybersecurity Education and Training," *Japan Advanced Institute of Science and Technology*, pp. 1-16, n.d..

[31] KnowBe4, "KnowBe4," 2022. [Online]. Available: https://www.knowbe4.com/.

[32] TrustRadius, "KnowBe4 Security Awareness Training," 2022. [Online]. Available: https://www.trustradius.com/products/knowbe4/reviews?qs=pros-and-cons#features-scorecard.

[33] Infosec, "Infosec," 2022. [Online]. Available: https://www.infosecinstitute.com/iq/.

[34] H. Al-Mohannadi, I. Awan, J. A. Hamar, Y. A. Hamar, M. Shah and A. Musa, "Understanding Awareness of Cyber Security Threat Among IT Employees," *International Conference on Future Internet of Things and Cloud Workshops*, p. 188, 2018.

[35] C. N. Nobles, "Botching Human Factors in Cybersecurity in Business Organizations," *HOLISTICA – Journal of Business and Public Administration*, p. 71, 2018.

[36] M. Carlton, Y. Levy and M. Ramim, "Mitigating cyber attacks through the measurement of non-IT professionals' cybersecurity skills," *Information and Computer Security*, p. 101, 2019.

[37] C. Nobles, "Establishing Human Factors Programs to Mitigate Blind Spots in Cybersecurity," *Midwest (MWAIS) at AIS Electronic Library (AISeL)*, p. 1, 2019.

[38] F. L. Al-Dawod and B. Stefanska, "The importance of risk awareness in cybersecurity among companies - A perspective on the role of top management," *Linköping University | Department of Management and Engineering*, p. 1, 2021.

[39] I. Corradini, Security: Human Nature and Behaviour, Cham: Springer, 2020.

[40] K. Khando, S. Gao, S. M. Islam and A. Salman, "Enhancing employees information security awareness in private and public organisations: A systematic literature review," *Elsevier*, p. 1, 2021.

[41] S. Shantikumar, Research Methods, United Kingdom: Health Knowledge, 2018.

[42] A. S. Acharya et al., "Sampling: Why and How of it?," *INDIAN JOURNAL OF MEDICAL SPECIALITIE*, pp. 330-333, 2013.