Enhance Public Cybersecurity Awareness By Understanding Cybersecurity And Cyberthreats

Ng Qi Xuan
School of Computing
Asia Pacific University of Technology and innovation (APU)
Kuala Lumpur, Malaysia
TP059957@mail.apu.edu.my

Dr. Intan Farahana Binti Kamsin
School of Computing
Asia Pacific University of Technology and innovation (APU)
Kuala Lumpur, Malaysia
intan.farahana@staffemail.apu.edu.my

***Abstract*-The aim of this paper is to provide effective methods for increasing public awareness of cybersecurity by understanding cybersecurity and cyber threats. This research gathered information from journals and articles as well as open-access online surveys. This study will greatly assist the public in preventing cyber threats by understanding the nature and impact of cybersecurity and cyber threats, as well as the importance of cybersecurity awareness. This will also contribute to the overall quality and ethics of future cyber users.**

Keywords—Cybersecurity, Cybersecurity Awareness, Cyberthreats

I. INTRODUCTION

With the development of technology and the Internet, the Internet has gradually integrated into the lives of people today. At this time, cyber criminals are using the internet to steal, embezzle and maliciously distribute other people's money and personal information. In Malaysia, for example, according to Prime Minister Muhyiddin Yassin, cybercrime is on the rise, with 4,237 incidents registered in the first quarter of 2021 alone, with a total loss of RM77 million. According to the police, there were 11,875 incidents in 2019 with a loss of RM498 million and 14,229 incidents worth RM413 million are expected in 2020. (Bernama, 2021) The trend of cybercrime growth is increasing year by year, but the reality is that people's awareness of cybersecurity is not. This study will provide an insight into the level of cyber security awareness of people today and hopefully provide some good solutions to increase the awareness of cyber security. Also, by understanding the dangers of cyber threats, it will serve to warn and prove to everyone that the trend of increasing cybersecurity awareness is imperative.

II. LITERATURE REVIEW (RESEARCH DOMAINS)

A. Facts of Cybersecurity and Cyberthreats

95% of cybersecurity breaches are reported in three industries: government, retail, and technology, because they store large amounts of personally identifiable information. (Brandon Vigliarolo, 2017) Over 90% of all cyber claims are the product of human error or action, according to research. (Ross Kelly, 2017) And data breaches exposed 36 billion records in the first half of 2020 alone, not including those who were not notified. (RiskBased Security Research Team, 2020) In September 2020 alone, 9.7 million medical records were exposed. "Eighty-three breaches occurred as a result of hacking/IT incidents, exposing 9,662,820 records," according to the HIPAA Journal. A ransomware attack on Blackbaud, a cloud software business, resulted in a huge increase in data breaches. (Devon, 2020) (Steve Alder, 2020) Only 5% of businesses, on average, have their files fully safeguarded. (Rob Sobers, 2021) In addition, 45% of cyberattacks in 2020 were hacking, 17% were malware, and 22% were phishing. (Verizon, 2020) Since COVID-19, cybercrime cases have increased by 300%, according to the FBI. The rise in remote work needs a larger attention on cybersecurity due to the increasing vulnerability to cyber threats. The 47% who are mislead when working from home, for example, indicate this. Cyber criminals see this outbreak as a chance to increase their unlawful activities by exploiting work-at-home workers' susceptibility and capitalising on the public's obsession with coronavirus-related news. As a result, they had discovered 12,377 Covid-related scams by the end of the summer in 2020. (Ellen Sheng, 2020) (Jenna Walter, 2020) (Cedric Nabe, n.d.) (Tim Sadler, Jeff Hancock, Harry and Norman Chandler Professor, 2020) As for Malaysia, Cybercrime was rampant throughout the epidemic, according to Communications and Multimedia Minister Datuk Saifuddin Abdullah, with roughly 5,000 incidents submitted to the national cybersecurity agency. Between January 2021 and May 2021, 4,615 cyber security events were reported to the Cyber999 Help Center of Cyber Security Malaysia (CSM). Malicious code (256), intrusion (765), and fraud were the most common types of cases recorded (3,299). (QISHIN TARIQ, 2021) Since 2017, Malaysians have lost almost RM2.23 billion as a result of cybercrime fraud. From 2017 through June 20 this year, a total of 67,552 cybercrime cases were reported, according to police statistics. E-commerce scams were the most common, accounting for 23,011 incidents, followed by unlawful loans (21,008) and investment fraud (6,273). (Mohamed Basyir, 2021)

"Criminal action is not started by computers. The person who uses the computer is the one who is guilty of the crime." (Ross Kelly, 2017).

B. About Public Cybersecurity Awareness

Knowing and doing something to secure information assets is what cybersecurity awareness includes. When someone is cybersecurity aware, they are aware of what a cyber threat is, the potential impact of a cyberattack on their information assets, and the steps that must be taken to mitigate risk and prevent cybercrime from infiltrating their online workspace. (CyberGuard Technologies Limited, n.d.)

Malaysians' awareness of cyber security remains low, and many do not follow methods or procedures for using technology and the Internet in a positive, ethical, and responsible manner. (Luqman Arif Abdul Karim, 2021) As previously stated, the great majority of network vulnerabilities are caused by humans, and network attacks are similarly caused by humans. That's why it's important to raise public awareness of cybersecurity. Although the academic community recognises the importance of cybersecurity awareness research and it frequently appears as an important concept in research, there is no clear and systematic theoretical development lineage with a clear conceptual definition. The goal and source of cybersecurity awareness is cybersecurity, while cybersecurity risk determines the specific connotation of cybersecurity awareness. (Tian Li, Liu Ning Ning & Peng Bing Hui, 2021)

As a result, I believe it is necessary to conduct research in order to gain a more comprehensive understanding of cyber security and cyber threats, as well as to provide some effective ways to prevent cyber threats by understanding their concepts.

III. Problem Statement, Aims and Objectives

The use of the Internet is as common as breathing in today's society, but even if you know how to use it, it doesn't mean you can fully understand the dangers it poses. It is obvious that not all of us are aware of the dangers and importance of cybercrime and cybersecurity in today's society. People are negligent and tend to let down their guard on things they often use, even when they don't know how to protect themselves on the Internet.

Cyber-threats have become more common in Malaysia. According to numerous studies, online threats increased by 82.5% during the local government's Mobile Control Order (MCO) enacted in response to the global epidemic. Over 800 security incidents were reported throughout Malaysia, affecting all organisations, including those in Kuala Lumpur. According to the Malaysian Computer Emergency Response Team, cyber fraud accounted for 70% of all reported incidents from 2020 to October (MyCERT). (YUEN MEIKENG, 2020) (Malaysia Computer Emergency Response Team (MyCERT), n.d.) According to BH reporter Luqman Arif Abdul Karim's interview with Datuk Dr Amirudin Abdul Wahab, CEO of Cyber Security Malaysia (CSM), and cyber security expert Fong Choong Fook, they revealed that the general public's awareness and alertness to cyber security in Malaysia is very low. Without full knowledge and understanding of the risks associated with the Internet, the uncontrolled use of the Internet exposes the general public to various cyber threats and dangers. (Luqman Arif Abdul Karim, 2021)

Perhaps we all thought that this danger does not happen in our lives, but the truth is actually worse than we thought. From my own experience, the impact of cybercrime on those around me has been a common occurrence. The most recent incident was when my friend A lost his STEAM account due to phishing, and my friend B, who spread the phishing URL around, apparently didn't know if the URL was trustworthy and safe. The other thing that happened was that my family was upset by the perceived damage that cybercrime can do to banks and the accounts of users under their doors. These two incidents directly show the importance of cyber knowledge and the dangers of cybercrime, as well as proving that the general public is very unaware of cybersecurity. I believe this is the main reason why I need to conduct research on this topic. This research is aimed to propose effective ways to increase the public's awareness of cybersecurity. While the objective of the research is:

- To explore the level of public understanding and awareness of cybersecurity.
- To identify the relationship between the occurrence of cyber threats and the public's cybersecurity awareness.

This research aimed to raise public awareness of cybersecurity, with three main benefits: first, the public will be able to protect personally identifiable assets on their own; second, everyone in every business will be able to prevent possible future cyberattacks and avoid creating more cyber vulnerabilities; and third, cyber threats will be greatly deterred by improving the quality of public Internet use. In terms of this research's objective, first and foremost, it is hoped to obtain a thorough understanding of cyber security and cyber risks in order to reach the ideal state of enabling the general public to raise cyber security awareness on their own. The occurrence of man-made cyber vulnerabilities and cyber dangers can be reduced with sufficient information and proper ethics. Data leakage and cyber vulnerability will be decreased, and damage to people and businesses will be avoided as a result of everyone knowing how to secure their cyber assets.

IV. Methodology

A. Overall Approach

This study is divided into three major stages: the first is to consider and clarify the objectives to be achieved in this study, as well as to clarify the target respondents, research methods, and so on, which simply means to prepare for this research beforehand. The second stage is to collect various types of data for the study's topic. The third stage entails analysing the collected data, writing a report, and drawing conclusions about the research findings.

TABLE I. Overall Research Approach.

	1st Stage				2nd Stage	3rd Stage
	Initialization	**Questionnaire Development**	**Sampling (Target respondent, design)**	**Survey Conduction**	**Data Collection**	**Data Analysis & Summarization**

What to do	○ Clarify the data required for this research ○ Determine the research methods to be used in this research. ○ Estimated time required to complete this research. ○ Determine the research`s target respondents.	○ Choose the topics for this questionnaire`s content. ○ Define the questionnaire`s format and design.	○ Classification based on the feedback recipient`s information ○ Examine the questionnaire`s content. ○ Determine the sampling methods to be used.	○ Examine the questionnaire`s content, again. ○ If necessary, the questionnaire will be updated. ○ Set up an online survey platform.	○ End the survey and close the online survey platform. ○ Gather information about the research from journals and articles. ○ Consolidate and document the data that has been gathered.	○ Analyze and sort through all of the collected data. ○ Reports should be written, and information sources should be documented.
Outcome Assumed	○ Calculate the workload of this study and establish clear objectives, conditions, and methods of research.	○ The survey questionnaire`s basic design and content selection have been completed.	○ Understand the feedback provider`s data classification clearly. ○ Confirm that the questionnaire does not contain any bias or discrimination. ○ More language options for questionnaire respondents	○ The questionnaire`s final confirmation has been completed. ○ The online survey platform is ready for conducting the survey.	○ Complete the gathering of all necessary information. ○ Survey completed successfully.	○ After analysing the data, conclude about the research`s strengths and weaknesses.

B. Methodology Used

In this research, the mixed-method methodology will be used, and this includes both quantitative and qualitative research. Quantitative research is concerned with the collection and testing of numerical data, whereas qualitative research is concerned with the collection and analysis of words (written or spoken). (Derek Jansen (MBA) & Kerryn Warren (PhD), 2020) The main purpose of using quantitative research is to meet the objective of finding out the relationship between cybersecurity awareness and cyber threats, and for this type of more relevant research, coming up with data for comparison and validation is a more efficient method (Data Collection). As for qualitative research, the nature of collecting and exploring the opinions of others allows for efficient collection of perceptions and opinions from interviewers and people about cybersecurity awareness, cybersecurity, and cyber threats (Questionnaire & Sampling).

C. Questionaire Development

The main objective of the initial phase of the questionnaire is to clarify what responses and feedback the questionnaire is intended to collect. This is critical, as it will affect the accuracy and relevance of our data. The second stage is primarily concerned with the design of the questionnaire, with the selection of appropriate and clear topics being at the core of this stage. The final stage consists of final adjustments, feedback collection, and data integration; if necessary, the questionnaire will be adjusted further. The questionnaire will be carried out to ensure that the feedback is both voluntary and acceptable.

TABLE II. QUESTIONAIRE DESIGN PHASES

1st Phase	2nd Phase	3rd Phase
Initialization	**Designing**	**Conduction & Evaluation**
• Clarify the questionnaire`s aims for this research. • Determine what info we want to gather in this research questionnaire. • Determine the research questionnaire`s target group. • Determine whether the questionnaire was done in an ethical manner.	• Choose which question to answer and how to answer them in this questionnaire. • Identify and prevent bias and discrimination questions in the questionnaire`s content. • Adapting the questionnaire`s format and design	• Examine the survey`s questions and replies for appropriateness and clarity. • Examine, count, and evaluate the responses and information provided by survey participants. • Additional updates to this survey will be made if necessary.

TABLE III. QUESTIONAIRE COMPONENT TABLE

No	Component	Area Involved
1	Personal Information	Age, Gender, Education Level
2	Internet/Network Usage	Network Activities
3	Cybersecurity	Password strength, Password sharing, Browsing security, Cybersecurity knowledge, Cybersecurity awareness
4	Cyberthreats	Understanding of cyberthreats, Protection against cyberthreats, Damage from cyberthreats
5	Perspective in Cybersecurity	Interaction focused on cybersecurity
6	Perspective in Cyberthreats	Interaction focused on cyberthreats

In order to determine the general content of the questionnaire, the respondent's personal information was required first. Then, from the daily use of the Internet class, a deeper exploration and discussion on the topic of Internet security was carried out step by step. Finally, the two topics, primarily cyber security and cyber threats, were discussed openly, and respondents were asked to explain their own perspectives on them.

D. Sampling (Target respondent, Design)

The probability sampling method will be used in this study to ensure that the findings are generalizable. To meet the minimum generalizability requirement, it is expected that this study will require at least 100 (as appropriate) or more respondents. The target respondent sampling conditions for this study are not overly restrictive because probability sampling is used, but the respondent must have at least a basic understanding of the questionnaire topic.

E. Data Collection

For data collection in this study, surveys, questionnaires, browsing journals, articles, documents, and records were primarily used. Surveys and questionnaires were used to determine what respondents thought about this research topic, which is very much in line with the goal of understanding the public's perception of cyber security awareness and the concept of cyber threats. Before drawing any conclusions about the relationship between cyber security awareness and cyber threats, the data collected is expected to be consolidated and analysed using clear data charts and data collected from journals and articles.

F. Limitation

The main limitations of this research's methodology are the time constraints and the methodology itself. Due to the variety of research methods used and data to be collected, the time needed to perform and conduct data integration and analysis was relatively long and tedious. Simultaneously, as previously stated, the number of respondents required for generalizability will increase, as will the amount of data that must be sorted and filtered.

V. Overview of the Proposed System

This proposal system is outlined by collecting data and analyzing the feedback from the target respondents to achieve the objectives of this study. The completed research objectives will be analyzed and summarized again to provide effective solutions to the social situation mentioned in the study. Ideally, cyber security awareness will increase, and the incidence of cyber threats will decrease.

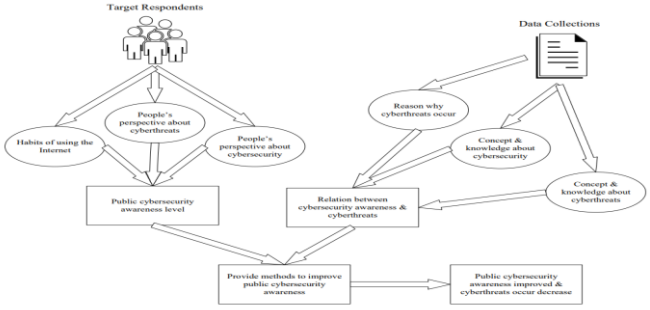

Fig. 1. Proposed System Flowchart

VI. Conclusion

This research work shows that the damage caused by cyber threats to society and public should not be underestimated. And, according to the findings of the research, the majority of cyber vulnerabilities are caused by human errors, so it is critical to raise public awareness of cyber security. Modern people's frequent online activities, associated with the pandemic, make cyber criminals more prevalent. We hope this research will provide more information about cyber security and cyber threats, as well as more useful insights to prevent and protect people from cyberattacks by cyber criminals, and to improve the quality and morality of Internet users.

References

Bernama. (2021, Jun 28). *Cyber Accidents and Crime Soar, Government Lists Cybersecurity as Top Issue*. Retrieved from malaysiakini: https://www.malaysiakini.com/news/580751

Brandon Vigliarolo. (2017, Jan 24). *Forrester: What can we learn from a disastrous year of hacks and breaches?* Retrieved from TechRepublic: https://www.techrepublic.com/article/forrester-what-can-we-learn-from-a-disastrous-year-of-hacks-and-breaches/

Cedric Nabe. (n.d.). *Impact of COVID-19 on Cybersecurity*. Retrieved from Deloitte: https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html

CyberGuard Technologies Limited. (n.d.). *The Importance of Cyber Security Awareness*. Retrieved from OGL: https://www.ogl.co.uk/the-importance-of-cyber-security-awareness

Derek Jansen (MBA) & Kerryn Warren (PhD). (2020, Jun). *What (Exactly) Is Research Methodology?* Retrieved from GRADCOACH: https://gradcoach.com/what-is-research-methodology/

Devon. (2020, Dec 23). *15 Alarming Cyber Security Facts and Stats*. Retrieved from Cybint: https://www.cybintsolutions.com/cyber-security-facts-stats/

Ellen Sheng. (2020, Jul 29). *Cybercrime ramps up amid coronavirus chaos, costing companies billions*. Retrieved from CNBC: https://www.cnbc.com/2020/07/29/cybercrime-ramps-up-amid-coronavirus-chaos-costing-companies-billions.html

Jenna Walter. (2020, May 2). *COVID-19 News: FBI Reports 300% Increase in Reported Cybercrimes*. Retrieved from IMC Grupo: https://www.imcgrupo.com/covid-19-news-fbi-reports-300-increase-in-reported-cybercrimes/

Luqman Arif Abdul Karim. (2021, May 23). *Malaysia is ready to face cyber threats*. Retrieved from BH Online: https://www.bharian.com.my/berita/nasional/2021/05/819815/malaysia-siap-siaga-hadapi-ancaman-siber

Luqman Arif Abdul Karim. (2021, May 23). *Malaysia is ready to face cyber threats*. Retrieved from BH online: https://www.bharian.com.my/berita/nasional/2021/05/819815/malaysia-siap-siaga-hadapi-ancaman-siber

Malaysia Computer Emergency Response Team (MyCERT). (n.d.). *Reported Incidents based on General Incident Classification Statistics 2020*. Retrieved from MyCERT: https://www.mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-4d11-8169-66677d694932&id=b9018870-c2a0-4b64-912d-39f65600abb8

Mohamed Basyir. (2021, Jul 16). *Malaysians suffered RM2.23 billion losses from cyber-crime frauds*. Retrieved from New Straits Times: https://www.nst.com.my/news/crime-courts/2021/07/708911/malaysians-suffered-rm223-billion-losses-cyber-crime-frauds#:~:text=According%20to%20statistics%20from%20the,investment%20scams%20with%206%2C273%20cases.

QISHIN TARIQ. (2021, Jun 3). *Saifuddin: More cybercrime reported during pandemic*. Retrieved from TheStar: https://www.thestar.com.my/tech/tech-news/2021/06/03/saifuddin-more-cybercrime-reported-during-pandemic

RiskBased Security Research Team. (2020). *2020 Q3 Report Data Breach QuickView.* 3308 W Clay St, Richmond, VA 23230, United States: Risk Based Security, Inc.

Rob Sobers. (2021, Mar 16). *134 Cybersecurity Statistics and Trends for 2021*. Retrieved from Varonis: https://www.varonis.com/blog/cybersecurity-statistics

Ross Kelly. (2017, Mar 3). *Almost 90% of Cyber Attacks are Caused by Human Error or Behavior*. Retrieved from Chief Executive: https://chiefexecutive.net/almost-90-cyber-attacks-caused-human-error-behavior/

Steve Alder. (2020, Oct 22). *September 2020 Healthcare Data Breach Report: 9.7 Million Records Compromised*. Retrieved from HIPAA Journal: https://www.hipaajournal.com/september-2020-healthcare-data-breach-report-9-7-million-records-compromised/

Tian Li, Liu Ning Ning & Peng Bing Hui. (2021, Nov 16). *A review of cybersecurity awareness research*. Retrieved from An Quan Nei Shen 安全内参: https://www.secrss.com/articles/36125

Tim Sadler, Jeff Hancock, Harry and Norman Chandler Professor. (2020, Sep 7). *Why We Click: The Psychology Behind Phishing Scams and How to Avoid Being Hacked*. Retrieved from Tessian: https://www.tessian.com/blog/why-we-click-on-phishing-scams/#:~:text=In%20a%20recent%20survey%20conducted,a%20phishing%20email%20at%20work

Verizon. (2020). *2020 Data Breach Investigation Report.* United States: Verizon.

YUEN MEIKENG. (2020, Apr 12). *Cybersecurity cases rise by 82.5%*. Retrieved from TheStar: https://www.thestar.com.my/news/focus/2020/04/12/cybersecurity-cases-rise-by-825