FACULTY OF COMPUTING

SEMESTER 2 2024/2025

UHLB2122 – PROFESSIONAL COMMUNICATION SKILLS 1

SECTION 53

INDIVIDUAL REPORT

NAME: CHUA JIA LIN

MATRIC NO: A23CS0069

GROUP: SUSHI

LECTURER: DR. NURUL NA`IMMAH BINTI HAMDAN

CYBERSECURITY THREATS INCREASES RAPIDLY DUE TO LIMITED CYBERSECURITY UNDERSTANDINGS

1.0 INTRODUCTION

Cybersecurity has become a critical issue in today's digital era, where people rely on the Internet for almost every aspect of their lives such as studying, shopping, banking, and connecting with friends and family. However, the number and complexity of cybersecurity threats are increasing as more people depend on digital technology. Rahman et al. (2020) reported that the lack of awareness about cybersecurity among users has become a big concern, while cybercriminals keep finding new ways to exploit digital weaknesses. However, many people are still unaware of how to stay online safely. Schools often ignore cybersecurity-related topics, and the public might not have easy access to clear cybersecurity guidance. As a result, society becomes more vulnerable to cybersecurity threats such as malware infections and data breaches. This report addresses this issue by examining how limited cybersecurity understanding causes the increase of online threats. It starts by discussing the cause and effect of the problem and proposes two useful solutions to solve the problem.

2.0 BACKGROUND OF THE PROBLEM

The problem's cause and effect are covered in this section.

2.1 CAUSE OF THE PROBLEM: LIMITED CYBERSECURITY EDUCATION

The reason why cybersecurity threats are increasing rapidly is due to the lack of proper education in schools. Although experts emphasize that "cybersecurity training is essential for students" (Guccione, 2025), most schools still do not include online safety in their curriculum. Without proper cybersecurity education, students are unable to identify common cybersecurity threats such as spoofing and phishing attacks. One example of a spoofing attack used in phishing scams is when students received an email that looks to be from their school, asking them to click on a link and enter their personal information (CrowdStrike, 2024). Without cybersecurity awareness, they will not doubt the authenticity of the email they received and will unknowingly

spread their personal information to cybercriminals (Hadlington, 2017). When faced with actual threats, students often panic and make bad choices because they do not have knowledge on how to handle cyber threats. Instead of reporting the email, they might continue to interact with the hackers which causes the situation to become even worse (Bada, Sasse, & Nurse, 2019).

2.2 EFFECTS OF THE PROBLEM

One effect of the problem is that uneducated users often become targets for cybercriminals. This increases the possibility that victims will become targets for cyberattacks such as phishing scams and identity theft. These attacks might cause significant financial damage and enable hackers to steal private data. For example, a successful phishing scam can compromise bank accounts or personal emails, causing emotional distress and costly recovery efforts (Anderson et al., 2019). In addition, the lack of cybersecurity awareness could also affect people on an emotional and social level. Many victims experience anxiety and lose confidence in using online services after cyber-attacks. For instance, their hesitation to use online platforms prevents them from utilizing new technologies. Because of this, people refuse to use digital tools, which slows down the adoption of new technology in society and worsens the cybersecurity issue.

3.0 POSSIBLE SOLUTIONS

This section outlines the two potential fixes for the issue.

3.1 Integrate Cybersecurity Education into School Curriculums

Integrating cybersecurity education into the school curriculum is a practical way to address the issue. This method can be done by integrating important cybersecurity topics such as phishing awareness, online safety, and digital etiquette into the Information and Communication Technology course from primary school level. At the same time, subjects like Malay and English can include cybersecurity as a discussion topic or an essay topic during examinations or daily classes (Rahman, Sairi, Zizi, & Khalid, 2020). This approach ensures that students are exposed to cybersecurity knowledge from an early age, so that they can protect themselves from cyber-attacks (Guccione, 2025). However, the disadvantage of this method is that students may not take cybersecurity seriously or may forget the lessons if they do not practice them in real life, causing the lessons to be less effective over time (Hadlington, 2017). To guarantee that students always remember cybersecurity knowledge, cybersecurity needs to be repeated and reinforced throughout their education.

3.2 Improve Accessibility of Cybersecurity Education Resources

Improving the accessibility of cybersecurity education materials is another possible solution for the growing cybersecurity threats problem. Cybersecurity resources are often written in difficult technical terms or are only accessible on particular websites that are hard for everyone to use. In order to execute this solution into real life, the government and technology companies should collaborate to translate and simplify the cybersecurity resources into easily understood language and distribute them through open-access channels such as community centers, local libraries, and social media sites like Facebook and YouTube. This approach enables more people to learn how to stay safe online, including senior citizens and those without formal education. However, this method has a drawback which is it requires user support and effective promotion of the materials, which can be expensive and time-consuming (Bada et al., 2019).

4.0 CONCLUSION

In conclusion, the rapid increase in cybersecurity threats is closely related to the general lack of awareness, especially among students and vulnerable groups. Two solutions are suggested in this report, and they are integrating cybersecurity education into the school curriculum and increasing the availability of simple and easy-to-read cybersecurity education materials. These strategies aim to provide necessary information and resources for the public so that they can learn how to protect themselves online. Collaboration between the education sector and technology providers is advised for the successful implementation of these solutions. These techniques may decrease the number of cybersecurity threat cases and foster a more cybersecurity-aware society. If these solutions are successful, people can confidently use digital technology and promote both individual and societal development.

REFERENCES

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M., Levi, M., Moore, T., & Savage, S. (2019). Measuring the cost of cybercrime. *The Journal of Cybersecurity*, 1(1), 33–49. https://doi.org/10.1093/cybsec/tyz002

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). *Cyber security awareness campaigns: Why do they fail to change behaviour?* arXiv. https://arxiv.org/abs/1901.02672

CrowdStrike. (2024). *What is a spoofing attack?* CrowdStrike. https://www.crowdstrike.com/en-us/cybersecurity-101/social-engineering/spoofing-attack/

Guccione, D. (2025, January 21). *Protecting our future: Why cybersecurity training is essential for students*. Forbes Technology Council. https://www.forbes.com/councils/forbestechcouncil/2025/01/21/protecting-our-future-why-cybersecurity-training-is-essential-for-students/

Hadlington, L. (2017). Human factors in cybersecurity: Examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon, 3*(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346

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

APPENDIX

Turnitin Report:

https://drive.google.com/drive/folders/1mfQJW42O48FNjkcrmpoVu3XPNHBjRt-D?usp=sharing