CYBERSECURITY AWARENESS TRACKER (CySAT)

Anas Rayyan Muhammad Shaifuddin[1], Amir Rayyan Muhammad Shaifuddin[2] , *Suhaily Hasnan[3], Alfiatul Rohmah Mohamed Hussain[4]

[1,2]Sekolah Kebangsaan Seksyen 9, Shah Alam, Selangor

[3,4]Faculty of Accountancy, Universiti Teknologi MARA, Shah Alam, Selangor

*Corresponding author's email: suhailyhasnan@uitm.edu.my

ABSTRACT

Cybercrime is globally disruptive and economically harmful, causing billions of dollars in financial losses and negatively impacting individuals and organisations. It threatens national security and diminishes trust in the digital economy and the internet. In this COVID-19 pandemic era, most activities have shifted from offline to online mediums, increasing malware and ransomware attacks. Previously, bullying may have occurred on school grounds. Still, currently, it happens in the cyber world, which revolves around emotions to take revenge that negatively impacts the individual involved. Thus, the CyberSecutity Awareness Tracker (CySAT) is invented purposely to measure the level of cybersecurity awareness among individuals to build a strong communications channel for addressing cyber threats. Besides, CySAT also aims to prevent the occurrence of cybercrimes by utilising the critical elements of cybersecurity to promote the importance of fighting against cybercrimes. The CySAT is beneficial to society as it promotes cybersecurity awareness and serves as a cybersecurity prevention mechanism. The CySAT is uniquely innovated to assist individuals, specifically school students who are vulnerable to such crime, to measure the level of cybersecurity awareness.

Keywords: Cybersecurity, awareness tracker, Malaysia

1. INTRODUCTION

The COVID-19 pandemic saw a shift from offline to an online medium. And, cybercriminals are getting smarter in bypassing security protocols to target their victims. Malaysian Communications and Multimedia Deputy Minister Datuk Zahidi Zainul Abidin states that the level of cybersecurity awareness among Malaysians is still low, thus, resulting in many ending up as victims of cybercrimes (The Star, 2021, June 10). Therefore, having fundamental knowledge about cybercrime and cybersecurity is vital.

Cybercrime is also known as computer crime. It involves using electronic devices as a medium to perform illegal activities, such as commutting online fraud, phishing scams, intellectual property, personal data breach, identity theft, cyber harassment, and intrusion cases like hacking and web defacements. Cybercrime fundamentally alters the nature of a traditional offline criminal act. Given the rapid growth in cybercrimes, cybersecurity awareness in Malaysia has neither received sufficient attention nor has the importance of security been investigated, especially among school students.

The internet can be a dangerous neighbourhood for everyone, but school students are incredibly vulnerable. From cyber predators to social media posts that can come back to haunt them later in life, online hazards can have severe, costly, even tragic consequences. Thus, school students must be aware of the implications and challenges of cybercrime and cybersecurity. Cybersecurity is defined as the technology implemented to protect oneself against any cybercrimes. Thus, a security issue is a cybersecurity issue involving using electronic devices, their related technology and the networked system. It functions to inflict harm, either tangible or intangible, on the victim.

It was reported that, within a period of five months (March 18 – July 31, 2020), about 3,075 cybersecurity incident reports were received by Cyber999 Help Centre, which doubled the number of incidents in the corresponding period of the year 2019 with 1,471 reports (Malay Mail, 2020, August 15). And early this year, 4,615 reports from January to May were received whereby 3,229 cases involved fraud, 765 cases due to hacking, and the remaining 256 cases implicate dangerous codes (The Sun Daily, 2021, October 6). Thus, on average, 31 cases of cybercrimes such as fraud, hacking and data breaches happen in Malaysia within 24 hours. This demonstrates an increase from the average of 29 cases a day reported to the CyberSecurity Malaysia in 2020 (Yuen, 2021). And, this situation negatively affects Malaysian socio-economic. A 2020 study by Microsoft on the cybersecurity threat landscape in the Asia Pacific revealed that cybersecurity incidents might cost the Malaysian economy a staggering RM49.15 billion, representing more than 4% of Malaysia's total Gross Domestic Product (Microsoft, 2021).

The Chief Executive Officer of CyberSecurity Malaysia, Dato' Ts. Dr. Haji Amirudin Abdul Wahab, at the launch of the first Asia Pacific Public Sector Cyber Security Executive Council, shared, "*Cybersecurity is an important national agenda that cannot rely solely on the back of the IT team. It should be a priority and responsibility of all individuals as we continue to see cyber-criminal activities rise exponentially with the proliferation of data and digital connectivity. This coalition certainly establishes stronger partnerships with industry leaders and practitioners that allow us to fortify our security postures and combat cybercrime.*" (Microsoft, 2021). It highlights the importance of individuals' awareness to react proactively and accountability towards the issue of cybercrime and cybersecurity.

And, in a live programme with Communications and Multimedia Minister, Datuk Saifuddin Abdullah, discussing cyber threats, Dato' Ts. Dr. Haji Amirudin Abdul Wahab also highlights that "*all Internet users should take responsibility for protecting themselves and increase their awareness about such threats.*" At the same programme, Intellize Tech Services Chief Strategy Officer, Dr Kavita Muthy said that cyber threats could be as or even more severe than the COVID-19 pandemic, as it could also lead to people losing their lives and businesses, besides impacting the economy (Bernama, 2021, February 4). Therefore, it is crucial to create awareness and ensure individuals are equipped with adequate knowledge on cybersecurity and always alert with the latest forms of cyber threats to uphold the responsibility of fighting against cybercrimes.

CySAT includes the critical elements of cybersecurity to encourage the environment that does not tolerate cybercrimes. Hence, the main objective of CySAT is to measure the level of cybersecurity awareness among individuals, specifically school students. By this, CySAT also aims to prevent the occurrence of cybercrimes.

2. METHODOLOGY

The CySAT used a survey approach whereby each student is required to answer a set of Likert-scale questionnaires. The accumulated marks can be immediately calculated to indicate their understanding of cybercrime and cybersecurity.

3. CONTRIBUTION AND USEFULNESS/COMMERCIALISATION

The CySAT is beneficial to society as it promotes cybersecurity awareness. Notably, the key elements included in CySAT are easily understood by the school students which help to encourage the environment that proactively fights against various types of cybercrimes. In addition, CySAT also may serve as a cybersecurity prevention mechanism since the results can be immediately obtained. The immediate results from CySAT enables school management to react efficiently and effectively. The school management must measure the level of cybersecurity awareness among the students to take proactive actions towards preventing and mitigating the occurrence of cybercrimes.

The CySAT can be commercialised to both public and private school students as it can promote cybersecurity awareness much earlier and prevent the occurrence of cybercrimes much sooner before it becomes a norm and among school students.

4. CONCLUSION

In conclusion, awareness is the key to changes. Thus, pre-occupying ourselves with the knowledge about cybercrime and cybersecurity to increase our awareness is essential to avoid being a victim. Therefore, CySAT provides the ability and promotes understanding of cybercrimes and cybersecurity, encouraging cybersecurity awareness. Tracking our awareness can help to mitigate the occurrence of cybercrimes.

ACKNOWLEDGEMENT

The authors would like to express appreciation to Universiti Teknologi MARA, Shah Alam, Selangor for funding the research project through the grant [600-RMC/GPK 5/3 (078/2020)]. Our appreciation also goes to the Sekolah Kebangsaan Seksyen 9, Shah Alam, Selangor for facilitating this research project.

REFERENCES

Bernama, (2021, February 4). CSM: Cyberthreats under check in Malaysia. The New Straits Times. Retrieved from https://www.nst.com.my/news/nation/2021/02/662961/csm-cyber-threats-under-check-malaysia

Malay Mail, (2020, August 15). Communication Ministry: Over 100pc Rise in Cybersecurity Incidents since Covid-19 Outbreak. Malay Mail. Retrieved from https://www.malaymail.com/news/malaysia/2020/08/15/communications-ministry-over-100pc-rise-in-cybersecurity-incidents-since-co/1894253

Microsoft. (2021, May 31). Microsoft Launches First Asia Pacific Public Sector Cyber Security Executive Council across Seven Markets in the Region. Retrieved from https://news.microsoft.com/apac/2021/05/31/microsoft-launches-first-asia-pacific-public-sector-cyber-security-executive-council-across-seven-markets-in-the-region/

The Star, (2021, June 10). Cybersecurity Awareness Still Low among Malaysians, says Comms Dep Minister. The Star. Retrieved from https://www.thestar.com.my/news/nation/2021/06/10/cyber-security-awareness-still-low-among-malaysians-says-comms-dep-minister

The Sun Daily, (2021, October 6). Cyber Security Awareness Still Low Among Malaysians – Zahidi. The Sun Daily. Retrieved from https://www.thesundaily.my/local/cyber-security-awareness-still-low-among-malaysians-zahidi-EG7954547

Yuen, M., (2021, September 19). Online Threats Continue to Spike. The Star. Retrieved from https://www.thestar.com.my/news/focus/2021/09/19/online-threats-continue-to-spike