Jurnal Pengabdian Masyarakat: Bisnis dan Iptek
Vol. 2 No. 1, May 2025, 01-11
ISSN Online: 3064 - 0415 X, https://doi.org/10.56447/jpmbistek
Published by LPMM, STMIK Mardira Indonesia, Bandung.

Cyber Security Survival Kit "Generation Z's Digital Survival Strategies"

Cahyo Hermanto[1], Sarah Azhar[2] , Septi[3], Yunisva[4], Siti Dini[5], Novi[6], Adel[7],Salsabilal[8],Risma[9], Rismawati[10], Ai Fitri[11], Arie[12]
[1,2,3,4,5,6,7,8,9,10,11] STMIK Mardira Indonesia, Bandung
*Email: cahyo.hermanto@stmik-mi.ac.id**

Abstract

The community service initiative, featuring academics and students from STMIK Mardira Indonesia, occurred at MA Persis Katapang to improve digital literacy, specifically in cybersecurity for Generation Z. The swift advancement of information technology yields advantages while simultaneously presenting numerous cyber risks, particularly to young people engaged in the digital realm. This curriculum seeks to provide students with the information and abilities necessary to identify, evade, and address cyber threats via the "Cyber Security Survival Kit" module. The employed methods consist of a blend of seminars, practical workshops, and interactive simulations. The outcomes of this activity demonstrated an enhancement in participants' comprehension of internet security protocols, password management, phishing threat recognition, and digital identity safeguarding. This program raises awareness of the importance of cybersecurity and promotes safe digital practices among students.

Keywords: *Cyber Security, Digital Literacy, Generation Z, Cyber Threats, Digital Safety*

Introduction

The advancement of information and communication technology (ICT) has revolutionized nearly every facet of human existence, encompassing our interactions, learning, employment, and socialization. Young individuals, especially those belonging to Generation Z, are the demographic most impacted by this digital transition. This generation was born and nurtured in a period of swift technological progress, rendering digital devices, social media, and internet connectivity integral components of their everyday existence.

Nevertheless, the swift integration of digital technology has not consistently led to a heightened understanding of cybersecurity. Although Generation Z is composed of digital natives, their comprehension of online hazards and threats remains limited. This phenomenon is manifested in the increasing incidents of personal data theft, social media account hacking, online fraud (phishing), virus dissemination, and cyberbullying, with numerous adolescents being victims.

A 2022 poll by the Ministry of Communication and Informatics (Kominfo) revealed that more than 60% of Indonesian adolescents lack a comprehensive understanding of the adequate protection of their personal data. Moreover, around 55% of individuals are unable to recognize the indicators of phishing messages or links that could compromise personal information. A report from the National Cyber and Encryption Agency (BSSN) documented almost 1.6 billion traffic anomalies as signs of probable cyber assaults in Indonesia throughout 2022.

This situation reveals a substantial disparity between the youth's technological proficiency and their capacity to safeguard themselves against cyber risks. Lack of knowledge about account security, personal information management, and digital ethics can lead to significant repercussions, affecting both people and the broader security of the digital community.

Various measures previously adopted to improve digital literacy among pupils encompass public seminars, social media initiatives, and

restricted training about media ethics. Nonetheless, these methodologies are predominantly unidirectional, less engaging, and deficient in actual implementation. Consequently, a more complete and pragmatic strategy is required that matches the learning traits of Generation Z, which is characterized by activity, interactivity, and visual engagement.

The strategy based on the Cyber Security Survival Kit is intended to fulfill this requirement. This curriculum delivers content in both theoretical and practical formats, including simulations, role-playing, case studies, and experiential practice in addressing diverse cyber risks. Consequently, participants comprehend digital security ideas both conceptually and in practical application within their regular digital endeavors.

A study of multiple prior studies, including the research of Sidharta & Rahmahwati (2023) on user satisfaction with information systems, indicates that technological literacy is intrinsically linked to the degree of security and comfort in utilizing digital services. Manik et al. (2023) assert that enhancing quality management competencies, particularly in digital security, substantially influences the quality and reliability of the used systems.

Nevertheless, the majority of current digital literacy initiatives emphasize commercial, industry, or higher education contexts, neglecting the implementation of cybersecurity literacy in secondary school, especially among madrasa students. Contemporary curricula prioritize the integration of technology and digital ethics but fail to concentrate on imparting the technical skills necessary for students to confront cyber risks effectively. By attaining this objective, we aspire for students to evolve into persons who are not only technologically proficient but also acutely cognizant of security and ethical considerations in the utilization of digital technology.

Method

This community service initiative employs a qualitative methodology utilizing a case study approach, aimed at improving digital literacy through

practical engagement in educational environments. This activity is designed collaboratively, integrating active learning methodologies that correspond with the learning traits of Generation Z.

1. **Activity Design**

   The activity design pertains to the Participatory Action Research (PAR) model, which designates participants as active agents in the learning process. We execute the activities through direct education employing a blend of lectures, question and answer sessions, practical demonstrations, and interactive presentation tools. The primary emphasis is on delivering content that is relevant and comprehensible, while also facilitating participants' direct application in their digital lives.

2. **Population and Sample**

   The participants in this exercise are students from MA Persis Katapang. Participants are selected purposefully based on school recommendations, taking into account the pupils' active engagement with digital technology and their requirement for improved comprehension of cybersecurity.

3. **Data Collection Techniques and Instruments**

   Data is gathered by direct observation of participants' interaction during activities, particularly during demonstration and interactive discussion sessions. The facilitator observes the students' proficiency in recognizing digital dangers, implementing security settings, and reacting to simulated cyber threats.

   a. The tools employed consist of an observation guide featuring indicators such as: a. Comprehension of fundamental cybersecurity principles.
   b. Response to digital threat scenarios, such as phishing.
   c. Capability to generate robust and secure passwords.
   d. Engaged in discussions and question-and-answer sessions.

4. Teaching Methods

Throughout the engagement, the facilitator employs many complementary learning methodologies, specifically:

a. Lecture: A succinct and targeted presentation of content designed to furnish participants with a fundamental comprehension.
b. Q&A: A transparent dialogue between participants and the facilitator to enhance comprehension of the content.
c. Demonstration: Practical engagement in account security configurations, phishing recognition, and personal data safeguarding.
d. Interactive Presentation (PPT): A visual exposition utilizing graphics, animations, and actual case studies to engage the audience and enhance comprehension.
e. Data Analysis Technique: The collected observational data are evaluated descriptively and qualitatively, categorizing the results into conceptual knowledge, technical skills, and attitudinal changes. The analysis employs a thematic methodology centered on the attainment of learning indicators.
f. Location and Duration of the Activity: The event is held in the auditorium of MA Persis Katapang for an entire day. The event sequence comprises an opening, content presentation, interactive sessions, practical demonstrations, and a concluding reflection.

Results and Discussion

The execution of the community service initiative at MA Persis Katapang, concentrating on digital literacy and cybersecurity, produced substantial outcomes in improving participants' comprehension of personal data protection principles and online risks. Direct observations during the activity revealed that

participants demonstrated heightened involvement, enthusiasm, and a deeper comprehension of the material conveyed through demonstrations and hands-on practice.

A primary finding of this activity is the enhancement of participants' capacity to recognize potential digital hazards, including phishing, inadequate password practices, and the dangers of indiscriminately disclosing personal information. The participants' success in addressing realistic cyber threat scenarios during the demonstration sessions is clearly apparent. Prior to acquiring this knowledge, the majority of participants were oblivious to the fact that dubious connections or solicitations for information from unfamiliar sources could provide significant risks. After the demonstrations and interactive conversations, students were able to identify and propose suitable preventive measures. Furthermore, participants demonstrated an enhanced comprehension of utilizing privacy settings on social media, employing two-factor authentication (2FA), and recognizing the significance of preserving digital identity confidentiality. This corresponds with the program's principal objective of fostering the cultivation of secure and responsible digital conduct.

These findings address the primary inquiry of this activity: how to enhance students' knowledge and competencies in addressing cyber threats through a practical methodology. This activity illustrates that participatory learning techniques, incorporating lectures, Q&A sessions, demonstrations, and interactive presentations, can effectively engage Generation Z's visual, interactive, and responsive learning preferences through direct encounters.

The results further suggest that digital literacy cannot be enhanced exclusively through theoretical methods. Pragmatic, contextual methodologies provide more efficacy in enhancing students' understanding and competencies in the application of cybersecurity principles in their everyday lives.

This action indicates that cybersecurity education for younger age groups should be developed using active, problem-based, and experiential learning methodologies. Initiatives such as the "Cyber Security Survival

Kit" function as pertinent and contextual educational frameworks, connecting digital security theory with its practical implementation in daily life.

Figure 1. Community Service Group

Figure 2. Community Service Activities

Figure 3. Community Service Activities

Figure 4. Community Service Activities

Conclusion

The community service initiative at MA Persis Katapang effectively accomplished its primary goal: improving students' comprehension and practical abilities in addressing cyber dangers via an interactive and contextual learning methodology. Through lectures, live demonstrations, Q&A sessions, and interactive presentation media, participants comprehended fundamental cybersecurity ideas and implemented them in their daily digital practices.

The results of this activity demonstrate that experiential learning is far more effective in cultivating digital literacy than solely theoretical methods. The Cyber Security Survival Kit learning paradigm has demonstrated a beneficial effect on fostering safe and responsible digital conduct, especially among the younger generation immersed in a wholly digital environment.

This activity enhances digital literacy education methods at the secondary level, which relevant cybersecurity literacy initiatives have insufficiently addressed. This study underscores the significance of

experiential learning methodologies in digital literacy and technology security, highlighting the necessity for the creation of educational resources that correspond with the traits of Generation Z.

In the future, programs of this nature can be duplicated and extended to other educational institutions with adjustments to address local requirements. Subsequent advancement may concentrate on incorporating cybersecurity curriculum into ICT or Pancasila Education courses, with the employment of more adaptive digital media, like instructional games, online simulations, or project-based learning.

Collaboration among educational institutions, government, and the technology sector is vital to establishing a robust cybersecurity education ecosystem. Furthermore, subsequent activities may be implemented to assess the enduring efficacy of this experiential learning method in cultivating safe digital practices among students.

References

Sidharta, I., & Rahmahwati, R. (2023). Cross Sectional Study on Information System Facilities on End-User Satisfaction: Study at Retail in Bandung. Electronic, Business, Management and Technology Journal, 1(1), 1–11. https://doi.org/10.55208/ebmtj.v1i1.81

Manik, E., Sidharta, I., Coenraad, D. P., Komara, A. T., Satria, R. O., & Riadi, F. (2023). Assessing total quality management and its impact on product quality: A cross-sectional study on textile industries in Bandung, Indonesia. International Journal of Applied Economics, Finance and Accounting, 15(2), 71–79. https://doi.org/10.33094/ijaefa.v15i2.820

Sari, P. R., & Nugroho, E. (2020). Digital Literacy and Its Impact on Online Learning during the COVID-19 Pandemic. Jurnal Teknologi dan Pendidikan, 9(2), 101–110.

Prasetyo, A. R., & Firman, F. (2021). Understanding the Digital Behavior of Generation Z in Indonesia. Indonesian Journal of Communication Studies, 14(1), 45–57.

Kurniawan, D., & Wulandari, A. (2022). Analisis Literasi Digital Pelajar dalam Menghadapi Ancaman Siber. Jurnal Komunikasi dan Teknologi Informasi, 6(1), 25–35.

Fitriyani, L., & Syamsuddin, M. (2022). Pengaruh Literasi Keamanan Digital terhadap Perilaku Aman Pengguna Internet. Jurnal kegiatan dan Pengabdian Masyarakat, 3(2), 113–121.

Kominfo. (2022). Survei Nasional Literasi Digital 2022. Kementerian Komunikasi dan Informatika Republik Indonesia. https://literasidigital.id/

Badan Siber dan Sandi Negara. (2022). Laporan Statistik Keamanan Siber Indonesia Tahun 2022. https://bssn.go.id/

Hapsari, R., & Setiawan, H. (2019). Penerapan Model Pembelajaran Interaktif dalam Meningkatkan Literasi Digital Siswa SMA. Jurnal Pendidikan Teknologi Informasi dan Komunikasi, 3(1), 12–21.

Nugroho, A. S., & Harahap, N. (2021). Cyber Security Awareness among High School Students in Indonesia. Journal of Cyber and Education Technology, 5(2), 80–89.

Taufik, M., & Novitasari, S. (2023). Implementasi Pembelajaran Berbasis Proyek dalam Edukasi Siber untuk Siswa. Jurnal Ilmu Pendidikan dan Teknologi, 4(1), 67–74.

Wijayanti, R. N., & Latifah, N. (2020). Analisis Kompetensi Literasi Digital Generasi Z pada Lingkungan Pendidikan Islam. Jurnal Pendidikan Islam, 8(2), 144–158.

Nasution, R. A., dkk. (2018). Strategi Edukasi Keamanan Siber Berbasis Kelas Digital. Prosiding Seminar Nasional Teknologi Informasi dan Komunikasi, 1(1), 53–60.

Damayanti, M., dkk. (2023). Peningkatan Kesadaran Keamanan Siber melalui Simulasi Praktik di Sekolah Menengah. Jurnal Pengabdian Masyarakat Digital, 2(1), 22–29.

Yuliana, S., & Rahmadani, F. (2017). Digital Natives dan Tantangan Literasi Siber. Jurnal Sosial Humaniora, 10(2), 95–104.