Jurnal Layanan Masyarakat (*Journal of Public Services*), Vol. **9** No. **2** Tahun **2025**, halaman **204–214**
ISSN 2580-8680, e-ISSN 2722-239X

IMPROVING AWARENESS OF INTERNET SECURITY AND ETHICS AMONG STUDENTS AT SMA NEGERI 2 MRANGGEN

MENINGKATKAN KESADARAN ETIKA DAN KEAMANAN INTERNET PADA SISWA SMA NEGERI 2 MRANGGEN

Muhammad Naufal[1], **Novianto Nur Hidayat**[1,2], **Gustina Alfa Trisnapradika***[1,2], **Harun Al Azies**[1,2]

*[1] Study Program in Informatics Engineering, Faculty of Computer Science, Universitas Dian Nuswantoro
[2] Research Center for Quantum Computing and Materials Informatics, Faculty of Computer Science, Universitas Dian Nuswantoro

*e-mail: gustina.alfa@dsn.dinus.ac.id

Abstract

This community service initiative aimed to enhance the awareness of internet security and ethics among high school students at SMA Negeri 2 Mranggen, Demak Regency, Central Java. The program utilized a structured methodology consisting of outreach, training, and evaluation stages conducted in a hands-on environment within the school's computer laboratory. The training covered key topics such as data security, phishing attacks, malware, and ethical internet use. The sessions were held in the school's computer laboratory to provide hands-on experience. Each training session had a duration of 3×45 minutes, attended by 31 students, allowing comprehensive exploration of the material. Pre- and post-tests were administered to assess the effectiveness of the training. The results demonstrated a significant improvement in students' knowledge, with average scores increasing from 49 in the pre-test to 72.67 in the post-test. A paired t-test analysis confirmed this improvement as statistically significant, with a T-statistic of -13.971 and a P-value of 2.07 × 10-14. The findings highlight the program's success in raising awareness and equipping students with the skills to navigate the digital world safely and responsibly. This initiative underscores the importance of educational programs in fostering internet literacy and security awareness among young users. To build on these findings, it is recommended that similar training sessions to be conducted regularly to reinforce the concepts learned. Additionally, a long-term plan is proposed as a form of sustainability of this community service program, namely by expanding the training targets not only to students but also to teachers, housewives and children who are already accustomed to gadgets.

***Keywords**: Internet Security; Digital Ethics; Technology Education.*

Abstrak

Pengabdian kepada masyarakat ini bertujuan untuk meningkatkan kesadaran akan keamanan internet dan etika penggunaan internet di kalangan siswa SMA Negeri 2 Mranggen, Kabupaten Demak, Jawa Tengah. Program ini menggunakan metode yang terstruktur yang terdiri dari tahap sosialisasi, pelatihan, dan evaluasi, yang dilakukan dalam lingkungan praktis di laboratorium komputer sekolah. Pelatihan mencakup topik-topik utama seperti keamanan data, serangan phishing, malware, dan etika penggunaan internet. Sesi pelatihan diadakan di laboratorium komputer sekolah untuk memberikan pengalaman langsung. Setiap sesi pelatihan berlangsung selama 3×45 menit dan diikuti oleh 31 siswa, sehingga

Received 8 December 2024; Received in revised form 19 May 2025; Accepted 21 May 2025; Available online 19 June 2025.

10.20473/jlm.v9i2.2025.204-214

memungkinkan eksplorasi materi secara menyeluruh. Tes awal dan tes akhir dilakukan untuk menilai efektivitas pelatihan. Hasilnya menunjukkan peningkatan signifikan dalam pengetahuan siswa, dengan rata-rata skor meningkat dari 49 pada tes awal menjadi 72,67 pada tes akhir. Analisis uji t-berpasangan mengonfirmasi peningkatan ini sebagai hasil yang signifikan secara statistik, dengan nilai T-statistik sebesar -13,971 dan P-value sebesar 2,07 × 10^-14. Temuan ini menyoroti keberhasilan program dalam meningkatkan kesadaran dan membekali siswa dengan keterampilan untuk menjelajahi dunia digital secara aman dan bertanggung jawab. Inisiatif ini menegaskan pentingnya program pendidikan dalam membina literasi dan kesadaran keamanan internet di kalangan pengguna muda. Berdasarkan pada keberhasilan program ini, sesi kegiatan serupa perlu diadakan secara berkala untuk menguatkan konsep-konsep yang sudah dipelajari. Selain itu, sebuah rencana jangka panjang diusulkan sebagai bentuk keberlanjutan dari program pengabdian masyarakat ini, yaitu dengan memperluas target pelatihan tidak hanya kepada siswa tetapi juga kepada guru, ibu rumah tangga, dan anak-anak yang sudah terbiasa dengan gadget.

***Kata kunci**: Keamanan Internet;Etika Digital; Pendidikan Teknologi.*

INTRODUCTION

The rapid development of information technology has transformed the way we interact, learn, and share information (Dakhi et al., 2020; Iivari et al., 2020; Szymkowiak et al., 2021). For the younger generation, the internet has become not only a communication tool but also an endless source of knowledge (Faik et al., 2020; Loos & Ivan, 2024). However, some significant challenges arise alongside this convenience, i.e., concerning security and ethics in internet usage (Moradi, 2021). Indonesian Cyber and Crypto Agency (BSSN) reports a notable increase in cybercrime case, where teenagers often fall victim to various forms of online fraud and data theft (Khoirunnisa & Jubaidi, 2024; Triwahyuni et al., 2024; Yusup, 2022). This phenomenon underscores the importance of a deep understanding of how to protect oneself in the digital world (Krishna et al., 2023).

At SMA Negeri 2 Mranggen in Demak Regency, Central Java, these challenges are increasingly felt. Preliminary research indicates that students have a limited understanding of data security and internet usage ethics. The average value calculated from 31 students is 49 points, with the individual score ranged from 30 to 80. The pre-test was conducted by providing 5 basic questions regarding the concept of cyber security, tools in preventing digital attacks and several social media that are vulnerable to attack by hackers. This community service activity will focus on assessing students' knowledge regarding computerization and data security before and after the training, as well as their perceptions of internet ethics and the cyber threats they may encounter. Given this context, the primary aim of the community service activity is to raise students' awareness of the importance of security and ethics in the digital realm. Specific objectives include enhancing students' basic knowledge about computerization, hardware, and software that supports internet usage; providing a practical understanding of cyber threats, particularly phishing techniques, and the steps to protect themselves; and fostering responsible attitudes in the online world, such as respecting others' privacy and avoiding harmful behavior.

To support this activity, a comprehensive literature review has been conducted, encompassing various references related to internet security and ethics. Research by AlShabibi and Al-Suqri (2021) demonstrates that education on cybersecurity can significantly reduce the risk of cyber-attacks among teenagers (AlShabibi & Al-Suqri, 2021). Similarly, a study by Alsobeh et al. (2023) emphasizes that a better understanding of digital ethics can encourage responsible behavior among internet users (Alsobeh et al., 2023). At the local level, findings indicate that students in this region often become victims of cyber-attacks due to insufficient knowledge of effective protection measures. This training program is designed to fill that knowledge gap and enhance students' awareness of cybersecurity (Sari et al., 2020).

SMA Negeri 2 Mranggen has considerable potential for human resource development, yet challenges regarding access to adequate information technology education persist. The internet infrastructure in this region is developing, but some areas remain underserved. Most students come from lower-middle socioeconomic backgrounds, highlighting an urgent need to strengthen their digital skills to better prepare them for the demands of the digital era. Through this community service activity, students are expected to gain not only theoretical knowledge but also practical skills to help them protect themselves in the digital world. By involving the community and receiving support from the school, this program aims to empower students to face the challenges of the digital era and prepare them to become smart and responsible internet users.

COMMUNITY SERVICE METHOD

This community service initiative employed a structured and systematic approach to raise awareness about internet security and ethics among 31 students at SMA Negeri 2 Mranggen, Demak Regency, Central Java. The program was conducted on Friday, August 23, 2024, in the school's computer laboratory, providing a hands-on environment to enhance student engagement. The methodology included three main stages: outreach, training, and evaluation, each designed to progressively build students' understanding of digital security concepts. Behind the success of increasing students' knowledge of the importance of internet security, there are obstacles faced by the service team, namely limited space which causes only 31 students to be able to receive education and training. In the future, the service team will strive to be able to facilitate training for a larger number.

Outreach Method

The initial stage of the program involves outreach activities designed to establish a foundational understanding of computerization, data security, and internet usage ethics. This phase includes interactive presentations complemented by group discussions, encouraging active participation. The sessions are led by a team of community service volunteers with expertise in information technology and cybersecurity, ensuring that the concepts are conveyed effectively and are accessible to the students.

Training Method

Building upon the outreach phase, a comprehensive training session is conducted to delve deeper into the subject matter. This training encompasses practical demonstrations of various cyber threats, particularly phishing, alongside techniques for safeguarding personal data. Students engage in hands-on simulations of phishing attacks (Scherb et al., 2023), which allows them to witness firsthand the potential risks and learn effective protective measures. This interactive approach fosters a more engaging learning environment, enhancing their understanding and retention of the material.

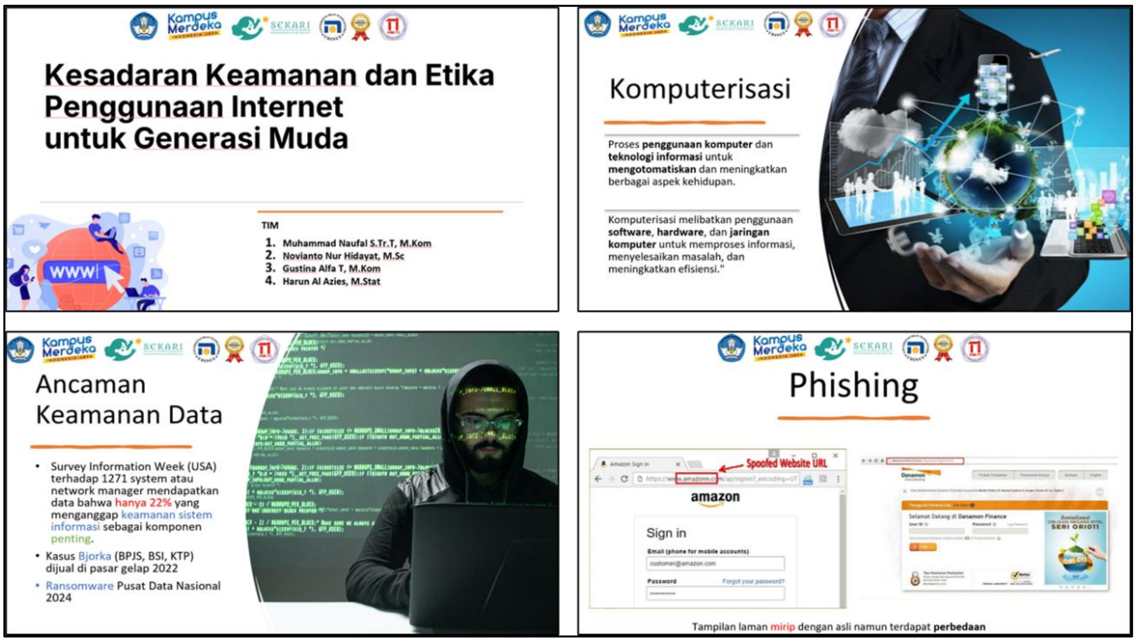
The second stage comprised comprehensive training sessions focusing on real-world cybersecurity threats, including phishing, malware, and personal data protection. Hands-on simulations were conducted to reinforce theoretical knowledge and provide practical skills for identifying and mitigating online threats. Each training session lasted for 3 × 45 minutes, providing sufficient time for students to explore the material in depth. Students were encouraged to participate in interactive exercises, including phishing email simulations, to enhance their understanding.

Measurement of Achievement

To evaluate the effectiveness of the community service activities, pre-test and post-test assessments are utilized. The pre-test is administered prior to the training to gauge students' baseline knowledge concerning internet security and ethics. Following the training, the post-test is conducted to measure any advancements in their understanding and awareness (Mishra et al., 2019; Naufal & Azies, 2024). The assessment tools consist of questionnaires featuring both closed and open-ended questions. These instruments are carefully crafted to assess students' comprehension of the taught concepts, their attitudes towards cybersecurity, and their grasp of ethical practices in internet usage. The responses gathered from these questionnaires undergo both descriptive and quantitative analysis. Subsequent to the data collection from pre-test and post-test assessments, statistical analysis is conducted using the t-test (Liu & Wang, 2021; Mishra et al., 2019; Muljono et al., 2024). This analysis aims to determine whether there is a statistically significant difference in students' knowledge before and after the training. Specifically, the t-test assesses if the increase in post-test scores in comparison to pre-test scores is significant, indicating the effectiveness of the training program (Liu & Wang, 2021; Naufal & Azies, 2024; Winarno & Azies, 2024). By employing this structured and systematic methodology, it is anticipated that the outcomes of this community service initiative will yield a significant positive impact on the students and the wider community surrounding SMA Negeri 2 Mranggen.

RESULTS AND DISCUSSIONS

The community service activity was successfully conducted in the computer laboratory of SMA Negeri 2 Mranggen, where 31 students eagerly participated. The focus of the session was to provide the students with in-depth knowledge about internet security and ethics, addressing critical issues they are likely to face in today's increasingly digital world. Conducting the session in the computer lab allowed for a hands-on, interactive learning environment that facilitated deeper engagement with both the material and the technological aspects. The session began with a dynamic and engaging introduction by the team, designed to capture the students' attention and emphasize the relevance of internet security in their daily lives. The discussion included prevalent threats such as identity theft, online scams, phishing, malware, and cyberattacks. To make the subject matter more relatable and impactful, relevant statistics were presented, showcasing real-world consequences for individuals and communities. This helped the students grasp the importance of protecting their personal data and the ethical responsibilities that come with internet use.



Kesadaran Keamanan dan Etika Penggunaan Internet untuk Generasi Muda

TIM

1. Muhammad Naufal S.Tr.T, M.Kom
2. Novianto Nur Hidayat, M.Sc
3. Gustina Alfa T, M.Kom
4. Harun Al Azies, M.Stat

Komputerisasi

Proses **penggunaan komputer** dan **teknologi informasi** untuk **mengotomatiskan** dan meningkatkan berbagai aspek kehidupan.

Komputerisasi melibatkan penggunaan **software**, **hardware**, dan **jaringan komputer** untuk memproses informasi, menyelesaikan masalah, dan meningkatkan efisiensi."

Ancaman Keamanan Data

- Survey Information Week (USA) terhadap 1271 system atau network manager mendapatkan data bahwa hanya 22% yang menganggap keamanan sistem informasi sebagai komponen penting.
- Kasus Bjorka (BPJS, BSI, KTP) dijual di pasar gelap 2022
- Ransomware Pusat Data Nasional 2024

Phishing

Tampilan laman mirip dengan asli namun terdapat **perbedaan**

Figure 1. Training Material on Internet Security and Ethics.

Figure 1 presents the slide materials used during the session, which featured a combination of visuals, infographics, and key points to explain internet security topics in a clear and engaging way. These slides covered various aspects of online safety, including how to recognize phishing attempts, secure passwords, and ethical behaviors when using the internet. The visual content was designed to keep the students' attention while reinforcing the importance of adopting safe online practices. The material presentation (as shown in Figure 1) played a crucial role in delivering key messages. Each slide was visually compelling, with clear text and diagrams to explain complex concepts. For example, one of the slides highlighted a step-by-step guide to spotting phishing emails, which included annotated screenshots showing typical features of fraudulent messages. Additionally, videos demonstrating real-world cyberattack scenarios were embedded within the slides, giving the students a practical understanding of how these threats occur and how to avoid them.

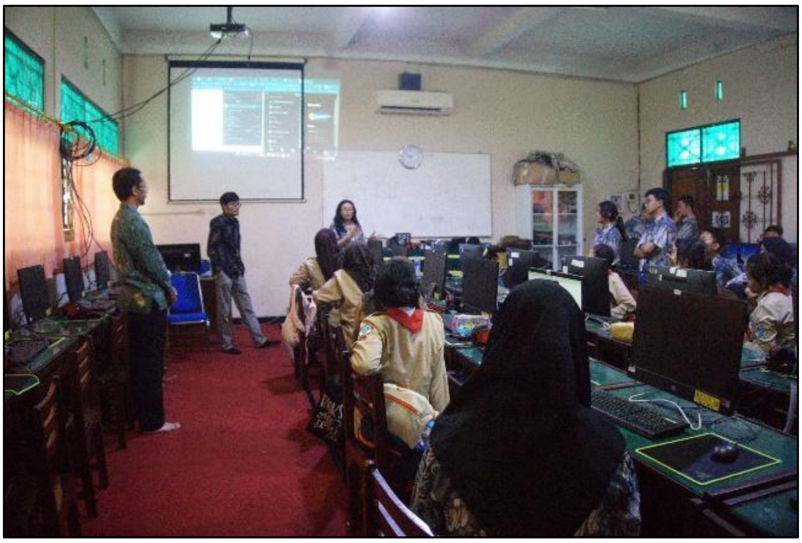


Figure 2. Training Workshop on Internet Security and Data Protection.

After the introduction, the team conducted an interactive workshop in the computer laboratory, where students engaged with the material through visually rich slides and informative videos. The content of the training was designed to break down complex topics such as data security and privacy into digestible concepts. The workshop introduced students to the basics of computing, including hardware and software, while focusing on more advanced topics like safeguarding personal information in the digital realm. The students were guided through the identification of cyber threats such as phishing, malware, and hacking, along with practical methods to counter these risks. For instance, they were taught how to create secure passwords, identify phishing attempts, and navigate online privacy settings, as shown in Figure 2, which illustrates the key topics and resources used during the workshop.

Figure 3. Interactive Q&A Session during the Community Service Workshop.

Following the workshop, the team facilitated an interactive Q&A session to foster a deeper understanding of the material presented. This segment encouraged students to actively engage by asking questions and discussing the topics covered, creating an inviting atmosphere that promoted open dialogue. From the results of this interactive Q&A, it is also known that most of students are starting to become aware of the vague links that are usually used for phishing, so it can be concluded that basically the participants are becoming aware of how phishing occurs on their social media. As shown in Figure 3, students enthusiastically shared their personal experiences related to internet use, with many contributing their thoughts and insights. This interaction not only clarified doubts but also strengthened the community bond among the participants, making the session more effective in achieving its educational goals.

Figure 4. Simulation of Phishing Attacks and Illustrative Examples of Phishing Tactics.

A key highlight of the session was a demonstration illustrating how phishing attacks function. The service team organized a simulation in the computer laboratory that vividly showcased the tactics employed by cybercriminals. During this demonstration, students analyzed how these attacks occur and examined examples of seemingly legitimate phishing emails, as illustrated in Figure 4. This hands-on experience provided students with valuable insights into the risks they may encounter online, enabling them to recognize deceptive messages and equipping them with practical strategies to protect themselves from such threats.

To assess the effectiveness of the training, the team implemented a thorough evaluation process using pre-tests and post-tests. Before the workshop began, students completed a pre-test to gauge their initial knowledge of internet security and ethics. This assessment included various questions that covered key topics to be addressed during the training. Once the workshop concluded, students took a post-test to evaluate their understanding after the training.

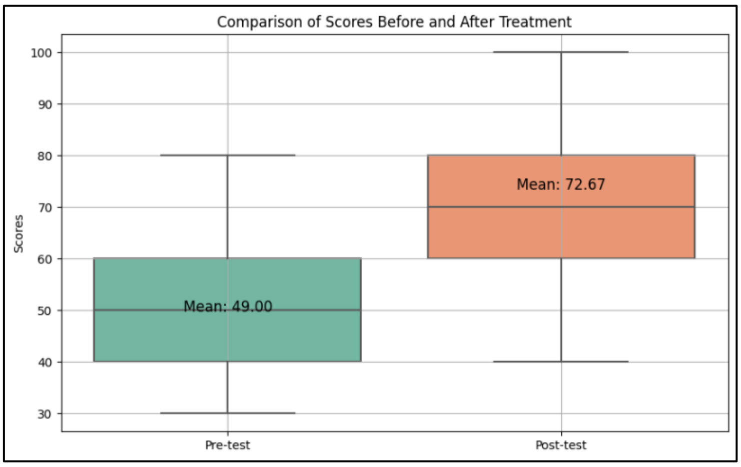


Figure 5. Box Plot Illustrating Pre-Test and Post-Test Scores.

The results were promising. The analysis revealed that the average score from the pre-test was 49, indicating a limited initial comprehension of the issues at hand. However, after the comprehensive training, the post-test results showed a significant improvement, with the average score rising to 72.67. To visually illustrate these findings, a box plot demonstrates a marked increase in performance among the students. This plot reveals that the majority of students displayed notable progress after the training, indicating not only a rise in average scores but also a larger number of students achieving higher scores in the post-test compared to the pre-test, as shown in Figure 5.

Table 1. Summary of Paired T-Test Results.

T-statistic	P-value
-13.971	2.0709×10^{-14}

To further validate these results, a paired t-test was conducted. The statistical analysis yielded a T-statistic of -13.9706 and a remarkably low P-value of 2.0709 × 10-14, as summarized in Table 1. This P-value, which is significantly below the conventional threshold of 0.05, clearly indicated a substantial difference between the pre-test and post-test scores. Thus, the training proved to be highly effective in enhancing students' knowledge of internet security and ethics. Therefore, a long-term plan was proposed as a form of sustainability of this community service program, namely by expanding the training targets not only to students but also to teachers, housewives and children who are already accustomed to gadgets.

CLOSING

Conclusion. The community service initiative significantly enhanced the awareness of internet security and ethics among students at SMA Negeri 2 Mranggen. The training effectively improved students' knowledge, as demonstrated by the notable increase in average test scores. This outcome aligns with the initiative's objective to equip students with essential skills for navigating the digital landscape safely. To build on these findings, it is recommended that similar training sessions be conducted regularly to reinforce the concepts learned.

Suggestions. Integrating internet security education into the school curriculum can ensure broader coverage for all students. Engaging parents and educators in future initiatives could further strengthen community awareness and foster a culture of cybersecurity.

ACKNOWLEDGEMENT

The authors would like to express their gratitude to the Research and Community Service Institute of Dian Nuswantoro University for their support in the implementation of this community service activity. Special thanks are also extended to the Principal of SMA Negeri 2 Mranggen for facilitating this program, as well as to the students of SMA Negeri 2 Mranggen who actively participated in the application of science and technology during the community service activity.

REFERENCES

AlShabibi, A., & Al-Suqri, M. (2021). Cybersecurity awareness and its impact on protecting children in cyberspace. *2021 22nd International Arab Conference on Information Technology, ACIT 2021*. https://doi.org/10.1109/ACIT53391.2021.9677117

Alsobeh, A. M. R., Alazzam, I., Shatnawi, A. M. J., & Khasawneh, I. (2023). Cybersecurity awareness factors among adolescents in Jordan: Mediation effect of cyber scale and personal factors. *Online Journal of Communication and Media Technologies*, *13*(2), e202312. https://doi.org/10.30935/OJCMT/12942

DAKHI, O., JAMA, J., IRFAN, D., AMBIYAR, & ISHAK. (2020). BLENDED LEARNING: A 21ST CENTURY LEARNING MODEL AT COLLEGE. *INTERNATIONAL JOURNAL OF MULTI SCIENCE*, *1*(08), 50–65. https://multisciencejournal.com/index.php/ijm/article/view/92

Faik, I., Barrett, M., & Oborn, E. (2020). How Information Technology Matters in Societal Change: An Affordance-Based Institutional Perspective. *MIS Quarterly, ISSN 0276-7783, ISSN-e 2162-9730, Vol. 44, Nº. 3, 2020, Págs. 1359-1390*, *44*(3), 1359–1390. https://dialnet.unirioja.es/servlet/articulo?codigo=7700455&info=resumen&idioma=ENG

Iivari, N., Sharma, S., & Ventä-Olkkonen, L. (2020). Digital transformation of everyday life – How COVID-19 pandemic transformed the basic education of the young generation and why information management research should care? *International Journal of Information Management*, *55*, 102183. https://doi.org/10.1016/J.IJINFOMGT.2020.102183

Khoirunnisa, K., & Jubaidi, D. (2024). Indonesia's Digital Security Strategy: Countering the Threats of Cybercrime and Cyberterrorism. *SSRN Electronic Journal*. https://doi.org/10.2139/SSRN.5068424

Krishna, B., Krishnan, S., & Sebastian, M. P. (2023). Understanding the process of building institutional trust among digital payment users through national cybersecurity commitment trustworthiness cues: a critical realist perspective. *Information Technology and People*, *38*(2), 714–756. https://doi.org/10.1108/ITP-05-2023-0434/FULL/PDF

Liu, Q., & Wang, L. (2021). t-Test and ANOVA for data with ceiling and/or floor effects. *Behavior Research Methods*, *53*(1), 264–277. https://doi.org/10.3758/S13428-020-01407-2/TABLES/7

Loos, E., & Ivan, L. (2024). Not only people are getting old, the new media are too: Technology generations and the changes in new media use. *New Media and Society*, *26*(6), 3588–3613. https://doi.org/10.1177/14614448221101783/ASSET/IMAGES/LARGE/10.1177_14614448221101783-FIG10.JPEG

Mishra, P., Singh, U., Pandey, C. M., Mishra, P., & Pandey, G. (2019). Application of Student's t-test, Analysis of Variance, and Covariance. *Annals of Cardiac Anaesthesia*, *22*(4), 407. https://doi.org/10.4103/ACA.ACA_94_19

Moradi, M. (2021). Importance of Internet of Things (IoT) in Marketing Research and Its Ethical and Data Privacy Challenges. *Business Ethics and Leadership*, *5*(1), 22–30. https://doi.org/10.21272/BEL.5(1).22-30.2021

Muljono, Herowati, W., Hidayat, N. N., & Azies, H. Al. (2024). Introduction of Computational Thinking Models in the Kurikulum Merdeka Through Scratch Games for Teachers at Gaussian Kamil School Semarang. *JATI EMAS (Jurnal Aplikasi Teknik Dan Pengabdian Masyarakat)*, *8*(1), 9–14. https://doi.org/10.12345/JE.V8I1.21

Naufal, M., & Azies, H. Al. (2024). Menumbuhkan Literasi Teknologi Melalui Pengenalan Aplikasi Computer Vision Di Kalangan Pelajar. *Masyarakat Berkarya : Jurnal Pengabdian Dan Perubahan Sosial*, *1*(3), 51–60. https://doi.org/10.62951/KARYA.V1I3.356

Sari, D., Sari, D., Rejekiningsih, T., & Muchtarom, Moh. (2020). Students' Digital Ethics Profile in the Era of Disruption: An Overview from the Internet Use at ... In *International Journal of Interactive Mobile Technologies* (Vol. 14, Issue 15). International Association of Online Engineering. https://doi.org/10.3991/ijim.v14i03.12207

Scherb, C., Bryan, L., Grimberg, F., Grieder, H., & Maurer, M. (2023). A Cyberattack Simulation for Teaching Cybersecurity. *EPiC Series in Computing*, *93*, 129–140. https://doi.org/10.29007/DKDW

Szymkowiak, A., Melović, B., Dabić, M., Jeganathan, K., & Kundi, G. S. (2021).

Information technology and Gen Z: The role of teachers, the internet, and technology in the education of young people. *Technology in Society*, *65*, 101565. https://doi.org/10.1016/J.TECHSOC.2021.101565

Triwahyuni, D., Putri, S. O., & Nurjati, F. S. (2024). The Role of Indonesia's National Cyber and Crypton Agency in Dealing with the Increase in Cybercrime at the Beginning of the COVID-19 Pandemic. *Advances in Social Science, Education and Humanities Research*, *854*, 13–22. https://doi.org/10.2991/978-2-38476-269-9_3

Winarno, S., & Azies, H. Al. (2024). The Effectiveness of Continuous Formative Assessment in Hybrid Learning Models: An Empirical Analysis in Higher Education Institutions. *International Journal of Pedagogy and Teacher Education*, *8*(1), 1–11. https://doi.org/10.20961/IJPTE.V8I1.89693

Yusup, D. K. (2022). Cyber Security Sharing Platform: Indonesia Approach in Law Enforcement of Financial Transaction Crimes. *Journal of Legal, Ethical and Regulatory Issues*, *25*. https://heinonline.org/HOL/Page?handle=hein.journals/jnlolletl25&id=329&div=&collection=.