Institute of Research and Publication Indonesia
CONSEN: Indonesian Journal of Community Services and Engagement
Journal Homepage: https://journal.irpi.or.id/index.php/consen
Vol. 6 Iss. 1 Mei 2026, pp: 48-54
P-ISSN: 2828-9943 E-ISSN: 2809-0217

Empowering Vocational School Students Through Digital Security Training to Prevent Cyber Threats: A Case Study at SMKN 7 Pekanbaru

Pemberdayaan Siswa SMK Melalui Pelatihan Keamanan Digital untuk Mencegah Ancaman Siber: Studi Kasus di SMKN 7 Pekanbaru

Guntoro[1*], Lisnawita[2], Winda Monika[3] , Loneli Costaner[4]

[1,2,4]Ilmu Komputer, Universitas Lancang Kuning, Indonesia
[3]Ilmu Budaya, Universitas Lancang Kuning, Indonesia

E-Mail: guntoro@unilak.ac.id

Makalah: Diterima 02 Oktober 2025; Diperbaiki 11 April 2026; Disetujui 14 Mei 2026
Corresponding Author: Guntoro

Abstrak

Perangkat digital kini menjadi tulang punggung hampir setiap ruang kelas, namun kemudahan tersebut juga disertai dengan ancaman baru di bidang keamanan siber. Siswa pada jalur vokasi berada di titik persimpangan: mereka mengakses modul pembelajaran sepanjang hari, tetapi jarang sekali mendapatkan pembelajaran khusus tentang cara menjaga keamanan diri mereka di dunia maya. Tanpa pengetahuan praktis tersebut, lorong-lorong sebuah sekolah dapat secara diam-diam menimbun risiko seperti kebocoran data, pencurian identitas, dan perangkat lunak berbahaya. Sebagai tanggapan, pengabdian ini menginisiasi sebuah lokakarya berbasis kampus yang dirancang untuk menjangkau peserta didik sesuai dengan kondisi mereka. Kegiatan ini dilaksanakan di SMKN 7 Pekanbaru dengan melibatkan tiga puluh siswa jurusan keahlian yang bersedia ikut meskipun jadwal mereka padat. Materi disampaikan dengan bahasa yang sederhana; latihan praktik merekonstruksi insiden nyata yang diambil dari berita lokal; kuis cepat dan diskusi kelompok yang hidup mengikat seluruh rangkaian kegiatan. Penguasaan siswa diukur melalui perbandingan hasil sebelum dan sesudah kegiatan, berdasarkan lima tolok ukur keamanan utama. Nilai rata-rata awal berada pada angka 18,7 dari 25, sedangkan nilai akhir meningkat menjadi 24,4. Uji t berpasangan terhadap 29 set data yang lengkap menghasilkan $t(29) = 13{,}25$, $p < 0{,}0001$, yang jelas menyingkirkan kemungkinan kebetulan. Jika melihat grafik perbandingan, tren peningkatan terlihat jelas: setiap siswa mengalami kemajuan, dan suasana kelas dipenuhi rasa percaya diri yang sebelumnya tidak tampak. Pengabdian ini menegaskan bahwa lokakarya keamanan siber yang terfokus dan singkat dapat secara signifikan meningkatkan pemahaman peserta didik terhadap ancaman daring serta kebiasaan defensif yang mereka terapkan. Karena kerangka pembelajaran ini terbukti praktis, institusi lain berada pada posisi yang tepat untuk mengadopsinya dan dengan demikian dapat mengurangi kerentanan siber yang memengaruhi komunitas kampus.

Keyword: Keamanan Siber, Pendidikan, Pengabdian, Kesadaran Digital, Perlindungan Data

Abstract

Digital devices now form the backbone of nearly every classroom, yet that convenience comes tangled with new cybersecurity peril. Students in vocational tracks sit at the crossroads: they click through learning modules all day but rarely receive targeted instruction on how to keep themselves safe online. Without that practical know-how, the hallways of a single school can quietly accumulate risks like data leaks, identity theft, and rogue software. In response, the present study piloted a campus-based workshop designed to meet learners exactly where they are. Courses were delivered at SMKN 7 Pekanbaru, involving thirty trade students who volunteered despite their busy schedules. Lectures spoke in plain language; hands-on exercises replayed incidents pulled from local news; quick-fire quizzes and spirited group debates stitched it all together. Student mastery was quantified by side-by-side snapshots taken before and after the event, measured against five essential security benchmarks. The opening average sat at a modest 18.7 out of 25; the closing number soared to 24.4. A paired t-test for the twenty-nine complete sets of data returned $t(29) = 13.25$, $p < 0.0001$, clearly ruling out chance. Glance at the run charts and the upward drift is obvious: every learner moved forward, and the room buzzed with confidence that had been absent hours earlier. Recent research confirms that focused, brief cybersecurity workshops can significantly boost learners grasp of online threats and the defensive habits they employ. Because the instructional framework proved practical, other institutions are well-positioned to adopt it and thereby reduce the cyber vulnerabilities that affect campus communities.

Keyword: Cybersecurity, Education, Community Services, Digital Awareness, Data Protection

1. Introduction

Recently, technology, particularly the internet, has rapidly advanced, revolutionizing nearly every aspect of schools. Devices and online platforms now sit at the heart of lessons, run administrative tasks, guard student records, and keep parents, teachers, and children in steady communication. Due to this integration, researchers indicate that technology plays a key role in making schools operate more efficiently and effectively [1]. Earlier studies also demonstrate that when classrooms adopt new tools, teaching quality improves, learning becomes more accessible, and managing information is significantly less burdensome [2]. Therefore, digitizing school systems is not just advantageous; it is essential for educators seeking to create more nurturing, agile, and responsive environments for student development [3].

While digital devices and online platforms facilitate teaching, they also expose schools to serious cybersecurity threats. Risks such as data breaches, service outages, and misuse can profoundly impact educational institutions, particularly when their security measures are inadequate [4]. Cybercriminals are often drawn to easily accessible stores of personal information such as student records and administrative documents [5]. With increasing instances of ransomware, phishing, malware, and other attacks, schools face ongoing challenges related to trust and privacy that they owe to families [6] [7]. As a result, educational systems are prioritized targets for cybercriminals, urging leaders to enhance their defenses without delay [7] [8].

A significant issue confronting schools today is that staff often lack understanding of digital security. Many educators and administrative personnel are unfamiliar with online threats and have not received training on how to respond effectively if a cyber incident occurs [9] [10]. Numerous institutions still lack clear policies and step-by-step procedures for managing cyber crises, and their basic hardware and software protections are commonly weak [6]. These vulnerabilities can allow intruders to enter systems, disrupt educational activities, and damage the institution's reputation. Research indicates that increasing awareness and providing hands-on cybersecurity training to all staff members is one of the most effective methods to mitigate these risks [11].

Safeguarding school networks and records is crucial not only for protecting personal data but also for fostering parental confidence, maintaining the school’s good reputation, and ensuring classroom learning continues with minimal disruptions [12]. Robust security protocols enable staff to identify issues early and restore files promptly after incidents occur [8].. Consequently, security awareness and training programs are necessary to bolster institutional capacity in preventing and managing cyber threats [3]. Empirical evidence suggests that well-structured training initiatives can significantly enhance the cybersecurity competencies of educational staff [13].

The community service team at SMKN 7 Pekanbaru runs short workshops that teach students and teachers basic digital security tips, helps the school draft sensible online safety rules, and shows staff how to spot and handle digital risks. With these simple steps, the school hopes to lower the chance of cyber-attacks and build a safer, calmer place to learn

2. Method

The community service activity was conducted using a structured and phased approach to ensure systematic implementation and measurable outcomes. As illustrated in Figure 1, the method consists of four main stages: (1) preparation and planning, (2) field survey and interviews, (3) implementation of mentoring and training, and (4) evaluation and final reporting.

2.1 Preparation and Planning

In this initial stage, the service team conducted internal coordination meetings to define objectives, prepare educational materials, design assessment instruments (pre- and post-tests), and establish the logistical framework for the activity. This stage also included the development of ethical guidelines and communication protocols with school partners.

2.2 Field Survey and Interviews

A field visit and informal interviews were conducted with the principal and staff of SMKN 7 Pekanbaru. This stage aimed to explore the school’s digital environment, identify cybersecurity challenges faced by students, and confirm the technical and contextual needs to be addressed during the training.

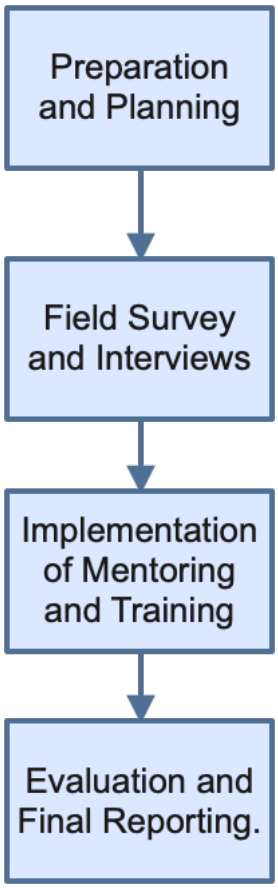

Figure 1. Research Methodology

2.3 Implementation of Mentoring and Training

The training phase was delivered in a one-day on-site session involving 30 students across various vocational disciplines. The structure consisted of:

- Pre-Training Assessment: A structured questionnaire (pre-test) was administered to evaluate students' baseline understanding in five domains: awareness of cyber threats, password strength practices, adoption of security tools (e.g., 2FA), response strategies to breaches, and willingness to share knowledge.
- Training Delivery: The training combined mini-lectures, interactive Q&A, group discussions, and guided demonstrations. Key topics included phishing recognition, data privacy, responsible social media use, and real-world cybersecurity cases.
- Post-Training Assessment: The same questionnaire was re-administered as a post-test to measure knowledge acquisition. Improvements in scores were used as the primary indicator of learning impact.
- Participant Observation: Instructors conducted informal observation to assess engagement levels, question participation, and application of concepts during practice scenarios.

2.4 Evaluation and Final Reporting

The effectiveness of the program was evaluated through quantitative and qualitative analyses. Pre- and post-test scores were compared using a paired sample t-test to determine the statistical significance of learning gains. Thematic insights from observation were synthesized to assess engagement and perceived relevance. A final report was produced containing findings, pedagogical reflections, and recommendations for broader adoption in other educational settings.

3. Results and Discussion

3.1 Quantitative Outcomes of the Training Intervention

To evaluate the impact of the digital security training, a pre-test and post-test design was conducted involving 30 vocational school students. Each test consisted of five Likert-scale statements related to cybersecurity awareness and practices, scored from 1 (strongly disagree) to 5 (strongly agree), yielding a maximum score of 25 per participant.

The results revealed a substantial increase in student scores after the training. The **mean pre-test score** was approximately **18.7**, while the **mean post-test score** increased to **24.4**. This indicates a significant gain in students' understanding and application of digital security principles.

A **paired t-test** was performed to determine the statistical significance of this improvement. The analysis yielded a **t-value of 13.25** and a **p-value < 0.0001**, demonstrating that the increase in scores was statistically significant at the 0.01 level.

Table 1. Summary of Pre-Test and Post-Test Results (N = 30)

Metric	Pre-Test	Post-Test
Mean Score (out of 25)	18.7	24.4
Min–Max Range	15–22	21–25
Standard Deviation	1.9	1.2
t-statistic	–	13.25
p-value	–	< 0.0001

These findings are consistent with prior studies (e.g., Siphambili, 2024; Księżopolski et al., 2022) that emphasize the importance of targeted training programs in enhancing digital literacy and reducing cyber risk, particularly among youth populations.

Visual Presentation and Statistical Interpretation

The impact of the training is further illustrated in **Figure 1**, which shows a clear rise in the average post-test score compared to the pre-test. This visualization reinforces the statistical evidence of the program's effectiveness in increasing students' knowledge of digital security.

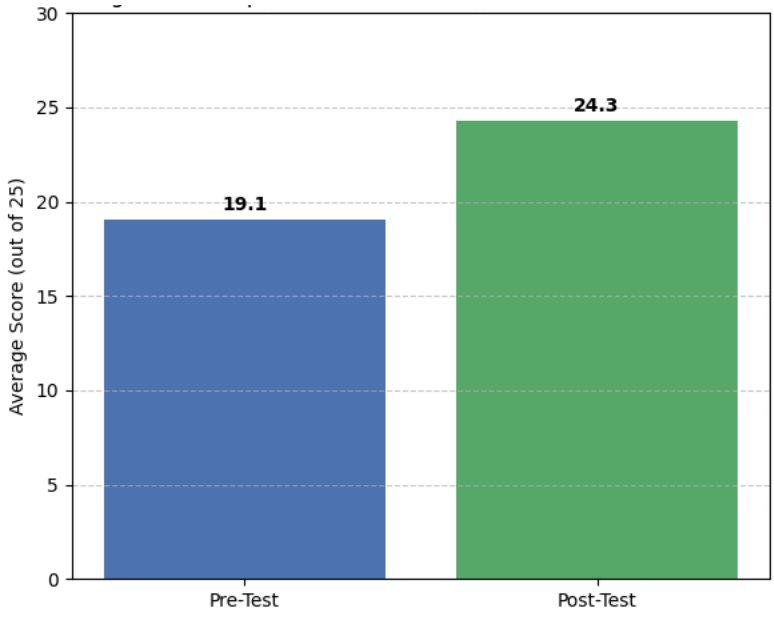

Figure 1. Comparison of Mean Pre-Test and Post-Test Scores

Additionally, **Figure 2** provides a detailed view of each student's performance before and after the training. Nearly all students exhibited score improvements, confirming a consistent positive trend across the sample.

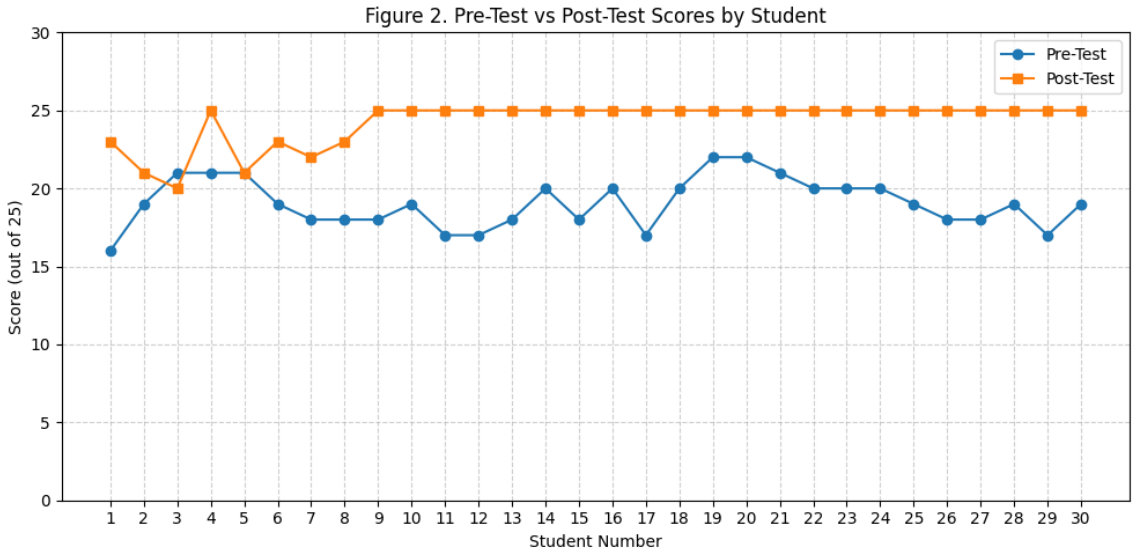

Figure 3. Pre-Test vs Post-Test Scores by Student

The mix of numbers and charts clearly shows the intervention made a noticeable, solid difference. The tight spread of post-test scores also tells us that everyone grasped the key cybersecurity ideas at about the same level.

Beyond the test data, we kept notes on how the program ran and how learners reacted, adding useful context. Figure 3 spotlights student engagement during the hands-on training sessions. These snapshots underline an active classroom and show the practical, behavior-shifting style we aimed for.

Figure 4. Vocational school students actively participating in the cybersecurity awareness session held at SMKN 7 Pekanbaru

3.2 Observational and Reflective Findings

Qualitative notes grabbed during the hands-on sessions and after-class chats showed that participants were noticeably involved. Students connected online dangers to everyday habits, like logging onto open Wi-Fi, sharing files carelessly, and leaving social media accounts wide open.

In follow-up reflections, most admitted they had previously brushed off such risks. Many pointed out that they reused passwords on several sites and seldom spotted strange links or phony sign-in forms. After the workshop, intentions to tighten security clearly grew, with learners pledging to switch on two-factor authentication and check privacy settings more often.

Although these intentions come from self-reporting, they mark an important mental jump from passive scrolling to active guarding. As Karagiannis and Magkos (2020) argue, knowing is useful only when it pushes people to act. If sustained, the findings hint at an encouraging turn from basic cybersecurity awareness toward engaged, responsible digital citizenship.

3.3 Contribution to Educational Cybersecurity Practice

The findings clearly show that cybersecurity classes should sit at the heart of the vocational syllabus rather than linger on the edges as after-hours, band-aid sessions. Because these learners work with niche programs and log into connected machines every day, they face real risks-yet most nationwide campaigns brush them aside.

To tackle that gap, the project also lays out a budget-friendly, easy-to-copy workshop model that any similar school could pick up. Tactics such as Kahoot quizzes, hands-on case chats, and brief animation clips kept the group alert and drove the key points home. In doing so, the method answers Verma and Pawars (2024) call for youth-centred cybersecurity plans across the Global South.

3.4 Limitations and Recommendations

Although the results collected right after training look good, there are clear weaknesses in the study. First, no one bothered to check whether knowledge sticks or whether users actually change their online habits, so a follow-up over months is essential. Second, diary entries and quick surveys rely on participants saying what sounds good, opening the door to social approval bias. Third, evidence was gathered from only one campus, leaving questions about whether the findings apply elsewhere.

To strengthen future trials and related service work, researchers and trainers should:

a) Add knowledge checks three to six months after the original session.

b) Loop in school IT staff and students families during the rollout.

4. Conclusion

The community-service program proved that a clear, step-by-step approach to online safety can lift cyber-awareness in vocational-school students. At SMKN 7 Pekanbaru, learners walked away with stronger grasp of real-world ideas like password care, daily digital habits, threat response, and sharing info responsibly. Numbers tell the story: participants average pre-test scores climbed from 18.7 to a near-perfect 24.4 out of 25 after the session. A paired t-test confirmed the change was real and not luck, showing $t(29) = 13.25$ with p well below 0.0001. Charts and graphs also made it clear-every learner improved, not just a few. Taken together, the findings underline how early, hands-on cybersecurity lessons inside classrooms can fortify young users against online dangers. They offer a straightforward, risk-tested blueprint other schools can follow as digital threats continue to rise. Future work could: invite parents and teachers into sessions so the whole school pulls together; add follow-up quizzes or practical tasks to see what students still remember weeks or months later; and draft clear, school-wide online safety rules that grow out of what the training reveals. When students gain basic cybersecurity know-how, schools build calmer, safer digital spaces that protect learning while teaching young people to spot risks, act wisely, and take shared responsibility for their online lives.

5. Acknowledgments
Acknowledgments are addressed to Pengabdian Kepada Masyarakat Dana Internal, Nomor: , Skema APBU Tahun 2025, Universitas Lancang Kuning, for providing the opportunity for the community service team to carry out this community service program. Thanks to SMKN 7 Kota Pekanbaru

References

[1] E. Akhmetshin, V. L. Vasilev, A. V. Kozachek, G. V. Meshkova, and M. V. Mikhailova, "Development of Digital University Model in Modern Conditions: Institutional Approach," *Digit. Educ. Rev.*, no. 40, pp. 17–32, 2021, doi: 10.1344/der.2021.40.17-32.

[2] L. Judijanto and H. Husnayetti, "The Effect of Financial Literacy, Digital Literacy, and Information Security on QRIS Adoption Among Students in Banten," *West Sci. Account. Finance*, vol. 2, no. 02, pp. 310–320, 2024, doi: 10.58812/wsaf.v2i02.1049.

[3] S. N. S. Nasir, "Exploring the Effectiveness of Cybersecurity Training Programs: Factors, Best Practices, and Future Directions," *Adv. Multidiscip. Sci. Res. J. Publ.*, vol. 2, no. 1, pp. 151–160, 2023, doi: 10.22624/aims/csean-smart2023p18.

[4] N. H. A. Rahim, S. Hamid, M. L. M. Kiah, S. Shamshirband, and S. Furnell, "A Systematic Review of Approaches to Assessing Cybersecurity Awareness," *Kybernetes*, vol. 44, no. 4, pp. 606–622, 2015, doi: 10.1108/k-12-2014-0283.

[5] M. J. L. Medina and C. Tnibar-Harrus, "Digital Security in Educational Training Programs: A Study Based on Future Teachers' Perceptions," *Inf. Technol. Learn. Tools*, vol. 95, no. 3, pp. 102–111, 2023, doi: 10.33407/itlt.v95i3.5204.

[6] O. Spivakovsky, S. Omelchuk, D. Malchykova, A. O. Цапів, and O. Lemeshchuk, "Academic Solidarity and Digitization: Management of a Displaced University," *Probl. Perspect. Manag.*, vol. 21, no. 2, pp. 40–51, 2023, doi: 10.21511/ppm.21(2-si).2023.06.

[7] J. Hajný, S. Ricci, E. Piesarskas, O. Levillain, L. Galletta, and R. D. Nicola, "Framework, Tools and Good Practices for Cybersecurity Curricula," *Ieee Access*, vol. 9, pp. 94723–94747, 2021, doi: 10.1109/access.2021.3093952.

[8] K. A. Y. Yaseen, "Importance of Cybersecurity in the Higher Education Sector 2022," *Asian J. Comput. Sci. Technol.*, vol. 11, no. 2, pp. 20–24, 2022, doi: 10.51983/ajcst-2022.11.2.3448.

[9] A. S. Gebeyew *et al.*, "Attitudes of Health Professionals Toward Digital Health Data Security in Northwest Ethiopia: Cross-Sectional Study," *Online J. Public Health Inform.*, vol. 16, pp. e57764–e57764, 2024, doi: 10.2196/57764.

[10] F. Filgueiras, "Artificial Intelligence and Education Governance," *Educ. Citizsh. Soc. Justice*, vol. 19, no. 3, pp. 349–361, 2023, doi: 10.1177/17461979231160674.

[11] M. J. G. Arrufat, N. Torres-Hernández, and T. Pessôa, "Competence of Future Teachers in the Digital Security Area," 2021, doi: 10.31219/osf.io/hgxwn.

[12] S. Lytvyn, "Introduction of Digital Technologies and Digitalisation in Higher Education Institutions of Ukraine: Current State and Prospects," *Sci. J. "Library Sci. Rec. Stud. Informology,"* vol. 20, no. 1, pp. 89–92, 2024, doi: 10.63009/lsrsi/1.2024.88.

[13] D. K. Respati, U. Widyastuti, T. Nuryati, A. M. Musyaffi, B. D. Handayani, and N. R. Ali, "How Do Students' Digital Financial Literacy and Financial Confidence Influence Their Financial Behavior and Financial Well-Being?," *Nurture*, vol. 17, no. 2, pp. 40–50, 2023, doi: 10.55951/nurture.v17i2.154.