

Penyuluhan Keamanan Siber untuk Siswa-Siswi Kursus dalam Menghadapi Ancaman Dunia Digital

Maulidina Rahmawati Surya^{1*}, Febriyansyah Ramadhan², Nia Novianti³, Sahara Abdy⁴, Munjiat Setiani Asih⁵

¹Sistem Informasi, Institut Teknologi dan Bisnis Tuban, Tuban, Indonesia

²Ilmu Komputer, Sistem Komputer, Universitas Indonesia Membangun, Bandung, Indonesia

³Teknologi Rekayasa Perangkat Lunak, Politeknik Hasan Abdi, Tanjung Morawa, Indonesia

⁴Manajemen Informatika, STMIK Logika, Medan, Indonesia

⁵Teknik Komputer, Teknik Informatika, Universitas harapan, Medan, Indonesia

Email: ^{1*}maulidinarahmawati14@gmail.com, ²febriyansyah.ramadhan@gmail.com,

³nia.politeknikhasanabdi@gmail.com, ⁴saharaabdy77@gmail.com, ⁵munjiat.stth@gmail.com

*Email Corresponding Author: maulidinarahmawati14@gmail.com

Abstrak

Perkembangan teknologi digital yang pesat meningkatkan risiko ancaman keamanan siber, terutama pada kalangan siswa yang aktif menggunakan internet namun memiliki literasi keamanan yang masih rendah. Kegiatan pengabdian ini bertujuan untuk meningkatkan pemahaman dan kesadaran siswa terhadap keamanan siber dalam menghadapi ancaman dunia digital. Metode yang digunakan meliputi penyuluhan dengan pendekatan ceramah interaktif, diskusi, dan simulasi kasus, yang melibatkan 30 siswa kursus sebagai peserta. Evaluasi dilakukan menggunakan instrumen pre-test dan post-test untuk mengukur peningkatan pemahaman peserta secara kuantitatif. Hasil kegiatan menunjukkan adanya peningkatan rata-rata nilai dari 48,2% pada pre-test menjadi 83,6% pada post-test, dengan persentase peningkatan sebesar 35,4%. Hasil ini menunjukkan bahwa kegiatan penyuluhan efektif dalam meningkatkan literasi keamanan siber peserta. Selain itu, terjadi perubahan perilaku peserta dalam penggunaan teknologi yang lebih aman, seperti peningkatan kewaspadaan terhadap phishing dan penggunaan password yang lebih kuat. Dengan demikian, kegiatan ini memberikan dampak positif secara kognitif dan perilaku, serta berpotensi mengurangi risiko kerugian akibat kejahatan siber. Kegiatan ini direkomendasikan untuk dilaksanakan secara berkelanjutan guna memperkuat kesiapan generasi muda dalam menghadapi tantangan digital.

Kata Kunci: Keamanan Siber, Literasi Digital, Penyuluhan, Siswa Kursus, Ancaman Digital.

Abstract

The rapid development of digital technology has increased the risk of cybersecurity threats, particularly among students who actively use the internet but have limited security awareness. This community service activity aims to improve students' understanding and awareness of cybersecurity in facing digital threats. The method used includes counseling through interactive lectures, discussions, and case simulations, involving 30 course students as participants. Evaluation was conducted using pre-test and post-test instruments to quantitatively measure participants' knowledge improvement. The results showed an increase in the average score from 48.2% in the pre-test to 83.6% in the post-test, with an improvement percentage of 35.4%. These findings indicate that the counseling activity was effective in enhancing participants' cybersecurity literacy. In addition, behavioral changes were observed, including increased awareness of phishing threats and improved password practices. Therefore, this activity provides positive impacts on both cognitive and behavioral aspects, and has the potential to reduce financial losses caused by cybercrime. It is recommended that similar activities be conducted continuously to strengthen the readiness of young generations in facing digital challenges.

Keywords: Cybersecurity, Digital Literacy, Counseling, Students, Digital Threats

1. PENDAHULUAN

Perkembangan teknologi digital yang semakin pesat telah membawa perubahan signifikan dalam berbagai aspek kehidupan, termasuk dalam dunia pendidikan dan aktivitas sehari-hari generasi muda. Siswa sebagai generasi digital native memiliki akses yang luas terhadap internet dan berbagai platform digital, namun tidak selalu diimbangi dengan pemahaman yang memadai terkait keamanan siber. Literasi digital kini tidak hanya mencakup kemampuan menggunakan teknologi, tetapi juga mencakup aspek keamanan, etika, dan perlindungan data pribadi. Hal ini menjadi penting karena ancaman digital seperti phishing, pencurian data, dan penyalahgunaan informasi semakin meningkat seiring dengan kemajuan teknologi. Studi menunjukkan bahwa rendahnya kesadaran keamanan siber dapat meningkatkan risiko kerentanan terhadap serangan digital pada kalangan pelajar (Baharuddin et al., 2025). Oleh karena itu, diperlukan upaya sistematis untuk meningkatkan literasi keamanan digital melalui pendekatan edukatif. Penguatan pemahaman ini menjadi fondasi dalam membentuk generasi yang cerdas dan aman dalam beraktivitas di dunia digital. Dengan demikian, penyuluhan keamanan siber menjadi relevan sebagai bentuk pengabdian kepada masyarakat.

Di sisi lain, transformasi digital dalam pendidikan telah menciptakan lingkungan pembelajaran yang sangat bergantung pada teknologi informasi. Penggunaan platform pembelajaran digital, media sosial, serta aplikasi berbasis internet menjadi bagian yang tidak terpisahkan dari aktivitas belajar siswa. Namun, kondisi ini juga membuka peluang terjadinya berbagai ancaman keamanan data dan privasi pengguna. Penelitian menunjukkan bahwa banyak siswa belum memiliki kompetensi yang cukup dalam menjaga keamanan data pribadi di lingkungan digital (Amin et al., 2025). Hal ini menunjukkan adanya kesenjangan antara penggunaan teknologi dan pemahaman terhadap risiko digital. Selain itu, kurangnya edukasi formal terkait keamanan siber memperparah kondisi tersebut. Oleh karena itu, diperlukan intervensi berupa kegiatan penyuluhan yang dapat menjembatani kesenjangan tersebut. Pendekatan edukasi praktis menjadi solusi efektif dalam meningkatkan kesadaran siswa. Dengan demikian, kegiatan pengabdian ini memiliki urgensi yang tinggi.

Literasi digital merupakan kompetensi dasar yang harus dimiliki oleh setiap individu di era modern. Kemampuan dalam mengakses, memahami, mengevaluasi, dan menggunakan informasi digital secara bijak menjadi indikator penting dalam kesiapan menghadapi era digital. Penelitian terbaru menunjukkan bahwa literasi digital memiliki pengaruh signifikan terhadap hasil belajar dan kemampuan adaptasi siswa terhadap teknologi (Yuan et al., 2025). Selain itu, literasi digital juga berperan dalam meningkatkan kemampuan berpikir kritis dan pengambilan keputusan berbasis informasi. Namun, literasi digital yang tidak disertai dengan pemahaman keamanan siber dapat menimbulkan risiko baru. Oleh karena itu, integrasi antara literasi digital dan keamanan siber menjadi sangat penting. Pendekatan ini memungkinkan siswa tidak hanya menjadi pengguna teknologi, tetapi juga pengguna yang cerdas dan aman. Hal ini menjadi landasan dalam merancang kegiatan penyuluhan yang efektif.

Ancaman dunia digital saat ini semakin kompleks dan beragam, mulai dari serangan malware, phishing, hingga penyebaran informasi palsu. Siswa sebagai pengguna aktif internet menjadi salah satu kelompok yang rentan terhadap berbagai ancaman tersebut. Kurangnya pengetahuan tentang cara mengenali dan menghindari ancaman digital menjadi faktor utama kerentanan tersebut. Penelitian empiris menunjukkan bahwa edukasi cybersecurity mampu meningkatkan pemahaman siswa terhadap risiko digital secara signifikan (Agung, 2025). Selain itu, edukasi ini juga berdampak pada peningkatan kesadaran dalam menjaga keamanan data pribadi. Hal ini menunjukkan bahwa intervensi edukatif memiliki peran penting dalam mitigasi risiko digital. Oleh karena itu, penyuluhan keamanan siber perlu dilakukan secara terstruktur dan berkelanjutan. Dengan demikian, siswa dapat lebih siap menghadapi tantangan dunia digital.

Dalam konteks pendidikan abad ke-21, integrasi literasi digital dan keamanan siber menjadi kebutuhan yang tidak dapat diabaikan. Pendidikan tidak hanya berfokus pada aspek kognitif, tetapi juga pada kemampuan adaptif terhadap perkembangan teknologi. Studi literatur menunjukkan bahwa literasi digital mencakup dimensi teknis,

sosial, dan etika dalam penggunaan teknologi (Fajri et al., 2024). Hal ini menunjukkan bahwa pendidikan digital harus bersifat holistik dan komprehensif. Selain itu, pendidikan keamanan siber juga harus mencakup aspek perilaku dan kesadaran pengguna. Pendekatan ini bertujuan untuk membentuk karakter digital yang bertanggung jawab. Oleh karena itu, kegiatan penyuluhan menjadi salah satu strategi yang efektif dalam implementasi pendidikan tersebut. Dengan demikian, kegiatan ini memiliki kontribusi dalam penguatan kapasitas siswa.

Selain itu, tren penelitian menunjukkan bahwa pengembangan literasi digital terus mengalami peningkatan dalam beberapa tahun terakhir. Hal ini menunjukkan adanya kesadaran global terhadap pentingnya kompetensi digital dalam pendidikan. Analisis bibliometrik menunjukkan bahwa literasi digital menjadi salah satu fokus utama dalam penelitian pendidikan modern (Oktarina et al., 2025). Namun, masih terdapat kesenjangan dalam implementasi literasi digital pada konteks pendidikan non-formal seperti kursus. Hal ini menjadi tantangan sekaligus peluang dalam pengembangan program pengabdian masyarakat. Kegiatan penyuluhan dapat menjadi solusi untuk menjangkau kelompok tersebut. Dengan pendekatan yang tepat, kegiatan ini dapat memberikan dampak yang signifikan. Oleh karena itu, penting untuk merancang program yang sesuai dengan kebutuhan peserta.

Kondisi empiris di lapangan menunjukkan bahwa siswa kursus seringkali lebih fokus pada penguasaan keterampilan teknis dibandingkan aspek keamanan digital. Hal ini menyebabkan kurangnya kesadaran terhadap risiko yang mungkin dihadapi dalam penggunaan teknologi. Selain itu, keterbatasan materi pembelajaran terkait keamanan siber menjadi salah satu faktor penyebab rendahnya pemahaman siswa. Penelitian menunjukkan bahwa edukasi yang terstruktur dapat meningkatkan kompetensi digital secara menyeluruh (Wang & Wang, 2025). Oleh karena itu, diperlukan intervensi yang dapat mengintegrasikan aspek keamanan dalam pembelajaran digital. Penyuluhan menjadi salah satu metode yang efektif dalam memberikan pemahaman tersebut. Dengan pendekatan yang interaktif, siswa dapat lebih mudah memahami materi yang disampaikan. Hal ini menjadi dasar dalam pelaksanaan kegiatan pengabdian ini.

Berdasarkan uraian tersebut, dapat disimpulkan bahwa penyuluhan keamanan siber merupakan kebutuhan mendesak dalam meningkatkan kesiapan siswa menghadapi ancaman dunia digital. Kegiatan ini bertujuan untuk meningkatkan pengetahuan, kesadaran, dan keterampilan siswa dalam menjaga keamanan digital. Selain itu, kegiatan ini juga diharapkan dapat memberikan dampak positif terhadap perilaku digital siswa. Dengan pendekatan yang sistematis dan berbasis kebutuhan, kegiatan ini diharapkan dapat memberikan kontribusi nyata bagi masyarakat. Oleh karena itu, pengabdian ini dirancang untuk memberikan solusi praktis terhadap permasalahan yang ada. Kegiatan ini juga menjadi bentuk implementasi peran akademisi dalam memberikan edukasi kepada masyarakat. Dengan demikian, penyuluhan keamanan siber menjadi langkah strategis dalam membangun generasi digital yang aman dan cerdas.

2. METODE PELAKSANAAN



Gambar 1. Tahapan Pelaksana

2.1 Subjek dan Lokasi Kegiatan

Kegiatan pengabdian ini dilaksanakan pada siswa-siswi lembaga kursus yang aktif menggunakan perangkat digital dalam proses pembelajaran. Subjek kegiatan berjumlah 30 peserta yang terdiri dari siswa tingkat menengah dengan rentang usia 15–18 tahun. Pemilihan peserta dilakukan secara purposive sampling dengan mempertimbangkan intensitas penggunaan internet dalam aktivitas belajar sehari-hari. Lokasi kegiatan berada di lingkungan lembaga kursus yang telah memiliki fasilitas pendukung seperti jaringan internet dan perangkat komputer. Karakteristik peserta menunjukkan bahwa sebagian besar telah menggunakan media sosial dan platform digital, namun belum memiliki pemahaman yang memadai terkait keamanan siber. Kondisi ini menjadikan peserta sebagai kelompok yang relevan untuk diberikan intervensi edukatif. Kegiatan ini dilaksanakan secara langsung (offline) dengan pendekatan partisipatif. Dengan demikian, subjek kegiatan mencerminkan kondisi nyata yang menjadi sasaran pengabdian masyarakat.

2.2 Tahapan Pelaksanaan Kegiatan

Pelaksanaan kegiatan dilakukan secara sistematis melalui beberapa tahapan yang terstruktur. Tahap pertama adalah analisis kebutuhan, yang dilakukan melalui observasi awal dan wawancara singkat untuk mengidentifikasi tingkat pemahaman peserta terkait keamanan siber. Tahap kedua adalah perencanaan materi, yang mencakup penyusunan modul penyuluhan berbasis literasi digital dan ancaman siber terkini. Tahap ketiga adalah pelaksanaan penyuluhan, yang dilakukan melalui metode ceramah interaktif, diskusi, dan simulasi kasus. Tahap keempat adalah evaluasi kegiatan, yang dilakukan menggunakan pre-test dan post-test untuk mengukur peningkatan pemahaman peserta. Selain itu, dilakukan juga observasi perilaku peserta selama kegiatan berlangsung. Tahap terakhir adalah refleksi dan tindak lanjut, yang bertujuan untuk mengevaluasi efektivitas kegiatan dan merancang perbaikan di masa mendatang. Setiap tahapan dirancang untuk memastikan ketercapaian tujuan kegiatan secara optimal. Dengan demikian, alur kegiatan bersifat sistematis dan terukur.

2.3 Instrumen dan Teknik Pengumpulan Data

Instrumen yang digunakan dalam kegiatan ini meliputi beberapa alat ukur yang dirancang untuk memperoleh data secara kuantitatif dan kualitatif. Instrumen utama adalah kuesioner pre-test dan post-test yang berisi 15 pertanyaan terkait konsep dasar keamanan siber, seperti phishing, password security, dan perlindungan data pribadi. Selain itu, digunakan lembar observasi untuk menilai partisipasi dan respons peserta selama kegiatan berlangsung. Instrumen pendukung lainnya adalah dokumentasi kegiatan berupa foto dan catatan lapangan. Validitas instrumen diuji secara sederhana melalui uji keterbacaan dan kesesuaian dengan materi yang disampaikan. Teknik pengumpulan data dilakukan sebelum dan sesudah kegiatan untuk melihat perubahan yang terjadi. Data yang diperoleh kemudian diklasifikasikan berdasarkan indikator yang telah ditentukan. Dengan demikian, instrumen yang digunakan mampu menggambarkan tingkat pemahaman peserta secara komprehensif.

2.4 Teknik Analisis Data

Analisis data dilakukan secara deskriptif kuantitatif dengan membandingkan hasil pre-test dan post-test peserta. Peningkatan pemahaman dihitung menggunakan rumus persentase peningkatan skor rata-rata. Selain itu, analisis kualitatif dilakukan berdasarkan hasil observasi untuk melihat perubahan perilaku peserta dalam memahami keamanan siber. Indikator keberhasilan kegiatan ditentukan berdasarkan peningkatan minimal $\geq 30\%$ dari skor awal. Data kemudian disajikan dalam bentuk tabel dan grafik untuk mempermudah interpretasi. Hasil analisis digunakan untuk mengevaluasi efektivitas metode penyuluhan yang telah dilakukan. Dengan pendekatan ini, kegiatan pengabdian tidak hanya bersifat deskriptif tetapi juga terukur secara empiris. Hal ini sesuai dengan standar penulisan jurnal pengabdian yang menekankan pada dampak nyata. Dengan demikian, analisis data memberikan gambaran yang jelas mengenai keberhasilan kegiatan.

2.5 Indikator Keberhasilan Kegiatan

Indikator keberhasilan kegiatan ditentukan berdasarkan beberapa aspek yang dapat diukur secara kuantitatif dan kualitatif. Pertama, adanya peningkatan nilai rata-rata post-test dibandingkan pre-test dengan minimal peningkatan sebesar 30%. Kedua, meningkatnya pemahaman peserta terhadap konsep keamanan siber yang ditunjukkan melalui jawaban yang lebih tepat. Ketiga, meningkatnya partisipasi aktif peserta selama kegiatan berlangsung. Keempat, adanya perubahan perilaku dalam penggunaan teknologi yang lebih aman, seperti penggunaan password yang kuat dan kewaspadaan terhadap phishing. Kelima, respon positif peserta terhadap kegiatan penyuluhan yang dilakukan. Indikator-indikator ini digunakan sebagai tolok ukur dalam menilai keberhasilan kegiatan secara menyeluruh. Dengan adanya indikator yang jelas, evaluasi kegiatan dapat dilakukan secara objektif. Hal ini memperkuat validitas hasil pengabdian yang dilakukan.

3. HASIL PEMBAHASAN

3.1 Hasil Pengukuran Pre-Test dan Post-Test

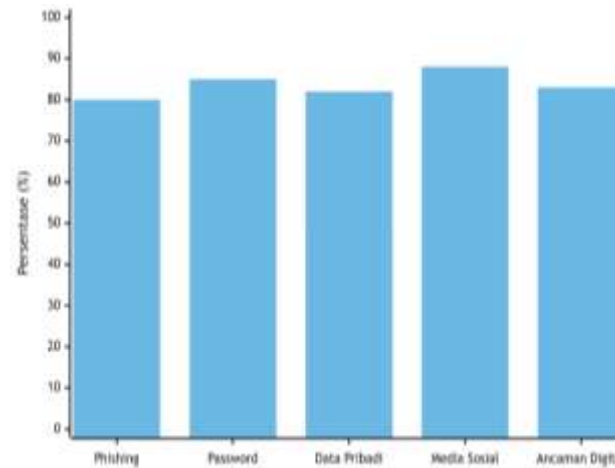
Kegiatan penyuluhan keamanan siber menunjukkan adanya peningkatan signifikan terhadap pemahaman peserta. Pengukuran dilakukan menggunakan instrumen pre-test dan post-test dengan jumlah 15 soal terkait konsep dasar keamanan siber. Hasil pengukuran menunjukkan bahwa rata-rata nilai peserta sebelum kegiatan masih tergolong rendah, yang mengindikasikan kurangnya pemahaman awal terhadap ancaman dunia digital. Setelah dilakukan penyuluhan, terjadi peningkatan yang cukup signifikan pada hasil post-test. Hal ini menunjukkan bahwa metode penyuluhan yang digunakan efektif dalam meningkatkan pemahaman peserta. Peningkatan ini juga didukung oleh keterlibatan aktif peserta selama kegiatan berlangsung. Dengan demikian, kegiatan pengabdian ini memberikan dampak positif secara kognitif. Berikut adalah hasil perbandingan nilai peserta.

Tabel 1. Hasil Pre-Test dan Post-Test Peserta

No	Indikator Materi	Pre-Test (%)	Post-Test (%)	Peningkatan (%)
1	Pemahaman Phishing	45	80	35
2	Keamanan Password	50	85	35
3	Perlindungan Data Pribadi	48	82	34
4	Penggunaan Media Sosial	52	88	36
5	Kesadaran Ancaman Digital	46	83	37
	Rata-rata	48,2	83,6	35,4

3.2 Visualisasi Peningkatan Hasil

Berikut grafik peningkatan hasil pre-test dan post-test dalam bentuk diagram:



Gambar 2. Diagram Peningkatan

3.3 Analisis Peningkatan dan Indikator Keberhasilan

Berdasarkan hasil pengukuran, rata-rata peningkatan pemahaman peserta mencapai **35,4%**, yang berarti telah melampaui indikator keberhasilan yang ditetapkan yaitu $\geq 30\%$. Hal ini menunjukkan bahwa kegiatan penyuluhan berhasil meningkatkan pengetahuan peserta secara signifikan. Indikator keberhasilan juga terlihat dari meningkatnya kemampuan peserta dalam menjawab soal terkait keamanan siber dengan benar. Selain itu, peserta menunjukkan peningkatan kesadaran dalam mengidentifikasi potensi ancaman digital. Keaktifan peserta dalam sesi diskusi juga menjadi indikator keberhasilan non-kuantitatif. Dengan demikian, kegiatan ini memenuhi kriteria keberhasilan secara kuantitatif dan kualitatif. Hal ini menunjukkan bahwa pendekatan yang digunakan sudah tepat sasaran. Evaluasi ini memperkuat bahwa kegiatan pengabdian memberikan dampak nyata.

3.4 Analisis Dampak Kegiatan

a. Dampak Kognitif

Kegiatan penyuluhan memberikan peningkatan signifikan pada aspek pengetahuan peserta. Peserta menjadi lebih memahami konsep dasar keamanan siber seperti phishing, malware, dan keamanan password. Selain

itu, peserta mampu mengidentifikasi ancaman digital secara lebih akurat. Hal ini ditunjukkan dari peningkatan nilai post-test yang signifikan. Peningkatan ini menunjukkan bahwa materi yang disampaikan dapat dipahami dengan baik. Dengan demikian, kegiatan ini berhasil meningkatkan literasi digital peserta. Dampak kognitif ini menjadi dasar penting dalam perubahan perilaku digital. Oleh karena itu, penyuluhan terbukti efektif dalam aspek edukasi.

b. Dampak Perilaku

Perubahan perilaku peserta terlihat dari meningkatnya kesadaran dalam menggunakan teknologi secara aman. Peserta mulai memahami pentingnya penggunaan password yang kuat dan tidak membagikan data pribadi secara sembarangan. Selain itu, peserta menjadi lebih berhati-hati dalam mengakses link atau informasi yang mencurigakan. Selama kegiatan, peserta juga aktif dalam diskusi terkait pengalaman mereka menghadapi ancaman digital. Hal ini menunjukkan adanya peningkatan kesadaran digital. Perubahan perilaku ini merupakan indikator penting dalam keberhasilan pengabdian. Dengan demikian, kegiatan ini memberikan dampak nyata dalam kehidupan sehari-hari peserta.

c. Dampak Ekonomi

Secara tidak langsung, kegiatan ini memberikan dampak ekonomi bagi peserta. Dengan meningkatnya pemahaman keamanan siber, peserta dapat menghindari potensi kerugian akibat penipuan digital. Hal ini penting mengingat banyak kasus kejahatan siber yang berdampak pada kerugian finansial. Selain itu, peserta juga dapat memanfaatkan teknologi digital secara lebih produktif dan aman. Pemahaman ini dapat mendukung kesiapan mereka dalam dunia kerja berbasis digital. Dengan demikian, kegiatan ini memiliki nilai tambah dari sisi ekonomi. Dampak ini menunjukkan bahwa pengabdian tidak hanya bersifat edukatif tetapi juga preventif. Oleh karena itu, kegiatan ini memiliki manfaat jangka panjang.

3.5 Dokumentasi Kegiatan

Berikut adalah dokumentasi kegiatan yang sesuai dengan template jurnal:



Gambar 3. Kegiatan Penyuluhan di Dalam Kelas



Gambar 4. Interaksi dan Diskusi Peserta

4. KESIMPULAN

Kegiatan penyuluhan keamanan siber yang dilaksanakan pada siswa-siswi kursus menunjukkan hasil yang efektif dalam meningkatkan pemahaman dan kesadaran peserta terhadap ancaman dunia digital. Berdasarkan hasil pengukuran kuantitatif melalui pre-test dan post-test, terjadi peningkatan rata-rata sebesar 35,4% yang telah melampaui indikator keberhasilan yang ditetapkan, yaitu minimal 30%. Hal ini menunjukkan bahwa metode penyuluhan yang digunakan, yang meliputi ceramah interaktif, diskusi, dan simulasi kasus, mampu memberikan pemahaman yang komprehensif kepada peserta. Selain peningkatan aspek kognitif, kegiatan ini juga berdampak pada perubahan perilaku peserta dalam menggunakan teknologi secara lebih aman dan bijak, seperti meningkatkan kewaspadaan terhadap phishing, penggunaan password yang lebih kuat, serta kesadaran dalam menjaga data pribadi. Dampak lain yang tidak kalah penting adalah aspek ekonomi, di mana peserta memiliki potensi untuk menghindari kerugian akibat kejahatan siber melalui peningkatan literasi keamanan digital. Meskipun demikian, masih terdapat keterbatasan dalam hal durasi kegiatan yang relatif singkat sehingga belum mampu menjangkau seluruh aspek keamanan siber secara mendalam. Oleh karena itu, diperlukan kegiatan lanjutan yang lebih intensif dan berkelanjutan, baik dalam bentuk pelatihan lanjutan maupun integrasi materi keamanan siber dalam kurikulum pembelajaran. Dengan demikian, kegiatan pengabdian ini tidak hanya memberikan dampak jangka pendek, tetapi juga memiliki potensi kontribusi jangka panjang dalam membentuk generasi digital yang cerdas, aman, dan adaptif terhadap perkembangan teknologi.

5. UCAPAN TERIMA KASIH

Penulis menyampaikan ucapan terima kasih kepada seluruh pihak yang telah berkontribusi dalam pelaksanaan kegiatan pengabdian kepada masyarakat ini. Terima kasih disampaikan kepada pihak lembaga kursus yang telah memberikan izin serta dukungan fasilitas selama kegiatan berlangsung, sehingga penyuluhan dapat terlaksana dengan baik. Apresiasi juga diberikan kepada para peserta yang telah berpartisipasi aktif dalam setiap rangkaian kegiatan, mulai dari tahap awal hingga evaluasi akhir. Selain itu, penulis mengucapkan terima kasih kepada tim

pelaksana yang telah bekerja sama secara optimal dalam mempersiapkan materi, melaksanakan kegiatan, hingga melakukan evaluasi. Ucapan terima kasih juga disampaikan kepada pihak institusi yang telah memberikan dukungan moral maupun administratif dalam pelaksanaan kegiatan ini. Semoga kegiatan pengabdian ini dapat memberikan manfaat yang berkelanjutan bagi peserta dan menjadi kontribusi nyata dalam meningkatkan literasi keamanan siber di masyarakat.

6. REFERENSI

- Agung, H. (2025). Efektivitas edukasi cybersecurity dalam meningkatkan pengetahuan siswa tentang ancaman digital pada siswa menengah atas. *Jurnal Ilmu Komputer*, 5(2). <https://doi.org/10.52060/pti.v4i1.1173>
- Amin, R., Khan, J., Akhtar, S., & Rustiyana, R. (2025). Cybersecurity challenges in educational technology: Protecting student data in digital learning platforms. *Journal Emerging Technologies in Education*, 3(4), 201–212. <https://doi.org/10.70177/jete.v3i4.2797>
- Baharuddin, M. F., Jalil, A., Amin, Z. M., Rahmad, F., & Shuhidan, S. M. (2025). Digital literacy and cybersecurity in higher education: The unseen power of academic librarians. *International Journal of Evaluation and Research in Education*, 14(6), 4404–4417. <https://doi.org/10.11591/ijere.v14i6.34916>
- Fajri, S. R., Fajri, N., Sarnita, F., Fitriani, H., Bago, A. S., Nitiasih, P. K., & Sudatha, I. G. W. (2024). Digital literacy dan cyber socialization in the context of 21st century education: A systematic review. *International Journal of Applied Science and Sustainable Development*, 6(2), 76–91. <https://doi.org/10.36733/ijassd.v6i2.9078>
- Oktarina, A. D., Hamdi, S., Wijaya, A., Zafrullah, Z., & Rashid, S. (2025). Research trends on the implementation of digital literacy in education: A bibliometric analysis of the Scopus database. *Indonesian Journal on Learning and Advanced Education*, 7(3), 481–502. <https://doi.org/10.23917/ijolae.v7i3.11087>
- Wang, Y., & Wang, S. (2025). Digital literacy education among students: Status, pathways, and implications in the current digital era. *International Journal of Education and Teaching Zone*, 4(1), 66–85. <https://doi.org/10.57092/ijetz.v4i1.385>
- Yuan, N., Yu, Q., & Liu, W. (2025). The impact of digital literacy on learning outcomes among college students. *Frontiers in Education*, 10, 1641687. <https://doi.org/10.3389/feduc.2025.1641687>
- Mujiono, M. (2024). Digital literacy: Fundamental competence for modern society. *Didaktika: Jurnal Pemikiran Pendidikan*, 30(1). <https://doi.org/10.30587/didaktika.v30i1.6906>
- Sautunnida, L., Ridayani, R., Khairani, K., Kurniasari, E., Utami, A. R., & Fajri, I. (2024). Digital legal education and cybersecurity awareness: A bibliometric study on student behavior. *Mukadimah*, 8(2).
- Setyadi, A., & Pawirosumarto, S. (2025). Risk management, digital technology literacy, and modern learning environments. *Education and Information Technologies*. <https://doi.org/10.1007/s10639-025-13380-4>