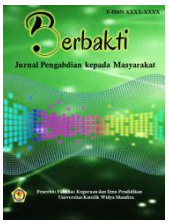
Vol. 3 No. 3, Januari 2026 ISSN 2987-033X



Berbakti

Jurnal Pengabdian Kepada Masyarakat

https://journal.unwira.ac.id/index.php/BERBAKTI

PENINGKATAN KESADARAN KEAMANAN SIBER SISWA SMK MELALUI PELATIHAN DAN SIMULASI SERANGAN DALAM LINGKUNGAN VIRTUAL

Agus Wijayanto[1*], Muhammad Fahmi Abdillah[2], Aqilah Aulya Maulidah[3], Aljosa Maynardian[4], Ghina Nur Madina[5], Apriliani Wijaya[6], Rachel Ajerna Cecilia Gerungan[7], Naillu Najha[8], Ahmad Zaki Ahsani[9], Satria Mahardika Ramadhan[10], Rama Danu Triwahyudi[11], Eryal Rivano Zistafa[12]

[1,2,3,4,5,6,7,8,9,10,11,12] Universitas Mulia, Indonesia

e-mail: aguswijayanto@universitasmulia.ac.id[1*]

Dikirim: 02 Januari 2026, Direvisi: 13 Januari 2026, Diterima: 16 Januari 2026

ABSTRAK

Perkembangan dunia siber yang semakin pesat menuntut peningkatan kesiapan dan kesadaran keamanan digital sejak dini, khususnya bagi siswa Sekolah Menengah Kejuruan (SMK) di bidang teknologi informasi. Kegiatan pengabdian kepada masyarakat ini bertujuan untuk meningkatkan kesadaran keamanan siber dan pemahaman teknis siswa Jurusan Teknik Komputer dan Jaringan (TKJ) di SMKN 6 Balikpapan melalui pelatihan dan simulasi serangan siber dalam lingkungan virtual. Program dilaksanakan melalui tiga tahapan, yaitu persiapan berupa pemaparan konsep dan urgensi keamanan siber, pelaksanaan pelatihan yang mencakup pre-test, simulasi serangan dan mitigasi, serta tahap evaluasi melalui post-test. Hasil kegiatan menunjukkan peningkatan signifikan pemahaman siswa, dengan rata-rata nilai meningkat sebesar 29%, dari 60% pada pre-test menjadi 89% pada post-test. Peningkatan tertinggi terjadi pada aspek teknis deteksi serangan dan mitigasi risiko jaringan. Temuan ini menunjukkan bahwa pelatihan berbasis simulasi serangan langsung dalam lingkungan virtual efektif dalam meningkatkan kesadaran dan kewaspadaan siswa terhadap ancaman siber, terutama terkait risiko membuka atau menjalankan file dari sumber yang tidak tervalidasi.

Kata kunci: Cybersecurity awareness; kali linux; metasploit; SMK; pelatihan cybersecurity.

ABSTRACT

The rapid development of the cyber world demands an increase in digital security preparedness and awareness from an early age, especially for vocational high school (SMK) students in the field of information technology. This community service activity aims to increase cyber security awareness and technical understanding among students majoring in Computer and Network Engineering (TKJ) at SMKN 6 Balikpapan through training and cyber attack simulations in a virtual environment. The program was implemented in three stages, namely preparation in the form of an explanation of the concepts and urgency of cyber security, implementation of training covering pre-tests, attack simulations and mitigation, and an evaluation stage through post-tests. The results of the activity showed a significant increase in student understanding, with an average score increase of 29%, from 60% in the pre-test to 89% in the post-test. The highest increase occurred in the technical aspects of attack detection and network risk mitigation. These findings indicate that simulation-based training in a virtual environment is effective in increasing students' awareness and vigilance against cyber threats, especially those related to the risks of opening or running files from unvalidated sources.

Keywords: Cybersecurity awareness; kali linux; metasploit; SMKN 6 balikpapan; attack simulation.

1. PENDAHULUAN

Internet telah menjadi tulang punggung aktivitas ekonomi dan Pendidikan, integrasi teknologi digital yang masif ini tidak dampingi dengan pemahaman keamanan yang memadai pada level pengguna akhir (Kahar et al., 2021). Di SMK Negeri 6 Balikpapan, khususnya pada siswa, ditemukan masalah nyata berupa perilaku daring yang berisiko. Sebagai *digital natives*, mereka terbiasa mengunduh aplikasi bajakan, menggunakan kata sandi yang lemah, dan terpapar pada tautan yang tidak jelas sumbernya. Selain itu, tantangan spesifik yang dihadapi mitra adalah persiapan menghadapi Lomba Kompetensi Siswa (LKS) bidang *cybersecurity*, di mana siswa dituntut memiliki keterampilan praktis yang melampaui kurikulum standar sekolah.

Jika perilaku berisiko ini tidak segera ditangani, dampaknya akan sangat signifikan baik secara material maupun non-material (Puteri et al., 2025). Faktor manusia sering kali disebut sebagai mata rantai terlemah dalam sistem keamanan informasi (Wijayanto, 2024). Secanggih apa pun perangkat keras dan perangkat lunak yang digunakan untuk memproteksi sistem, akan menjadi sia-sia jika penggunanya tidak memiliki kesadaran keamanan (*security awareness*) (Afandi et al., 2017). Serangan berbasis rekayasa sosial seperti *phishing*, *baiting*, atau penipuan identitas, memanfaatkan kelalaian dan ketidaktahuan manusia untuk membobol sistem pertahanan yang sebenarnya sudah kuat secara teknis (Revilia & Irwansyah, 2020). Bagi siswa TKJ yang merupakan calon administrator jaringan, kebiasaan buruk ini tidak hanya membahayakan data pribadi mereka, tetapi juga mengancam integritas sistem di instansi tempat mereka akan bekerja kelak (Yudistira et al., 2025).

Saat ini, terdapat kesenjangan besar antara materi pembelajaran di sekolah dengan dinamika ancaman siber yang terus berevolusi (Aulia et al., 2025). Kurikulum SMK saat ini cenderung berfokus pada aspek fungsionalitas, bagaimana membangun sistem agar berjalan namun kurang memberikan porsi pada aspek keamanan ofensif. Siswa sering kali merasa cukup hanya dengan memasang antivirus, padahal serangan siber saat ini jauh lebih kompleks (Suhendra, 2024). Mereka memahami cara kerja jaringan, namun kurang memahami terhadap bagaimana seorang peretas melihat celah dalam jaringan tersebut (Wijayanto et al., 2023). Dibutuhkan metode pembelajaran melalui simulasi serangan nyata atau Live Hacking untuk memberikan memori visual yang kuat mengenai bahaya siber (Idris et al., 2023).

Untuk menjawab tantangan tersebut, diperlukan metode pembelajaran yang tidak konvensional, yaitu melalui simulasi serangan nyata atau Live Hacking (Pradana, 2024). Metode ini memberikan *shock therapy* yang efektif. Dengan melihat secara langsung bagaimana mudahnya sebuah perangkat diambil alih hanya karena satu kesalahan kecil (misalnya mengunduh file sembarangan), siswa akan memiliki memori visual yang kuat mengenai bahaya siber (Tandirerung et al., 2023). Pemahaman mengenai *offensive security* ini diajarkan bukan untuk mencetak peretas jahat, melainkan untuk membangun defense (pertahanan) yang lebih baik dengan memahami pola pikir penyerang (Marwati et al., 2025).

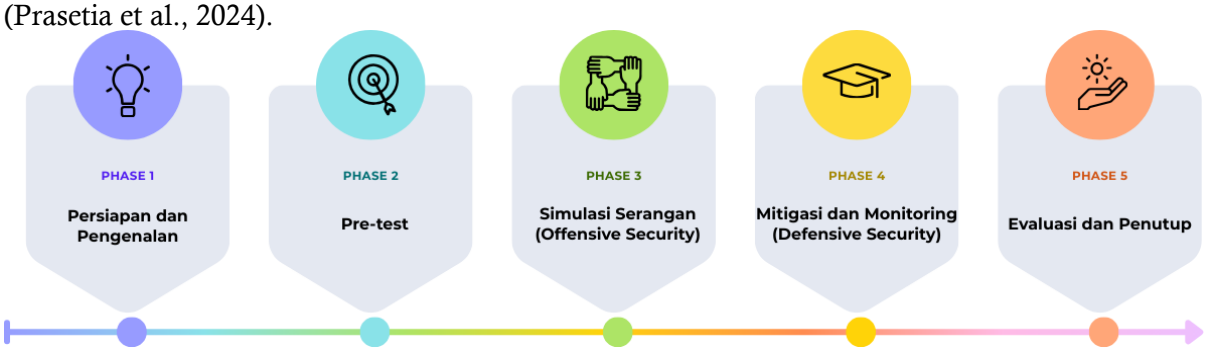
Program Studi Teknologi Informasi, Fakultas Ilmu Komputer, Universitas Mulia, memiliki tanggung jawab moral dan akademis untuk melakukan transfer pengetahuan ini melalui skema Pengabdian Kepada Masyarakat (PKM). Kegiatan ini merupakan implementasi nyata dari Tri Dharma Perguruan Tinggi, di mana akademisi turun langsung memberikan solusi atas permasalahan mitra. Dalam pelaksanaannya, kegiatan ini bermitra dengan SMK Negeri 6 Balikpapan yang memiliki basis siswa teknik yang relevan dengan materi keamanan siber.

Selain memberikan pemahaman akan kesadaran cyber, SMK Negeri 6 juga setiap tahunnya menyiapkan siswa untuk dapat mengikuti berbagai Lomba Kompetensi Siswa (LKS) yaitu kompetisi tahunan untuk siswa SMK seluruh Indonesia yang menguji keterampilan kejuruan sesuai bidangnya, dan salah satu bidang yang diikuti berkaitan dengan cybersecurity. Melalui kegiatan "Pelatihan Cybersecurity Awareness dan Simulasi Serangan Siber" ini, diharapkan tercipta ekosistem digital yang lebih aman di lingkungan sekolah. Tujuan utamanya adalah meningkatkan kewaspadaan siswa terhadap validitas data dan aplikasi, serta menanamkan etika berinternet yang aman. Dengan demikian, diharapkan siswa SMKN 6 Balikpapan tidak hanya mahir secara teknis, tetapi juga memiliki integritas dan kesadaran keamanan yang tinggi sebagai benteng pertahanan siber masa depan.

2. METODE PELAKSANAAN

Kegiatan pengabdian kepada masyarakat ini menggunakan pendekatan pelatihan partisipatif dan simulasi IPTEKS. Fokus utama metode ini bukan sekadar transfer teknologi teknis, melainkan pemberdayaan siswa agar memiliki kemandirian dalam mendeteksi dan memitigasi ancaman siber secara dini. Kegiatan ini berjumlah 33 siswa yang berasal dari jurusan Teknik Komputer dan Jaringan (TKJ) di SMKN 6 Balikpapan. Karakteristik peserta adalah individu *digital natives* yang memiliki latar belakang pengetahuan dasar jaringan komputer, namun masih memiliki kerentanan tinggi terhadap serangan siber akibat perilaku daring yang berisiko. Selain itu, pemilihan peserta didasarkan pada kebutuhan mitra untuk menyiapkan delegasi siswa dalam menghadapi Lomba Kompetensi Siswa (LKS) bidang *cybersecurity*.

Metode Pelaksanaan dipilih untuk memberikan pengalaman praktis *(hands-on)* kepada siswa mengenai konsep keamanan ofensif dan defensif dalam lingkungan yang terkontrol (Prasetia et al., 2024).



Gambar 1. Tahapan Pelaksanaan Pelatihan

Pelaksanaan kegiatan di mana total durasi selama 3 jam dibagi menjadi tiga tahapan utama, yaitu tahap persiapan, tahap pelaksanaan pelatihan, dan tahap evaluasi.

a) Tahap Persiapan dan Pengenalan (15 Menit); Tahap ini diawali dengan sesi pembukaan yang memaparkan latar belakang pentingnya kesadaran keamanan siber serta tujuan kegiatan. Pada tahap ini, dilakukan proses distribusi alat dan bahan praktikum kepada peserta. Mengingat simulasi serangan siber berisiko tinggi jika dilakukan pada jaringan publik, persiapan difokuskan pada pembangunan lingkungan laboratorium virtual (Virtual Lab). Peserta dibimbing untuk menyiapkan perangkat lunak virtualisasi (VirtualBox), sistem operasi penyerang (attacker) menggunakan Kali Linux, dan sistem operasi target (victim) menggunakan Windows.
b) Tahap Pelaksanaan Pelatihan merupakan inti kegiatan yang terdiri dari beberapa sesi terstruktur:
    1) Pre-test (15 menit); Sebelum masuk ke materi teknis, peserta mengerjakan soal pre-test. Aktivitas ini bertujuan untuk mengukur tingkat pengetahuan dasar (baseline knowledge) siswa mengenai terminologi keamanan siber dan jenis-jenis serangan sebelum menerima materi.
    2) Simulasi Serangan (90 menit); Sesi ini dilakukan sepenuhnya di dalam lingkungan virtual. Instruktur mendemonstrasikan dan membimbing siswa menggunakan framework Metasploit pada Kali Linux. Siswa melakukan simulasi pembuatan payload berbahaya yang disamarkan menjadi file eksekusi (.exe). Skenario serangan dijalankan ketika "korban" (Windows) mengeksekusi file tersebut, yang memungkinkan penyerang mendapatkan akses kontrol penuh terhadap sistem target.
    3) Mitigasi dan Monitoring (30 menit): Setelah serangan berhasil, fokus beralih pada sisi pertahanan. Siswa diajarkan cara mendeteksi keberadaan koneksi mencurigakan yang sedang aktif. Teknik yang diajarkan adalah verifikasi koneksi jaringan menggunakan perintah netstat pada command prompt untuk mengidentifikasi Foreign Address yang tidak dikenal, serta memutus serangan tersebut secara manual.
c) Tahap Evaluasi dan Penutup (30 Menit); Setelah sesi simulasi berakhir, kegiatan dilanjutkan dengan post-test untuk mengukur peningkatan pemahaman siswa pasca pelatihan. Data dari pre-test dan post-test kemudian dibandingkan untuk melihat

efektivitas metode pelatihan. Rangkaian kegiatan ditutup dengan penyerahan sertifikat pelatihan sebagai bukti kompetensi dan partisipasi siswa dalam kegiatan peningkatan kesadaran keamanan siber ini.

Keberhasilan program pemberdayaan ini diukur menggunakan instrumen tes yang mencakup 10 butir pertanyaan strategis, mulai dari aspek kesadaran umum seperti manajemen kata sandi dan *phishing* hingga aspek teknis operasional. Peningkatan selisih nilai antara *pre-test* dan *post-test* menjadi indikator utama tercapainya tujuan pengabdian dalam membangun benteng pertahanan siber di lingkungan sekolah

3. HASIL DAN PEMBAHASAN

Pelaksanaan Kegiatan Kegiatan pengabdian kepada masyarakat ini dilaksanakan di SMKN 6 Balikpapan dengan partisipasi aktif dari siswa jurusan Teknik Komputer dan Jaringan (TKJ). Beberapa aktivitas pelaksanaan ditampilkan mulai dari tahap awal yang ditunjukkan Gambar 2. Setelah pemahaman dasar terbentuk, kegiatan dilanjutkan dengan sesi inti yaitu pelatihan teknis dan simulasi. Sesi ini dilakukan menggunakan lingkungan virtual (Virtual Lab) untuk memastikan keamanan jaringan sekolah dan didokuentasikan dalam Gambar 3.

Gambar 2. Sesi Pembukaan dan Pemaparan Materi Dasar Keamanan Siber

Gambar 3. Peserta Melakukan Simulasi Serangan Menggunakan Metasploit pada Kali Linux

Selanjutnya, pelatihan berfokus pada sisi defensif (defensive security). Peserta diajarkan cara mendeteksi serangan yang sedang berlangsung secara real-time. Siswa melakukan praktik monitoring lalu lintas jaringan menggunakan perintah netstat pada Command Prompt di sistem operasi Windows. Praktik ini bertujuan agar siswa mampu mengidentifikasi koneksi asing dan memutus jalur serangan tersebut, sebagaimana ditunjukkan pada Gambar 4.

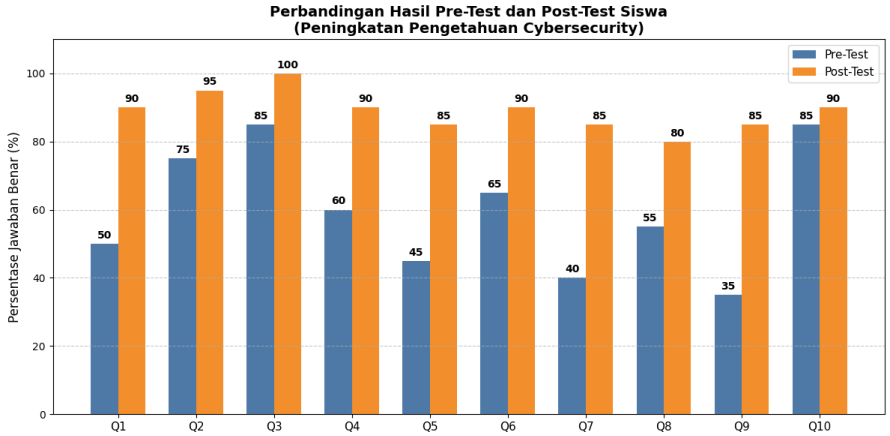

Gambar 4. Praktik Verifikasi Koneksi Jaringan dan Mitigasi Serangan

Berdasarkan data yang dikumpulkan dari setiap tahapan, peningkatan signifikan rata-rata nilai siswa sebesar 29% (dari 60% menjadi 89%) membuktikan bahwa metode simulasi serangan nyata atau live hacking jauh lebih efektif dibandingkan pendekatan konvensional yang hanya berbasis teori yang ditunjukkan pada Tabel 1. Dari Tabel 1, ditampilkan juga dalam bentuk visualisasi data pada Gambar 5 mempertegas efektivitas metode pelatihan yang diterapkan. Grafik batang berwarna oranye (Post-test) secara konsisten menunjukkan posisi yang lebih tinggi dibandingkan grafik biru (Pre-test) di seluruh butir pertanyaan.

Tabel 1. Hasil Evaluasi Perbandingan *Pre-Test* dan *Post-Test* Pengetahuan Keamanan Siber

No	Daftar Pertanyaan (Instrumen Tes)	Jawaban Benar (%) *(Pre-Test)*	Jawaban Benar (%) *(Post-Test)*
1	Keamanan siber hanya berkaitan dengan pemasangan antivirus pada komputer.	50%	90%
2	*Phishing* adalah upaya penipuan untuk mencuri data sensitif melalui tautan palsu.	75%	95%
3	Menggunakan *password* yang sama untuk semua akun media sosial adalah tindakan aman.	85%	100%
4	Kali Linux adalah sistem operasi yang umum digunakan untuk pengujian penetrasi (*penetration testing*).	60%	90%
5	File dengan ekstensi .exe selalu aman untuk dibuka jika dikirim oleh teman.	45%	85%
6	*Social Engineering* memanfaatkan kelemahan psikologis manusia, bukan kelemahan perangkat keras.	65%	90%
7	Metasploit adalah *framework* yang digunakan untuk membuat dokumen teks, bukan serangan siber.	40%	85%
8	Serangan siber dapat terjadi meskipun komputer tidak terhubung ke internet sama sekali.	55%	80%
9	Perintah netstat pada Command Prompt digunakan untuk memantau koneksi jaringan yang aktif.	35%	85%
10	Memperbarui (*update*) sistem operasi penting untuk menambal celah keamanan.	85%	90%
	Rata-rata	60%	89%

Dari hasil yang didapatkan, secara metodologis, hal ini terjadi karena simulasi memberikan bukti yang kuat sehingga mengubah pemahaman abstrak menjadi pengalaman konkret. Siswa tidak hanya menghafal definisi serangan, tetapi memvalidasi pengetahuan tersebut melalui praktik langsung dalam lingkungan virtual yang aman. Keberhasilan ini sejalan dengan pelatihan (Harjito et al., 2025) yang menyatakan bahwa pembelajaran berbasis pengujian penetrasi mampu meningkatkan keterlibatan aktif siswa secara drastis dibandingkan pembelajaran teori.



Gambar 5. Grafik Perbandingan Peningkatan Pengetahuan Siswa (Pre-test vs Post-test)

Tidak hanya itu, Hasil ini juga diperkuat oleh temuan (Ira et al., 2022) dalam pengabdian di SMK Negeri 2 Salatiga, yang menyatakan bahwa edukasi keamanan siber yang disertai demonstrasi praktis dan pendampingan mampu meningkatkan keterampilan mandiri siswa dalam mengamankan data pribadi serta memitigasi serangan siber secara lebih efektif dibandingkan hanya melalui sosialisasi satu arah.

Berdasarkan observasi selama kegiatan, terjadi perubahan sikap yang nyata pada siswa SMKN 6 Balikpapan. Pada awal sesi, mayoritas peserta menunjukkan sikap pasif dan menganggap remeh keamanan digital karena merasa sudah cukup terlindungi oleh perangkat lunak antivirus. Namun, antusiasme melonjak drastis saat sesi simulasi dimulai; siswa yang semula ragu menjadi sangat ingin tahu dan mulai berpikir kritis tentang setiap tautan atau file yang mereka temui. Respon dari pihak sekolah selaku mitra sangat positif; guru pendamping menyatakan bahwa materi keamanan ofensif ini merupakan bagian yang selama ini hilang dari kurikulum TKJ standar, yang selama ini lebih banyak fokus pada aspek fungsionalitas jaringan tanpa menyadari celah keamanannya. Hasil dari kegiatan ini memiliki implikasi krusial bagi SMKN 6 Balikpapan, terutama dalam meningkatkan daya saing siswa pada ajang Lomba Kompetensi Siswa (LKS) bidang cybersecurity. Secara institusional, pelatihan ini menjadi dasar bagi sekolah untuk mengembangkan ekosistem digital yang lebih aman melalui peningkatan literasi teknis calon administrator jaringan masa depan. Untuk menjaga keberlanjutan program, tim PKM merekomendasikan agar pihak mitra mengintegrasikan modul simulasi serangan siber praktis ini ke dalam kurikulum muatan lokal atau sebagai materi inti pada kegiatan ekstrakurikuler bidang IT. Dengan demikian, penguasaan aspek defensive security tidak hanya menjadi kegiatan sesaat, melainkan menjadi kompetensi berkelanjutan yang melekat pada lulusan SMKN 6 Balikpapan di tengah ancaman siber yang terus berevolusi.

Meskipun secara keseluruhan kegiatan berjalan dengan sukses, tim PKM mengidentifikasi beberapa kendala di lapangan yang dapat menjadi pelajaran untuk program di masa mendatang:

1) Kendala Teknis Infrastruktur: Beberapa komputer di laboratorium sekolah memiliki spesifikasi perangkat keras (RAM dan CPU) yang terbatas, sehingga mengalami perlambatan saat menjalankan mesin virtual (VirtualBox) secara simultan.
2) Variasi Kecepatan Pemahaman Siswa: Mengingat peserta terdiri dari 45 siswa dari dua kelas yang berbeda, terdapat perbedaan kecepatan dalam menyerap instruksi teknis mengenai perintah baris *(command line interface)*.
3) Keterbatasan Durasi: Waktu 3 jam dirasakan sangat padat untuk mencakup teori sekaligus simulasi serangan yang kompleks.

Dari kendala yang dialami, sebagai bentuk evaluasi kedepan tim melakukan optimasi dengan melakukan prainstalasi konfigurasi pada setiap mesin virtual sebelum sesi dimulai, sehingga beban komputasi dapat diminimalisir selama kegiatan berlangsung, menerapkan strategi pendampingan sejawat dengan melibatkan mahasiswa sebagai asisten instruktur yang ditempatkan di setiap kelompok kecil. Hal ini memungkinkan siswa yang mengalami kesulitan teknis mendapatkan bantuan langsung tanpa mengganggu ritme instruksi utama. Tim juga

melakukan efisiensi dengan menyediakan modul cetak yang dapat diakses melalui platform online canva.

4. KESIMPULAN

Kegiatan pengabdian kepada masyarakat ini telah berhasil meningkatkan kesadaran dan kompetensi keamanan siber siswa SMKN 6 Balikpapan secara signifikan, yang dibuktikan dengan kenaikan rata-rata nilai evaluasi dari 60% menjadi 89%. Nilai tambah utama dari program PKM ini dibandingkan pelatihan konvensional terletak pada penggunaan metode offensive security melalui simulasi live hacking. Pendekatan ini terbukti mampu mengubah paradigma siswa dari sekadar mengetahu menjadi waspada karena mereka melihat langsung kerentanan sistem dari sudut pandang penyerang. Secara metodologis, artikel ini memberikan kontribusi nyata bagi praktik pengabdian masyarakat dengan menawarkan model edukasi keamanan siber yang aplikatif bagi jenjang sekolah menengah kejuruan (SMK). Model ini menjembatani kesenjangan antara kurikulum sekolah yang berfokus pada fungsionalitas dengan tuntutan industri yang memprioritaskan keamanan infrastruktur. Sebagai tindak lanjut, disarankan agar pihak sekolah dapat mengintegrasikan materi keamanan siber praktis ke dalam kurikulum muatan lokal atau kegiatan ekstrakurikuler, guna menjaga keberlanjutan kompetensi siswa di tengah ancaman siber yang terus berkembang.

UCAPAN TERIMA KASIH

Tim pelaksana menyampaikan terima kasih kepada Program Studi Teknologi Informasi, Universitas Mulia yang telah membantu terlaksananya kegiatan Pengabdian dalam bentuk dana kegiatan serta kepada SMK Negeri 6 Balikpapan sebagai tempat penyelenggara kegiatan.

REFERENSI

Afandi, I. A., Kusyanti, A., & Wardani, N. H. (2017). Analisis hubungan kesadaran keamanan, privasi informasi, dan perilaku keamanan pada para pengguna media sosial Line. *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, *1*(9), 783–792.

Aulia, N., Harahap, U. H., & Silitonga, N. E. (2025). Tantangan Dan Strategi Manajemen Kurikulum Di Era Digital : Studi Literatur Untuk Inovasi Pendidikan Challenges And Strategies Of Curriculum Management In The Digital Era : A Literature Study For Educational Innovation. *JIIC: Jurnal Intelek Insan Cendikia*, 10283–10302.

Harjito, B., Prasetyo, H., & Sihwi, S. W. (2025). Pelatihan Keamanan Siber Sebagai Pengetahuan Dasar Keamanan Untuk Peningkatan Security Awarness. *Jurnal Ilmu Pengetahuan, Teknologi, Dan Seni Bagi Masyarakat*, *V*(1).

Idris, N. B., Wijayanto, A., Insan, P. P., & ... (2023). Pelatihan Aplikasi Open Broadcaster Software Dan Canva Guru-Guru Smk Negeri 5 Balikpapan. *Jurnal …*, *2*(2), 109–113. https://doi.org/10.47002/jpm.v2i2.688

Ira, P., Candra, D., Perdana, D. P., Kurniawan, A. A., & Fauzi, R. (2022). Sosialisasi Cyber Security Awareness untuk meningkatkan literasi digital di SMK N 2 Salatiga. *Kacanegara Jurnal Pengabdian Pada Masyarakat*, *6717*, 213–218.

Kahar, M. I., Cika, H., Afni, N., & Wahyuningsih, N. E. (2021). Pendidikan era revolusi industri 4.0 menuju era society 5.0 di masa pandemi covid 19. *Moderasi: Jurnal Studi Ilmu Pengetahuan Sosial*, *2*(1), 58–78.

Marwati, F., Astofa, A., Studi, P., Informasi, S., Pamulang, U., & Security, D. (2025). *Pelatihan Cyber Security Sebagai Pengetahuan Dasar Keamanan Untuk Peningkatan Security Awarness*. *3*.

Pradana, D. S. S. (2024). *Pengembangan Hack The Box: sebagai Prototype Media Pembelajaran Keamanan Jaringan Komputer Berbasis Open Source*.

Prasetia, O., Machfud, S., Ibnurhus, G. A., Studi, P., Informasi, S., Pamulang, U., Conditioner, A., & Computer, P. (2024). Sosialiasi Pengenalan Pentingnya Cyber Security Guna Menjaga Keamanan Data Di Era Digital Pada Siswa / I SMK Bakti Idhata Jakarta. *JIPM: Jurnal Inovasi Pengabdian Masyarakat*, *2*, 16–20.

Puteri, A. R., Nasution, W. N., & Nasution, M. I. P. (2025). Integrasi teknologi informasi dan komunikasi dalam pendidikan: konsep, perkembangan, dan inovasi media pembelajaran. *Jurnal Pendidikan Indonesia: Teori, Penelitian, Dan Inovasi*, *5*(4).

Revilia, D., & Irwansyah, N. (2020). Social Media Literacy: Millenial's Perspective of Security and Privacy Awareness. *Jurnal Penelitian Komunikasi Dan Opini Publik*, *24*(1), 478416.

Suhendra, I. (2024). *Model Pembelajaran Teaching Factory Dalam Meningkatkan Kompetensi Keahlian Siswa Pada Konsentrasi Keahlian Teknik Komputer Dan Jaringan Di SMK Aceh Selatan (Kajian Multi Situs)*. Universitas Bina Bangsa Getsempena.

Tandirerung, V. A., Riana T. Mangesa, & Syahrul. (2023). Pengenalan Cyber Security Bagi Siswa Sekolah Menengah Atas. *Teknovokasi : Jurnal Pengabdian Masyarakat*, *1*(2), 89–94. https://doi.org/10.59562/teknovokasi.v1i2.131

Wijayanto, A. (2024). Mengenal Cybersecurity: Perlindungan Data Pribadi Dan Privasi Di Sma Negeri 1 Samboja. *Jurnal Mulia*, *3*(2), 165–172. https://doi.org/10.47002/jpm.v3i2.867

Wijayanto, A., Riadi, I., & Prayudi, Y. (2023). Taara Method for Processing on the Network Forensics in the Event of an ARP Spoofing Attack. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *7*(2), 208–217. https://doi.org/10.29207/resti.v7i2.4589

Yudistira, N., Lamba, E. F., Jauhari, R., Farhanna, F. R., & Yayu'Palangan, C. (2025). Penyuluhan Keamanan Informasi Terkait Ancaman Phishing untuk Meningkatkan Literasi Digital Warga Kompleks Yadara Babarsari Yogyakarta. *GIAT: Teknologi Untuk Masyarakat*, *4*(1), 52–63.