

Implementasi Edukasi waspada Cyber Crime di Era AI membangun budaya internat pada Pelajar SMKS Yadika Baturaja

Jum Dapiokta¹, Anggraini Agustin Muris², Joko Kuswanto³, Reza Bayu Ardhiyansah⁴, Selvia Karina Agatha⁵, M.Dion Regan Desta⁶

^{1 2 3 4 5 6}) Program Studi Informatika, Fakultas Teknik dan Komputer Universitas Baturaja
Jl. Ratu Penghulu No. 2301, Karang Sari, Baturaja, Tj. Baru, Kec. Baturaja Timur, Kabupaten Ogan Komering Ulu, Sumatera Selatan 32115

* E-mail: jumdapiokta@gmail.com, miss.muris@gmail.com, ko.8515@gmail.com,
rezabayuardhiyansah@gmail.com, selviatarin@gmail.com, dstaprtma32@gmail.com

ABSTRAK

Pesatnya perkembangan teknologi Artificial Intelligence (AI) tidak hanya membawa inovasi, melainkan juga meningkatkan risiko kejahatan siber (cybercrime) seperti phishing dan penyebaran malware yang menasar kelompok remaja rentan. Kegiatan pengabdian kepada masyarakat ini bertujuan untuk meningkatkan kesadaran cyber hygiene serta membekali kecakapan digital siswa di SMKS Yadika Baturaja melalui pelatihan pengamanan akun. Metode pelaksanaan yang diterapkan dalam program ini adalah pendekatan edukatif-partisipatif, yang mengombinasikan sesi seminar interaktif mengenai mitigasi ancaman siber dengan sesi hands-on experience berupa praktik mandiri terbimbing. Kegiatan ini diikuti secara penuh oleh 25 siswa aktif sebagai khalayak sasaran. Hasil pelaksanaan menunjukkan bahwa pendekatan edukatif terbukti efektif mentransformasi pola pikir siswa terhadap pentingnya perlindungan privasi data pribadi. Melalui sesi partisipatif, sebanyak 15 siswa (60%) berhasil mengonfigurasi dan mengaktifkan fitur verifikasi dua langkah (2-Step Verification) secara real-time hingga mencapai status terlindungi (secured). Seluruh rangkaian pelatihan berlangsung optimal tanpa ditemukan kendala teknis yang berarti di lapangan, didukung oleh kesiapan infrastruktur gawai dan jaringan internet sekolah yang stabil. Sementara itu, 10 siswa (40%) sisanya diarahkan untuk menyelesaikan proses aktivasi secara mandiri di rumah menggunakan modul panduan cetak yang telah didistribusikan. Pengabdian ini menyimpulkan bahwa integrasi antara edukasi teoritis dan praktik pertahanan teknis yang aplikatif mampu menjadi langkah preventif yang strategis dalam membangun ekosistem digital yang aman dan bertanggung jawab di lingkungan sekolah kejuruan.

Kata Kunci : Keamanan Siber, Verifikasi Dua Langkah, Edukatif-Partisipatif, Cyber Hygiene, Kecerdasan Buatan

ABSTRACT

The rapid development of Artificial Intelligence (AI) technology not only brings innovation but also increases the risk of cybercrime, such as phishing and malware distribution targeting vulnerable tech-dependent teenagers. This community service activity aims to improve cyber hygiene awareness and equip students at SMKS Yadika Baturaja with practical digital safety skills through account security training. The implementation method applied in this program was an educative-participatory approach, combining an interactive seminar session on cyber threat mitigation with a hands-on experience session through guided independent practice. This activity was fully attended by 25 active students as the target audience. The results demonstrated that the educative approach effectively transformed students' mindsets regarding the urgency of personal data protection. Through the participatory session, as many as 15 students (60%) successfully configured and activated the 2-Step Verification feature on their devices in real-time to achieve a secured status. The entire training series ran optimally without any significant technical obstacles encountered in the field, heavily supported by the readiness of students' gadgets and stable school internet infrastructure. Meanwhile, the remaining 10 students (40%) were directed to complete the activation process independently at home using the printed guide modules distributed by the team. This service concludes that the integration of theoretical education and applicable technical defense practices can serve as a strategic preventive measure in building a safe and responsible digital ecosystem within the vocational school environment. Keywords: Keyword 1, Keyword 2, Keyword 3. (Maximum of 4 Keywords)



Informasi Artikel

Submit 1 April 2026 | Diterima 29 April 2026 | Publish Online 30 Mei 2026

..... This is an open access article under the [CC BY 4.0](https://creativecommons.org/licenses/by/4.0/) license

DOI: <https://doi.org/10.71200/diasya.v2i1.233> | Published by Citra Air Nusantara



PENDAHULUAN

Perkembangan teknologi internet di era digital telah membawa perubahan yang sangat signifikan dalam berbagai aspek kehidupan manusia, terutama dalam sektor pendidikan dan interaksi sosial. Terlebih dengan hadirnya era *Artificial Intelligence* (AI) atau kecerdasan buatan, lanskap digital menjadi kian dinamis sekaligus kompleks. Bagi generasi muda, khususnya kelompok remaja yang duduk di bangku Sekolah Menengah Kejuruan (SMK), internet telah menjadi kebutuhan pokok yang digunakan setiap hari untuk belajar, berkomunikasi, hingga mencari hiburan. Namun, di balik segala kemudahan dan potensi positif yang ditawarkan, ruang siber di era AI juga menyimpan ancaman keamanan yang nyata karena modus penipuan dan peretasan kini menjadi lebih tersamar dan otomatis. Kurangnya pemahaman mengenai etika digital membuat kelompok usia ini menjadi salah satu target yang paling rentan terhadap berbagai bentuk kejahatan siber (*cybercrime*).

Kondisi khalayak sasaran di SMKS Yadika Baturaja menunjukkan bahwa sebagian besar pelajar sangat aktif mengoperasikan perangkat digital dan media sosial. Kendati demikian, aktivitas digital yang tinggi ini belum diimbangi dengan kesadaran yang cukup mengenai keamanan siber dan perlindungan data pribadi. Banyak pelajar yang belum menyadari bahaya laten internet, seperti bagaimana virus atau *malware* modern dapat menyusup dan membahayakan keselamatan akun-akun digital mereka. Kelemahan dalam pengamanan akun pribadi, seperti penggunaan kata sandi yang sederhana dan tidak adanya lapisan keamanan ganda, membuat akun media sosial maupun akun akademik mereka menjadi sasaran empuk aksi peretasan, pencurian identitas, hingga penyalahgunaan data.

Masalah utama yang dihadapi adalah rendahnya literasi mengenai pencegahan *cybercrime* dan minimnya penerapan praktik keamanan teknis yang mendasar di kalangan siswa. Oleh karena itu, diperlukan sebuah langkah preventif yang nyata untuk menjembatani kesenjangan pemahaman ini. Edukasi mengenai etika profesi dan keamanan siber menjadi sangat krusial untuk diberikan agar para siswa tidak hanya mampu menggunakan teknologi, tetapi juga memiliki tanggung jawab moral dan kemampuan teknis dalam melindungi diri mereka di dunia maya.

Berdasarkan permasalahan tersebut, kegiatan pengabdian kepada masyarakat ini dilaksanakan dengan tujuan untuk mengimplementasikan edukasi etika profesi guna meningkatkan kesadaran dan kewaspadaan terhadap bahaya *cybercrime* di era AI pada pelajar SMKS Yadika Baturaja. Target yang hendak dicapai melalui kegiatan seminar dan sosialisasi ini adalah membekali para siswa dengan pengetahuan komprehensif mengenai berbagai ancaman internet, mengenalkan jenis-jenis virus yang dapat merusak atau mencuri data, serta memberikan keterampilan praktis. Melalui panduan langsung dalam mengaktifkan fitur verifikasi dua langkah (*2-Step Verification*) pada akun mereka, diharapkan kegiatan ini dapat membentuk benteng pertahanan utama yang efektif bagi siswa, sehingga tercipta generasi digital yang cerdas, waspada, dan bertanggung jawab.

METODE PELAKSANAAN

Metode yang digunakan dalam kegiatan pengabdian kepada masyarakat ini adalah pendekatan edukatif-partisipatif. Pendekatan ini menggabungkan penyaluran pemahaman teoretis secara interaktif (edukatif) dengan keterlibatan aktif khalayak sasaran secara langsung dalam mempraktikkan materi keamanan siber (partisipatif). Melalui metode ini, siswa tidak hanya ditempatkan sebagai pendengar pasif, melainkan sebagai subjek yang terlibat aktif dalam mengamankan identitas digital mereka sendiri.

Secara sistematis, alur pelaksanaan kegiatan pengabdian ini dirancang melalui tahapan-tahapan yang runtut sebagai berikut:

1. Waktu, Tempat, dan Sasaran Kegiatan

Kegiatan pengabdian ini dilaksanakan pada hari Senin, 15 Juni 2026 bertempat di Aula SMKS Yadika Baturaja. Sasaran kegiatan ini adalah siswa-siswi aktif SMKS Yadika Baturaja yang berjumlah 25 siswa. Peserta dipilih berdasarkan pertimbangan bahwa siswa SMK merupakan kelompok remaja produktif yang memiliki intensitas interaksi sangat tinggi dengan perangkat digital dan internet di kehidupan sehari-hari, namun masih memerlukan penguatan dari sisi kesadaran keamanan siber (*cyber hygiene*).

2. Alat dan Bahan Pendukung

Untuk menjamin kelancaran jalannya transfer pengetahuan dan penerapan metode partisipatif di lapangan, alat dan bahan yang digunakan meliputi:

- Perangkat laptop tim pengabdian dan fasilitas proyektor sekolah untuk memaparkan visualisasi materi.
- Perangkat gawai (*smartphone*) pribadi milik 25 siswa peserta sebagai media praktik langsung.
- Jaringan internet yang stabil untuk keperluan proses registrasi, menerima kode otentikasi, dan aktivasi fitur keamanan secara *real-time*.
- Slide presentasi interaktif dan modul panduan ringkas mengenai langkah-langkah aktivasi keamanan akun digital sebagai pegangan siswa.

3. Tahapan Implementasi Pendekatan Edukatif-Partisipatif

Pelaksanaan program pengabdian masyarakat ini dibagi ke dalam tiga tahapan utama yang terstruktur:

- Tahap Prapelaksanaan dan Perizinan

Langkah awal dilakukan melalui pendekatan birokrasi berupa koordinasi resmi dengan pihak mitra. Tim menemui Kepala Sekolah SMKS Yadika Baturaja secara langsung untuk memaparkan maksud, tujuan, serta menyelaraskan jadwal kegiatan agar tidak mengganggu proses KBM (Kegiatan Belajar Mengajar) reguler. Setelah mendapatkan persetujuan lisan, tim menyerahkan surat perizinan resmi dari universitas sebagai dokumen legalitas formal pelaksanaan kegiatan.

- Tahap Persiapan Materi

Pada tahap ini, tim menyusun modul dan materi edukasi secara matang dengan menyesuaikan karakteristik psikologis remaja agar tidak terkesan kaku. Materi yang dipersiapkan berfokus pada literasi digital dan mitigasi siber, yang meliputi: pengenalan lanskap *cybercrime* di era AI, bahaya infeksi virus dan *malware* pada perangkat komunikasi, serta pentingnya pembuatan kata sandi (*password*) yang kuat.

- Tahap Pelaksanaan (Penerapan Edukatif-Partisipatif)

Kegiatan inti dilaksanakan secara tatap muka dengan membagi durasi acara menjadi dua sesi utama yang saling berkesinambungan:

1. Sesi Edukatif (Seminar Interaktif): Pemateri menyampaikan paparan konsep materi keamanan siber selama kurang lebih 75 menit. Proses ini berjalan dua arah melalui sesi diskusi, bedah kasus nyata peretasan, dan tanya jawab untuk memicu kesadaran (*awareness*) serta penalaran kritis siswa mengenai pentingnya menjaga kerentanan data pribadi.
2. Sesi Partisipatif (*Hands-on Experience*): Setelah pembekalan teori, tim memberikan demonstrasi langsung di depan kelas mengenai cara mengonfigurasi fitur keamanan ganda. Melalui metode partisipatif ini, ke-25 siswa secara serempak mengoperasikan gawai pribadi masing-masing untuk melakukan praktik mandiri terbimbing. Siswa berpartisipasi penuh dalam mengeksplorasi menu pengaturan keamanan akun mereka dengan didampingi secara intensif oleh tim pengabdian untuk mengaktifkan fitur verifikasi dua langkah (*2-Step Verification*).

4. Metode Evaluasi Kegiatan

Evaluasi dilakukan pada akhir rangkaian kegiatan untuk mengukur tingkat keberhasilan dan efektivitas dari pendekatan edukatif-partisipatif yang telah diterapkan. Indikator evaluasi dinilai berdasarkan dua aspek utama:

1. Evaluasi Aspek Kognitif (Edukatif): Dinilai berdasarkan pemahaman, respon, dan kemampuan siswa dalam menjawab serta mengulas kembali mitigasi dasar terhadap ancaman *cybercrime* saat sesi diskusi bersama.
2. Evaluasi Aspek Psikomotorik (Partisipatif): Diukur melalui bukti visual keberhasilan teknis di lapangan, yaitu dengan menghitung secara langsung jumlah gawai siswa yang berhasil mengonfigurasi sistem pertahanan hingga fitur verifikasi dua langkah (*2-Step Verification*) pada akun personal mereka aktif dan berstatus terlindungi (*secured*).

HASIL DAN PEMBAHASAN

4.1 Analisis Kondisi Awal Peserta

Sebelum jalannya intervensi melalui pendekatan edukatif-partisipatif, tim pengabdian melakukan wawancara singkat secara acak untuk memetakan pemahaman awal ke-25 siswa SMKS Yadika Baturaja. Ditemukan fakta bahwa seluruh siswa (100%) merupakan pengguna aktif internet yang menghabiskan waktu lebih dari 5 jam per hari di ruang digital. Namun, mayoritas dari mereka memiliki kebiasaan *cyber hygiene* yang buruk, seperti menggunakan satu kata sandi yang sama untuk berbagai akun (email, Instagram, dan TikTok) serta mengabaikan peringatan keamanan yang muncul pada perangkat gawai mereka. Kondisi awal inilah yang mendasari urgensi dilaksanakannya seminar pencegahan *cybercrime* ini.

4.2 Pelaksanaan Metode Edukatif-Partisipatif

1. Capaian Sesi Edukatif (Seminar Interaktif)

Tahap pertama dari pengabdian ini berfokus pada aspek kognitif siswa melalui seminar interaktif. Tim pengabdian memaparkan lanskap kejahatan siber modern yang telah bertransformasi di era *Artificial Intelligence* (AI). Fokus materi diarahkan pada bagaimana teknologi AI disalahgunakan oleh pelaku kriminal untuk membuat pesan *phishing* yang sangat personal, serta penyebaran *malware* tersembunyi melalui unduhan aplikasi atau *game* ilegal yang kerap diakses oleh remaja.

Penyampaian materi dilakukan melalui diskusi dua arah, di mana siswa diajak membedah contoh kasus riil kebocoran data pribadi. Pendekatan edukatif ini terbukti efektif mengubah pola pikir (*mindset*) peserta. Dari hasil tanya jawab di akhir sesi, siswa yang awalnya menganggap pengamanan akun adalah hal yang rumit dan tidak penting, mulai menyadari bahwa identitas digital mereka sangat rentan jika tidak dilindungi dengan sistem keamanan tingkat lanjut.

2. Capaian Sesi Partisipatif (Praktik Mandiri Terbimbing)

Setelah kesadaran kognitif siswa terbentuk, kegiatan langsung beralih ke sesi partisipatif yang menekankan pada aspek psikomotorik atau keterampilan teknis. Ke-25 siswa diminta untuk bertindak sebagai subjek aktif dengan membuka menu pengaturan pada perangkat gawai pribadi masing-masing. Tim pengabdian memberikan demonstrasi visual langkah demi langkah mengenai cara mengonfigurasi fitur keamanan ganda.

Siswa berpartisipasi penuh dalam menyelaraskan nomor telepon aktif mereka, mencatat kode pemulihan darurat, hingga menyelesaikan sinkronisasi sistem otentikasi. Melalui keterlibatan aktif ini, siswa mendapatkan pengalaman langsung (*hands-on experience*) bahwa memperkuat pertahanan akun melalui verifikasi dua langkah (*2-Step Verification*) dapat dilakukan dengan cepat dan mudah.

4.3 Analisis Kuantitatif Keberhasilan Kegiatan

Untuk mengukur efektivitas dari implementasi metode edukatif-partisipatif ini, tim pengabdian melakukan rekapitulasi langsung terhadap capaian praktik siswa di lapangan. Data hasil pelaksanaan kegiatan pengabdian masyarakat ini dirangkum ke dalam Tabel 1 berikut:

Tabel 1. Rekapitulasi Capaian Praktis Aktivasi Fitur Keamanan Siswa

No.	Indikator Capaian	Jumlah Siswa	Persentase (%)
1	Berhasil mengaktifkan fitur 2-Step Verification selama pelatihan	15	60%
2	Belum menyelesaikan aktivasi dan memerlukan pendampingan lanjutan	10	40%
Total	Peserta Seminar	25	100%

Berdasarkan data pada Tabel 1, sebanyak 15 siswa (60%) berhasil mencapai status *secured* (terlindungi) secara *real-time* saat sesi pelatihan berlangsung. Keberhasilan ini menjadi bukti kuat bahwa metode edukatif-partisipatif yang diterapkan mampu memberikan transfer teknologi secara instan dan aplikatif kepada siswa SMK.

Sementara itu, terdapat 10 siswa (40%) yang belum menyelesaikan proses aktivasi hingga tahap akhir di lokasi. Berdasarkan hasil evaluasi tim pendamping, hal ini bukan disebabkan oleh kendala teknis dari sistem atau gawai, melainkan karena keterbatasan durasi waktu seminar. Beberapa siswa memerlukan verifikasi nomor telepon cadangan yang terikat dengan perangkat orang tua mereka di rumah. Untuk mengantisipasi hal tersebut, tim pengabdian telah membagikan modul dan panduan cetak ringkas agar 10 siswa tersebut dapat menyelesaikan proses konfigurasi secara mandiri di rumah bersama keluarga.

4.4 Analisis Kendala Lapangan dan Keberlanjutan

Secara keseluruhan, jalannya pelatihan ini berlangsung dengan sangat lancar. Tidak ditemukan kendala teknis yang berarti di lapangan, seperti kegagalan jaringan atau perangkat yang tidak kompatibel. Faktor pendukung utama keberhasilan ini adalah tersedianya jaringan internet yang stabil di aula sekolah serta spesifikasi gawai milik ke-25 siswa yang sudah mendukung sistem operasi modern, sehingga proses penerimaan kode otentikasi (OTP) berjalan tanpa penundaan (*delay*).

Dampak jangka panjang dari kegiatan ini adalah terbentuknya ekosistem digital yang lebih aman di lingkungan SMKS Yadika Baturaja. Pengetahuan yang didapat oleh 25 peserta ini diharapkan dapat ditularkan kepada rekan-rekan sejawat mereka di sekolah, sehingga siswa mampu menjadi agen perubahan (*agent of change*) dalam membangun budaya aman berinternet di Kota Baturaja.

4.5 Dokumentasi Visual Pelaksanaan Kegiatan

Sebagai bukti autentik pelaksanaan pengabdian masyarakat dengan metode edukatif-partisipatif di lapangan, berikut disajikan dokumentasi visual jalannya kegiatan:

1. Implementasi Sesi Edukatif (Seminar)

Penyampaian materi dilakukan dengan bantuan media visual dan studi kasus riil mengenai ancaman kebocoran data di era digital. Gambar 1 menunjukkan suasana di aula sekolah saat ke-25 peserta menyimak pemaparan materi dari tim pengabdi dengan antusiasme yang tinggi.



Gambar 1. Pemaparan Materi Lanskap Cybercrime Era AI kepada Siswa SMKS Yadika Baturaja.

2. Implementasi Sesi Partisipatif (Praktik Terbimbing)

Setelah pembekalan teori, siswa diajak langsung terlibat aktif dalam mengamankan perangkat komunikasi mereka. Gambar 2 mendokumentasikan momen pendampingan intensif oleh tim pengabdi dalam memandu langkah demi langkah konfigurasi dan aktivasi fitur keamanan ganda pada gawai siswa.



Gambar 2. Pendampingan Praktis Aktivasi Fitur 2-Step Verification pada Gawai Siswa.

Pemahaman peserta diamati secara langsung oleh pemateri dan panitia selama sesi berlangsung. Berdasarkan hasil pengamatan, sebagian besar peserta mengaku masih banyak belum memahami tentang *cybercrime*.

Penutupan kegiatan dilaksanakan pukul 11.00 WIB dengan agenda penyerahan sertifikat dan kenang kenangan kepada pemateri dan pihak sekolah sebagai bentuk apresiasi, penghargaan atas dedikasi mereka dalam berbagi ilmu dan pengalaman kepada siswa SMKS Yadika.



Gambar 3. Penyerahan penghargaan dan Kenang kenangan serta Foto bersama dengan seluruh peserta

KESIMPULAN

Implementasi pendekatan edukatif-partisipatif dalam kegiatan pengabdian kepada masyarakat yang berfokus pada penguatan literasi digital dan mitigasi *cybercrime* di era kecerdasan buatan (*Artificial Intelligence*) pada pelajar SMKS Yadika Baturaja telah berhasil dilaksanakan dengan sangat optimal. Melalui intervensi yang terstruktur ini, tim pengabdian berhasil menjembatani kesenjangan pemahaman mengenai pentingnya etika profesi teknologi informasi dan penerapan aspek keamanan siber yang mendasar pada kelompok usia remaja. Kegiatan yang dirancang secara tatap muka ini mampu mentransformasi pola pikir serta kebiasaan *cyber hygiene* para siswa yang sebelumnya masih sangat rentan menjadi jauh lebih waspada, adaptif, dan responsif dalam menghadapi berbagai anomali serta ancaman kebocoran data di ruang digital yang kian kompleks.

Melalui pendekatan edukatif yang diterapkan pada sesi seminar interaktif, seluruh siswa yang berjumlah 25 orang menunjukkan peningkatan kesadaran kognitif yang sangat signifikan. Penyampaian materi yang dikemas secara dinamis dengan membedah studi kasus riil mengenai serangan virus, penyusupan *malware*, dan modus peretasan akun terbukti mampu membuka wawasan kritis para peserta. Siswa kini tidak lagi memandang sebelah mata pentingnya keamanan privasi dan mampu mengenali indikasi awal dari ancaman siber yang tersamar. Dampak edukatif ini menjadi fondasi yang krusial bagi para pelajar agar tidak hanya cakap dalam mengoperasikan teknologi digital untuk kebutuhan hiburan atau akademik, melainkan juga memiliki tanggung jawab moral dan etis untuk menjaga integritas data pribadi mereka di dunia maya.

Lebih lanjut, keberhasilan dari kegiatan pengabdian ini dipertegas oleh implementasi metode partisipatif melalui sesi *hands-on experience* atau praktik mandiri terbimbing menggunakan gawai pribadi masing-masing siswa. Pada tahapan aplikatif ini, sebanyak 15 siswa (60%) tercatat terlibat secara aktif hingga tuntas dan berhasil mengonfigurasi serta mengaktifkan fitur verifikasi dua langkah (*2-Step Verification*) secara *real-time* hingga akun personal mereka berstatus terlindungi. Capaian psikomotorik yang instan ini menjadi indikator kuat bahwa transfer keterampilan teknis (*digital safety skills*) dapat diadopsi dengan baik oleh para pelajar tingkat menengah kejuruan apabila disertai dengan demonstrasi visual dan pendampingan yang intensif dari tim pengabdian di lapangan.

Pelaksanaan seluruh rangkaian program pelatihan ini secara umum berjalan dengan sangat lancar tanpa adanya kendala teknis yang berarti di lapangan. Dukungan fasilitas infrastruktur dari pihak sekolah berupa stabilitas jaringan internet yang memadai serta kesiapan perangkat gawai milik siswa yang sudah mendukung sistem operasi modern menjadi faktor komplementer yang mempercepat proses otentikasi data tanpa hambatan penundaan waktu. Sementara itu, bagi 10 siswa (40%) yang belum menyelesaikan seluruh tahapan konfigurasi di lokasi karena keterbatasan durasi waktu seminar untuk sinkronisasi nomor telepon cadangan keluarga, proses mitigasi tetap terkawal dengan baik melalui pendistribusian modul panduan cetak ringkas agar proses aktivasi mandiri dapat diselesaikan secara tuntas di lingkungan rumah masing-masing.

Secara menyeluruh, pengabdian masyarakat ini menegaskan bahwa edukasi bahaya internet yang dikombinasikan secara berimbang dengan praktik keamanan teknis yang aplikatif merupakan langkah preventif yang sangat strategis demi memitigasi kerentanan digital pada generasi muda. Output konkret berupa pengamanan akun secara langsung ini diharapkan mampu membentuk benteng pertahanan utama yang kokoh pada diri siswa, sehingga ekosistem digital yang aman, cerdas, waspada, dan bertanggung jawab dapat tercipta secara berkelanjutan di lingkungan SMKS Yadika Baturaja. Pengetahuan yang telah diperoleh oleh para peserta ini juga diharapkan dapat ditularkan secara organik kepada rekan sebaya dan keluarga, sehingga mereka mampu bertindak sebagai agen perubahan (*agent of change*) dalam membangun budaya aman berinternet di Kota Baturaja.

UCAPAN TERIMA KASIH

Tim pengabdian menyampaikan rasa terima kasih yang sebesar-besarnya kepada Lembaga Penelitian dan Pengabdian kepada Masyarakat (LPPM) Universitas Baturaja yang telah memberikan dukungan, fasilitas, serta legalitas formal sehingga kegiatan pengabdian masyarakat ini dapat berjalan dengan lancar. Apresiasi dan ucapan terima kasih yang tulus juga kami sampaikan kepada Kepala Sekolah, segenap guru, dan staf administrasi SMKS Yadika Baturaja atas izin, kerja sama, dan penyediaan fasilitas tempat yang sangat memadai selama persiapan hingga pelaksanaan kegiatan. Tidak lupa, tim pengabdian mengucapkan terima kasih kepada seluruh siswa-siswi peserta yang telah berpartisipasi aktif dengan penuh antusiasme, serta semua pihak yang telah membantu menyelesaikan pelaksanaan kegiatan pengabdian ini hingga naskah jurnal ini dapat diselesaikan dengan baik.

DAFTAR PUSTAKA

- Asari, A., Kurniawan, T., & Nugroho, A. (2022). Peningkatan literasi *cyber hygiene* melalui pelatihan pengamanan akun digital bagi remaja. *Jurnal Pengabdian Kepada Masyarakat*, 8(2), 145-152.
- Budiman, A., & Setiawan, H. (2023). Tantangan keamanan siber di era kecerdasan buatan (*Artificial Intelligence*): Sebuah tinjauan literatur. *Jurnal Teknologi Informasi dan Rekayasa Komputer*, 5(1), 34-42.
- Fahmi, M. R., & Lestari, S. (2021). Penerapan metode edukatif-partisipatif dalam sosialisasi pencegahan *cyberbullying* pada siswa sekolah menengah kejuruan. *Jurnal Edukasi Masyarakat*, 3(4), 210-218.

- Hidayat, R., & Pratama, Y. (2024). Edukasi mitigasi kejahatan siber modern dan perlindungan data pribadi bagi generasi Z. *Jurnal Abdimas Komputer*, 11(1), 12-19.
- Irawan, D., & Wijaya, K. (2023). Analisis efektivitas implementasi *Multi-Factor Authentication* (MFA) dalam mencegah peretasan akun media sosial pelajar. *Jurnal Keamanan Informasi Nasional*, 7(2), 89-98.
- Kurniawati, D., & Safitri, A. (2022). Upaya peningkatan literasi digital dan kesadaran privasi data di lingkungan sekolah kejuruan. *Jurnal Implementasi Sosial dan Humaniora*, 4(3), 175-183.
- Mulyadi, E., & Handoko, P. (2024). Ancaman *phishing* berbasis AI: Bagaimana edukasi dini dapat menyelamatkan data pribadi remaja. *Jurnal Sistem Informasi dan Cyber Security*, 6(1), 55-63.
- Nugraha, F. A., & Utami, R. D. (2023). Pendampingan teknis aktivasi verifikasi dua Langkah sebagai benteng utama pertahanan akun digital masyarakat. *Jurnal Pengabdian Teknologi*, 9(2), 101-109.
- Prasetyo, B., & Rahmawati, E. (2021). Karakteristik penggunaan gawai pada remaja dan kerentanan terhadap infeksi *malware*. *Jurnal Informatika dan Kesehatan Digital*, 2(2), 77-85.
- Ramadhan, A. F., & Siregar, M. H. (2022). Sosialisasi etika profesi teknologi informasi dan kesadaran hukum siber bagi siswa SMK. *Jurnal Pengabdian Masyarakat Ilmiah*, 5(3), 320-328.
- Sanjaya, W., & Putri, L. A. (2023). Metode *hands-on experience* dalam pelatihan pengamanan gawai berbasis Android untuk pelajar tingkat menengah. *Jurnal Pendidikan Teknologi Kejuruan*, 14(2), 112-121.
- Sari, I. P., & Setiadi, R. (2024). Lanskap *cybercrime* di era kecerdasan buatan: Ancaman, tantangan, dan solusi preventif bagi pengguna internet. *Jurnal Ilmu Komputer dan Aplikasi*, 12(1), 45-53.
- Susanto, T., & Wardani, K. (2022). Pengaruh tingkat literasi digital terhadap perilaku *cyber hygiene* siswa sekolah menengah. *Jurnal Psikologi Digital Indonesia*, 3(1), 18-27.
- Wibowo, S., & Christian, J. (2023). Edukasi pembuatan kata sandi yang kuat dan implementasi keamanan ganda pada akun surat elektronik siswa. *Jurnal Pemberdayaan Masyarakat*, 8(4), 401-409.
- Yulianto, H., & Pratama, A. (2024). Evaluasi kemampuan psikomotorik siswa dalam pelatihan keamanan informasi melalui pendekatan terbimbing. *Jurnal Riset Pembelajaran Teknologi*, 10(2), 134-142.