

EDUKASI INTERNET SEHAT DAN AMAN UNTUK PENCEGAHAN KEJAHATAN SIBER PADA REMAJA: WORKSHOP DETEKSI DAN VERIFIKASI KONTEN DEEPPAKE BAGI SISWA SMK

Dikky Suryadi¹, Adam Puspabhuana², Arif Siswandi³

Institut Sains dan Teknologi Nasional¹, Universitas Cakrawala², Universitas Pelita Bangsa³

¹dikky98@gmail.com, ²adam.bhuana@gmail.com, ³arif.siswandi@pelitabangsa.ac.id

Diterima: 22 Agustus 2026 Disetujui: 26 Agustus 2026 Dipublikasikan: 30 Agustus 2026

Abstrak

Perkembangan teknologi kecerdasan artifisial memunculkan ancaman baru berupa kejahatan siber berbasis manipulasi digital, salah satunya deepfake, yang berisiko bagi remaja sebagai pengguna aktif internet. Kegiatan Pengabdian kepada Masyarakat ini bertujuan meningkatkan pemahaman dan keterampilan siswa Sekolah Menengah Kejuruan (SMK) dalam mengenali, memverifikasi, dan menyikapi konten digital yang berpotensi menyesatkan, sekaligus membangun kebiasaan berinternet yang sehat dan aman. Workshop dilaksanakan selama satu hari di Laboratorium Komputer SMK N 2 Cikarang Barat dengan melibatkan 18 siswa (13 laki-laki dan 5 perempuan) dari jurusan Rekayasa Perangkat Lunak, Teknik Komputer dan Jaringan, serta Akuntansi Bisnis. Materi disampaikan secara bertahap, meliputi internet sehat dan literasi digital, pengenalan jenis kejahatan siber seperti phishing, cyberbullying, dan hoaks, keamanan data pribadi, hingga praktik deteksi dan verifikasi konten deepfake menggunakan pendekatan triangulasi dan tools berbasis kecerdasan artifisial. Peserta juga dilatih membuat prototipe alat verifikasi sederhana berbasis JavaScript dan Large Language Model (LLM) API. Evaluasi pemahaman dilakukan melalui pretest dan posttest terhadap 10 peserta yang mengisi kuesioner secara lengkap, menunjukkan peningkatan skor rata-rata dari 29,72 menjadi 43,22 (skala maksimum 50), serta pergeseran proporsi jawaban kategori tinggi dari 34,44% menjadi 86,67%. Hasil ini menunjukkan bahwa pendekatan edukatif berbasis praktik langsung efektif meningkatkan literasi digital dan kesiapan remaja menghadapi ancaman kejahatan siber, serta relevan untuk dikembangkan berkelanjutan di sekolah lain.

Kata Kunci: internet sehat, keamanan siber, deepfake, literasi digital, remaja

Abstract

The rapid advancement of artificial intelligence has introduced new cybercrime threats based on digital manipulation, including deepfake content, which pose particular risks to adolescents as active internet users. This community service program aimed to enhance the understanding and practical skills of vocational high school (SMK) students in recognizing, verifying, and responding appropriately to potentially misleading digital content, while fostering healthy and safe internet habits. The one-day workshop was conducted at the computer laboratory of SMK N 2 Cikarang Barat, involving 18 students from the Software Engineering, Computer and

Network Engineering, and Business Accounting programs. The material was delivered progressively, covering healthy internet use and digital literacy, common forms of cybercrime such as phishing, cyberbullying, and hoaxes, personal data security, and hands-on practice in detecting and verifying deepfake content through a triangulation approach supported by AI-based tools. Participants were also guided in building a simple verification prototype using JavaScript and a Large Language Model (LLM) API. Evaluation through pretest and posttest measurements administered to 10 of 12 participants who completed the questionnaire in full showed the average score increasing from 29.72 to 43.22 (out of a maximum of 50), along with a shift in high-category responses from 34.44% to 86.67%. These findings indicate that a practice-based educational approach effectively improves adolescents digital literacy and preparedness against cybercrime threats, and merits continued development in other schools.

Keyword: *internet safety, cybercrime, deepfake, digital literacy, adolescents*

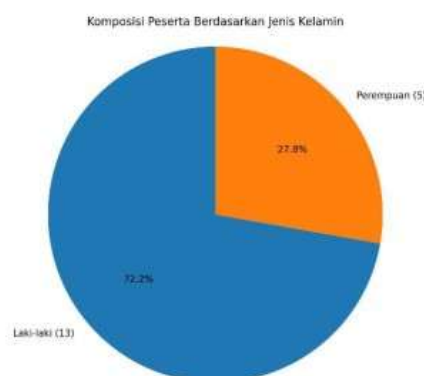
PENDAHULUAN

Perkembangan teknologi kecerdasan artifisial (Artificial Intelligence/AI) telah membuka peluang besar dalam berbagai bidang, namun di sisi lain turut memunculkan ancaman baru berupa kejahatan siber berbasis manipulasi digital, salah satunya deepfake. Konten deepfake yang menyerupai video, audio, atau gambar asli berpotensi digunakan untuk penipuan, pencemaran nama baik, maupun penyebaran disinformasi, dan remaja sebagai pengguna aktif internet menjadi kelompok yang rentan terhadap ancaman tersebut. Selain deepfake, remaja juga masih menghadapi bentuk-bentuk kejahatan siber konvensional seperti phishing, cyberbullying, dan penyebaran hoaks, yang menuntut penguatan literasi digital dan kebiasaan berinternet yang sehat dan aman sejak usia sekolah. Berbagai kajian terdahulu menunjukkan bahwa literasi digital berperan penting dalam menekan dampak negatif deepfake dan hoaks di kalangan pelajar. Fajri dkk. (2025) melalui kegiatan pengabdian edukasi internet sehat dan aman bagi remaja juga melaporkan adanya peningkatan pemahaman serta perubahan sikap peserta terhadap keamanan berinternet setelah mengikuti program edukatif-partisipatif, meskipun kegiatan tersebut masih berfokus pada penyuluhan dan simulasi kasus tanpa praktik teknis penggunaan tools deteksi. Ridha (2025) melaporkan bahwa edukasi literasi digital dan keamanan jaringan sosial efektif meningkatkan kewaspadaan siswa SMK terhadap ancaman deepfake. Mutmainnah dkk. (2024) menegaskan bahwa penguatan literasi digital menjadi solusi strategis dalam menghadapi meningkatnya penyalahgunaan teknologi deepfake sebagai sarana penyebaran hoax.

Sementara itu, Sudana dkk. (2022) menunjukkan bahwa pelatihan literasi digital bagi remaja usia sekolah perlu mencakup pemahaman terhadap regulasi transaksi elektronik, hoaks, dan cyberbullying secara terintegrasi. Namun demikian, sebagian besar kegiatan tersebut masih berfokus pada penyampaian materi secara satu arah dan belum banyak yang menggabungkan edukasi konseptual dengan praktik langsung penggunaan tools deteksi berbasis AI serta pembuatan alat verifikasi konten secara mandiri, yang menjadi kebaruan dari kegiatan pengabdian ini. Berdasarkan uraian tersebut, kegiatan Pengabdian kepada Masyarakat ini bertujuan untuk meningkatkan pemahaman dan keterampilan praktis siswa SMK dalam mengenali, memverifikasi, dan menyikapi konten digital yang berpotensi menyesatkan, termasuk konten deepfake, phishing, cyberbullying, dan hoaks, sekaligus membangun kebiasaan berinternet yang sehat dan aman melalui pendekatan edukatif-partisipatif yang menggabungkan penyampaian materi, diskusi, dan praktik langsung.

METODE

Kegiatan pengabdian ini menggunakan pendekatan edukatif-partisipatif (participatory action) yang menempatkan peserta sebagai subjek aktif dalam proses pembelajaran, bukan sekadar penerima informasi. Sasaran kegiatan adalah 18 siswa Sekolah Menengah Kejuruan (SMK) N 2 Cikarang Barat (13 laki-laki dan 5 perempuan) dari jurusan Rekayasa Perangkat Lunak (RPL), Teknik Komputer dan Jaringan (TKJ), serta Akuntansi Bisnis, yang dipilih karena keterkaitan program keahlian dengan pemanfaatan teknologi digital sehari-hari.



Gambar 7. Komposisi Peserta Berdasarkan Jenis Kelamin

Kegiatan dilaksanakan dalam satu hari di Laboratorium Komputer SMK N 2 Cikarang Barat pada 29 April 2026, dengan tahapan meliputi: (1) registrasi dan pengisian pretest untuk

mengukur pemahaman awal peserta; (2) penyampaian materi internet sehat, literasi digital, dan pengenalan jenis-jenis kejahatan siber (phishing, cyberbullying, hoaks); (3) materi keamanan data pribadi dan pengenalan deepfake; (4) praktik langsung deteksi dan verifikasi konten deepfake menggunakan prinsip triangulasi (analisis sumber, pemeriksaan visual-audio, dan tools deteksi berbasis AI) serta praktik pembuatan prototipe alat verifikasi sederhana berbasis JavaScript dan Large Language Model (LLM) API; dan (5) pengisian posttest untuk mengukur peningkatan pemahaman peserta. Data dikumpulkan melalui instrumen kuesioner pretest dan posttest berskala ordinal (skor 1-5 per pertanyaan pada 10 butir soal, skor maksimum total 50), yang diisi lengkap oleh 10 dari 12 peserta yang mengikuti sesi evaluasi dari total 18 peserta workshop, kemudian dianalisis secara deskriptif-kuantitatif dengan membandingkan skor rata-rata dan distribusi kategori pemahaman (rendah, sedang, tinggi) sebelum dan sesudah kegiatan.

Tabel 1. Kategori Skala Ordinal Kuesioner

Skor	Kategori
1	Tidak Paham
2	Kurang Paham
3	Sedang
4	Cukup Paham
5	Sangat Paham

HASIL DAN PEMBAHASAN

Data mentah hasil pretest terhadap 10 peserta pada setiap butir soal (S1–S10) ditampilkan pada Tabel 2 berikut, sebagai dasar sebelum data tersebut diringkas dan dibandingkan dengan hasil posttest.

Tabel 2. Rekap Data Pretest Peserta Berdasarkan Skala Ordinal

Peserta	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	Total
P1	4	4	3	4	5	5	5	4	3	3	40
P2	5	5	2	4	4	3	3	2	2	1	31
P3	3	4	3	4	4	2	2	2	1	2	27
P4	3	5	4	5	5	3	4	2	2	2	35
P5	4	5	3	3	2	2	4	3	2	2	30
P6	5	5	3	5	5	3	5	3	2	1	37
P7	4	3	3	4	4	3	3	2	2	1	29
P8	3	4	2	3	3	1	3	2	2	1	24
P9	4	5	2	3	4	1	4	1	1	1	26
P10	4	3	2	3	3	2	2	1	1	1	22

Keterangan: S1–S10 = Soal 1 sampai Soal 10; skor 1 = Tidak Paham, 2 = Kurang Paham, 3 = Sedang, 4 = Cukup Paham, 5 = Sangat Paham.

Hasil evaluasi terhadap 10 dari 12 peserta yang mengisi kuesioner pretest-posttest secara lengkap menunjukkan peningkatan pemahaman yang signifikan setelah mengikuti workshop. Skor rata-rata total meningkat dari 29,72 pada saat pretest menjadi 43,22 pada saat posttest, dari skor maksimum 50. Jika dilihat dari distribusi kategori jawaban (10 peserta x 10 butir soal = 180 respons per tahap), proporsi respons pada kategori pemahaman rendah menurun tajam dari 43,33% menjadi 2,78%, kategori sedang menurun dari 22,22% menjadi 10,56%, sedangkan kategori tinggi meningkat signifikan dari 34,44% menjadi 86,67%. Pergeseran ini menunjukkan bahwa sebagian besar responden berhasil mencapai tingkat pemahaman yang lebih baik terhadap materi internet sehat, kejahatan siber, dan verifikasi konten deepfake setelah mengikuti kegiatan. Pola peningkatan pemahaman dan perubahan sikap berinternet yang lebih aman ini konsisten dengan temuan Fajri dkk. (2025) pada kegiatan edukasi internet sehat serupa, yang juga mencatat pergeseran kategori pemahaman peserta ke arah yang lebih tinggi setelah intervensi edukatif-partisipatif; namun demikian, kegiatan yang dilaporkan dalam artikel ini memperluas cakupan tersebut dengan menambahkan praktik teknis deteksi dan verifikasi deepfake berbasis tools AI serta pembuatan prototipe alat verifikasi mandiri, yang belum menjadi fokus pada penelitian sebelumnya.

Peningkatan pemahaman tersebut tidak terlepas dari pendekatan praktik langsung yang diterapkan selama workshop, khususnya pada sesi deteksi dan verifikasi deepfake. Peserta tidak hanya menerima materi secara konseptual, tetapi juga mempraktikkan langsung penggunaan tools deteksi berbasis kecerdasan artifisial untuk menganalisis konten digital secara berkelompok, seperti ditunjukkan pada Gambar 2, yang kemudian didiskusikan bersama untuk memahami batasan dan tingkat keandalan setiap tools. Pendekatan ini sejalan dengan temuan Ridha (2025) yang menekankan pentingnya kombinasi literasi digital konseptual dan praktik teknis dalam meningkatkan kewaspadaan siswa SMK terhadap ancaman deepfake. Peserta juga dilatih membuat prototipe alat verifikasi sederhana berbasis JavaScript dan Large Language Model (LLM) API, sehingga memperoleh pengalaman langsung merancang solusi teknis untuk membantu proses verifikasi konten. Hasil ini menegaskan bahwa pendekatan edukatif yang menggabungkan pemahaman konsep, praktik teknis, dan evaluasi terukur efektif membekali remaja dengan kemampuan verifikasi konten secara kritis, serta relevan untuk terus

dikembangkan mengingat pesatnya perkembangan teknologi deepfake berbasis AI (Mutmainnah dkk., 2024).

Dokumentasi pelaksanaan kegiatan workshop ditunjukkan pada gambar berikut:



Gambar 1. Narasumber Memberikan Pendampingan Praktik Keamanan Siber kepada Peserta di Laboratorium Komputer SMK N 2 Cikarang Barat



Gambar 2. Narasumber Mendampingi Peserta dalam Sesi Praktik Keamanan Siber di Laboratorium Komputer

Materi kegiatan turut disosialisasikan melalui flyer edukatif yang memuat ringkasan waspada kejahatan siber dan langkah aman berinternet, sebagaimana ditunjukkan pada Gambar 3. Kegiatan dilaksanakan di Laboratorium Komputer SMK N 2 Cikarang Barat dengan suasana pelaksanaan sebagaimana ditunjukkan pada Gambar 4. Selama sesi praktik, peserta secara berkelompok aktif mendiskusikan dan menyusun kesimpulan verifikasi berdasarkan prinsip triangulasi (sumber data, metode, dan audit manual), seperti terlihat pada Gambar 5.



Gambar 3. Flyer Sosialisasi Internet Sehat dan Aman untuk Pencegahan Kejahatan Siber



Gambar 4. Lokasi dan Suasana Pelaksanaan Workshop Pencegahan Keamanan Siber di SMK N 2 Cikarang Barat



Gambar 5. Aktivitas Peserta dalam Praktik Diskusi dan Verifikasi Triangulasi Temuan

Gambaran lokasi mitra pengabdian, yaitu gedung sekolah dan laboratorium komputer SMK N 2 Cikarang Barat tempat pelaksanaan workshop berlangsung, ditunjukkan pada Gambar 6.



Gambar 6. Gedung SMK N 2 Cikarang Barat, Laboratorium Komputer, dan Suasana Pelaksanaan Workshop

PENUTUP

Kegiatan Pengabdian kepada Masyarakat ini berhasil menjawab tujuan yang ditetapkan, yaitu meningkatkan pemahaman dan keterampilan praktis siswa SMK dalam mengenali, memverifikasi, dan menyikapi konten digital yang berpotensi menyesatkan. Hal ini ditunjukkan oleh peningkatan skor rata-rata pemahaman peserta dari 29,72 menjadi 43,22, serta pergeseran proporsi jawaban menuju kategori pemahaman tinggi hingga mencapai 86,67%. Pendekatan edukatif-partisipatif yang menggabungkan penyampaian materi, diskusi, dan praktik langsung penggunaan tools deteksi AI terbukti efektif dalam membangun kesiapan remaja menghadapi ancaman kejahatan siber, khususnya deepfake. Sebagai tindak lanjut, disarankan agar kegiatan serupa dapat direplikasi di sekolah lain dengan cakupan peserta yang lebih luas, disertai pendampingan berkelanjutan serta pengembangan modul edukasi internet sehat yang dapat digunakan secara mandiri oleh pihak sekolah.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Pimpinan Institut Sains dan Teknologi Nasional (ISTN), Fakultas Sains Terapan dan Teknologi ISTN, serta Program Studi Sistem Informasi/Teknik Informatika ISTN atas dukungan yang diberikan terhadap pelaksanaan kegiatan pengabdian ini. Terima kasih juga disampaikan kepada pihak SMK N 2 Cikarang Barat yang telah memberikan akses dan fasilitas laboratorium komputer, serta kepada seluruh siswa peserta yang telah berpartisipasi aktif selama kegiatan berlangsung.

DAFTAR PUSTAKA

- Fajri, T. I., Selviana, R., Budiarto, B. W., Eldo, H., & Suryadi, D. (2025). Edukasi Internet Sehat dan Aman untuk Pencegahan Kejahatan Siber pada Remaja. *Civic Action: Jurnal Pengabdian dan Inovasi Masyarakat*, 1(3), 159–164. <https://doi.org/10.59696/civicaction.v1i3.263>
- Ridha, M. (2025). Edukasi Dampak dan Pencegahan Deepfake melalui Literasi Digital dan Keamanan Jaringan Sosial bagi Siswa SMKN 53 Jakarta. *Jurnal SOLMA*, 14(3). <https://doi.org/10.22236/solma.v14i3.19761>

- Mutmainnah, A., Suhandi, A. M., & Herlambang, Y. T. (2024). Problematika Teknologi Deepfake sebagai Masa Depan Hoax yang Semakin Meningkat: Solusi Strategis Ditinjau dari Literasi Digital. *UPGRADE: Jurnal Pendidikan Teknologi Informasi*, 1(2), 67–72. <https://doi.org/10.30812/upgrade.v1i2.3702>
- Sudana, D., Amir., Suryana, D., & Suherman, A. (2022). Model Pelatihan Literasi Digital untuk Remaja Usia Sekolah. *Dimasatra: Jurnal Pengabdian kepada Masyarakat*, 3(1), 31–42.
- Salim, H., Widjojoko., & Hanif, M. (2021). Analisis Wacana Kritis Berbasis Teknologi Informasi dan Komunikasi di Komunitas Sekolah untuk Menangkal Berita Hoaks. *Jurnal Pengabdian Masyarakat PGSD*, 1(1), 1–16.