AJAD
JURNAL PENGABDIAN KEPADA MASYARAKAT
DOI: 10.59431/ajad.v6i3.1030.
E-ISSN: 2797-2356 | P-ISSN: 2797-2364
COMMUNITY ENGAGEMENT ARTICLE

Edukasi Pencegahan *Phishing* dan Hoaks bagi Siswa SMPN 4 Pangalengan

Mohammad Bayu Anggara [1*], Hamdan Abdul Aziz [2], Yusuf Muharam [3], Yaya Suharya [4], Wini Fetia Wardhiani [5], Rendi Permadi [6]

Affiliation
[1*, 3, 4] Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Bale Bandung, Kabupaten Bandung, Provinsi Jawa Barat, Indonesia.

[2] Program Studi Rekayasa Sistem Komputer, Sekolah Tinggi Teknologi Terpadu Nurul Fikri, Kota Depok, Provinsi Jawa Barat, Negara Indonesia.

[5] Program Studi Pendidikan Bahasa dan Sastra Indonesia, Fakultas Keguruan dan Ilmu Pendidikan, Universitas Bale Bandung, Kabupaten Bandung, Provinsi Jawa Barat, Indonesia.

[6] Program Studi Agribisnis, Fakultas Pertanian, Universitas Bale Bandung, Kabupaten Bandung, Provinsi Jawa Barat, Indonesia.

Correspondence
[1*] Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Bale Bandung, Kabupaten Bandung, Provinsi Jawa Barat, Indonesia.

Email: mohammadbayuanggara@unibba.ac.id

Funding Information
Universitas Bale Bandung.

Article History
Received: 9 Sep 2026.
Revised: 11 Sep 2026.
Accepted: 14 Nov 2026.
Available online: 20 November 2026.
Published: 1 December 2026.

Abstract
The development of digital technology requires adolescents to master internet security. Junior high school students are highly vulnerable to social engineering threats, phishing exploitation, hoax dissemination, and digital media ethics violations. This community service aimed to strengthen the cybersecurity understanding of 59 students at SMPN 4 Pangalengan. The educational intervention utilized a participatory action approach, comprising interactive socialization and case study analysis. The materials focused on three main domains: phishing prevention, digital ethics application, and independent information verification techniques. Students' cognitive understanding was evaluated using a one-group pretest–posttest design with a score range of 0 to 100. Data analysis revealed an absolute increase of 8.82 points, with the class mean score rising from 65.76 on the pretest to 74.58 on the posttest. Based on a paired-sample t-test with a significance threshold of $\alpha = 0.05$, this improvement was statistically significant ($t(58) = -7.43$, $p < 0.001$). Practically, contextual case-study-based cybersecurity education effectively improves students' cognitive understanding to mitigate digital threats at school.

Keywords
Cybersecurity; Digital Literacy; Hoaxes; Phishing; Social Media Ethics.

Abstrak
Perkembangan teknologi digital menuntut remaja menguasai keamanan berinternet. Siswa sekolah menengah pertama rentan terhadap ancaman rekayasa sosial, eksploitasi *phishing*, penyebaran hoaks, dan pelanggaran etika bermedia digital. Kegiatan pengabdian kepada masyarakat ini bertujuan memperkuat pemahaman keamanan siber pada 59 siswa di SMPN 4 Pangalengan. Intervensi edukatif dilakukan melalui pendekatan aksi partisipatif yang mencakup sosialisasi interaktif dan bedah studi kasus. Materi difokuskan pada tiga domain utama, yaitu pencegahan *phishing*, penerapan etika digital, serta teknik verifikasi informasi secara mandiri. Evaluasi pemahaman kognitif siswa diukur menggunakan desain *one-group pretest–posttest* dengan rentang skor instrumen 0 hingga 100. Hasil analisis data menunjukkan peningkatan sebesar 8,82 poin, dengan nilai rata-rata kelas yang naik dari 65,76 pada saat *pretest* menjadi 74,58 pada *posttest*. Berdasarkan hasil uji *paired-sample t-test* pada ambang batas signifikansi $\alpha = 0,05$, peningkatan pemahaman tersebut terbukti bermakna secara statistik ($t(58) = -7,43$; $p < 0,001$). Secara praktis, edukasi keamanan siber berbasis studi kasus kontekstual efektif meningkatkan pemahaman kognitif siswa dalam memitigasi ancaman digital di sekolah.

Kata Kunci
Etika Bermedia Sosial; Hoaks; Keamanan Siber; Literasi Digital; Phishing.

1 | PENDAHULUAN

Di tengah perkembangan transformasi digital yang pesat, literasi digital menjadi kompetensi penting bagi remaja untuk melindungi data pribadi dan berperilaku secara bertanggung jawab di ruang siber (Akbar *et al*., 2026). Namun, siswa sekolah menengah pertama masih rentan terhadap berbagai ancaman siber, seperti eksploitasi *phishing* dan penyebaran hoaks (Arisanty *et al*., 2025; Pradipta *et al*., 2024). Kurangnya pengalaman saat berinteraksi dengan tautan mencurigakan dapat berujung pada peretasan akun yang kerap disalahgunakan untuk penipuan atau pencemaran nama baik (Arisanty *et al*., 2025; Primananda *et al*., 2023). Rendahnya kemampuan menyaring informasi dan memahami taktik rekayasa sosial juga mempermudah remaja terjebak dalam narasi disinformasi yang sarat dengan bias dan stereotip (Rodríguez-Díaz & Rodríguez-Ferrándiz, 2026). Jika dibiarkan, kondisi ini berisiko memicu perpecahan sosial serta kerusakan reputasi individu (Manuhutu *et al*., 2026; Soraya *et al*., 2026).

Untuk mengatasi kerentanan tersebut, diperlukan edukasi terstruktur guna membekali siswa dengan kemampuan mengidentifikasi, memverifikasi, dan mencegah kejahatan siber (Bhagaskoro *et al*., 2023; Pradipta *et al*., 2024). Pemahaman mengenai pentingnya verifikasi sumber merupakan bagian utama dari pertahanan informasi (*information defense*) agar siswa dapat membedakan informasi akurat dari konten manipulatif (Khomarudin *et al*., 2025; Tsary & Muttaqin, 2026). Pendekatan edukatif yang sistematis mendorong siswa bersikap lebih kritis di platform daring sehingga meminimalkan risiko serangan siber yang kompleks (Khomarudin *et al*., 2025; Manan *et al*., 2026). Melalui edukasi tersebut, siswa diharapkan memiliki keterampilan untuk mengenali tanda-tanda ancaman digital sejak dini sekaligus melindungi privasi data pribadi di lingkungan daring (Arisanty *et al*., 2025; Manuhutu *et al*., 2026). Pemahaman ini juga berperan penting dalam mengurangi risiko manipulasi informasi yang sering kali tidak disadari oleh pengguna (Hossain & Jabbari, 2026; Primananda *et al*., 2023). Selain itu, penguasaan etika digital akan menumbuhkan rasa tanggung jawab dalam pemanfaatan teknologi sekaligus menciptakan lingkungan sekolah yang lebih tangguh terhadap disinformasi (Nurrofi, 2026; Soraya *et al*., 2026).

Penerapan program literasi yang terpadu, seperti pemanfaatan studi kasus dan simulasi interaktif, terbukti efektif meningkatkan keterampilan siswa dalam menghadapi tantangan siber (Arisanty *et al*., 2025). Pendekatan partisipatif membantu siswa mengevaluasi informasi secara mandiri sebelum membagikan konten sehingga dapat menekan laju penyebaran disinformasi di lingkungan sekolah (Arisanty *et al*., 2025; Soraya *et al*., 2026). Program ini juga mendukung pembentukan kewarganegaraan digital yang bertanggung jawab melalui pengelolaan identitas secara aman (Escoda *et al*., 2026). Penguatan kognitif ini harus disertai dengan keterampilan teknis, mengingat rendahnya kesadaran sering memicu peserta didik membagikan data kepada pihak yang tidak bertanggung jawab (Pradipta *et al*., 2024). Mitigasi teknis seperti penggunaan autentikasi dua faktor sangat penting untuk melindungi akun dari akses ilegal (Adama *et al*., 2026; Arisanty *et al*., 2025). Selain itu, pemahaman yang memadai tentang rekayasa sosial, seperti mengenali tautan hadiah palsu, diperlukan untuk mencegah pencurian akun akibat tindakan impulsif (Arisanty *et al*., 2025; Bhagaskoro *et al*., 2023). Mengingat keamanan siber menuntut perubahan perilaku secara konsisten (Manuhutu *et al*., 2026), efektivitas intervensi ini dievaluasi melalui instrumen *pretest* dan *posttest* guna mengukur peningkatan kewaspadaan siswa terhadap bahaya hoaks dan *phishing* (Akbar *et al*., 2026; Arisanty *et al*., 2025).

Meskipun urgensi literasi keamanan siber telah menjadi perhatian nasional, tantangan di tingkat akar rumput membutuhkan intervensi yang spesifik dan kontekstual. Berdasarkan tahap penjajakan dan observasi awal di lokasi pengabdian, ditemukan kesenjangan literasi digital yang nyata pada perilaku harian siswa. Laporan dari pihak sekolah mengindikasikan bahwa tantangan yang dihadapi tidak hanya berpusat pada kerentanan privasi data terhadap ancaman *phishing* atau hoaks, tetapi juga meluas pada aspek penerapan etika bermedia sosial. Hasil pengamatan menunjukkan bahwa sejumlah siswa terdorong untuk mengikuti tren digital, seperti gaya berpakaian atau ekspresi melalui konten video, yang terkadang belum sepenuhnya selaras dengan norma kesopanan dan etika pelajar. Perilaku ini umumnya dipicu oleh tingginya keinginan untuk mendapatkan pengakuan teman sebaya (*peer validation*) di dunia maya tanpa diimbangi dengan pemahaman mengenai dampak jejak digital jangka panjang. Minimnya penyaringan mandiri (*self-censorship*) ini mencerminkan kebutuhan dasar (*baseline needs*) siswa dalam memahami batasan ruang publik dan etika digital. Kondisi empiris inilah yang menjustifikasi pemilihan SMPN 4 Pangalengan melalui teknik *purposive sampling*. Intervensi ini dirancang khusus dengan menargetkan 59 siswa guna menjembatani wacana keamanan siber dan kebutuhan mendesak terkait pembentukan karakter serta ketahanan digital peserta didik di lapangan.

2 | LANDASAN TEORI

2.1 Literasi Digital dan Etika Bermedia Sosial pada Remaja

Etika digital didefinisikan sebagai panduan nilai dan prinsip moral yang mengatur perilaku manusia dalam menggunakan, mengembangkan, dan berinteraksi dengan teknologi digital (Pradana & Amol, 2024), sedangkan verifikasi informasi merupakan proses menilai kredibilitas, akurasi, otoritas, dan relevansi informasi dengan membandingkannya

pada sumber independen sebelum informasi tersebut dipercaya atau disebarluaskan (Haider & Sundin, 2020). Literasi digital pada jenjang remaja tidak hanya mencakup kecakapan teknis operasional, tetapi juga menuntut internalisasi etika serta perlindungan privasi yang selaras dengan perkembangan kematangan kognitif dan sosial individu (Al-kfairy *et al*., 2025). Dengan mengintegrasikan perilaku etis sebagai fondasi, remaja dapat membangun ketahanan terhadap disinformasi melalui kemampuan berpikir kritis yang aktif, bukan sekadar menerima konten secara pasif (Tondeur *et al*., 2025). Oleh karena itu, remaja perlu dibekali dengan strategi validasi sumber dan deteksi bias yang sistematis agar mampu menjalankan pertahanan informasi (*information defense*) secara mandiri (Rana *et al*., 2025). Mengingat karakteristik kognitif siswa sekolah menengah pertama yang cenderung dinamis, edukasi mengenai keamanan siber yang kompleks memerlukan pendekatan interaktif berbasis bedah kasus atau gamifikasi untuk mendukung internalisasi kompetensi pemecahan masalah (Blanc *et al*., 2025). Implementasi metode ini bertujuan mengubah peran remaja dari pengguna pasif menjadi komunikator digital yang reflektif dalam menyaring konten multimodal. Pendekatan adaptif tersebut memastikan bahwa kapasitas literasi digital individu berfungsi sebagai moderator yang menentukan efektivitas setiap bentuk interaksi di ruang siber dan platform media sosial (Yaseen *et al*., 2025). Integrasi kemampuan evaluasi ini menuntut siswa untuk secara sistematis mengorganisasi dan mensintesis temuan mereka dengan memverifikasi data terhadap skema sosial atau sumber eksternal yang tepercaya (Nasr *et al*., 2025). Strategi ini secara langsung meningkatkan kompetensi individu dalam menghadapi kompleksitas dunia digital yang terus berubah sekaligus memitigasi risiko penyebaran hoaks melalui penguatan literasi informasi (Ma & Ismail, 2025).

2.2 Ancaman Rekayasa Sosial dan *Phishing*

Rekayasa sosial merupakan strategi manipulasi psikologis yang mendorong pengguna untuk melakukan tindakan tertentu atau mengungkapkan informasi sensitif dengan mengeksploitasi kepercayaan, persepsi otoritas, dan kerentanan pengambilan keputusan manusia (Brissett & Wall, 2025). Pemahaman atas pola ancaman ini memungkinkan remaja mengembangkan skeptisisme kritis untuk memvalidasi legitimasi setiap transmisi informasi sebelum berinteraksi dengan tautan yang diterima. Dalam kaitan ini, *phishing* didefinisikan sebagai kejahatan siber berbasis rekayasa sosial yang secara sistematis mengeksploitasi kelalaian kognitif pengguna untuk mencuri kredensial serta identitas pribadi melalui simulasi autentik yang mengecoh. Pada platform media sosial, pelaku memanfaatkan taktik manipulasi psikologis seperti bukti sosial, otoritas palsu, dan akun kloning untuk mengikis kewaspadaan korban melalui janji hadiah atau urgensi semu (Opara *et al*., 2025). Fenomena kebutaan atensi (*inattentional blindness*) pada remaja sering kali memicu kegagalan deteksi tautan berbahaya karena perhatian mereka terfokus secara eksklusif pada indikator sosial semu, seperti jumlah suka (*likes*) atau tekanan teman sebaya. Kondisi psikologis inilah yang mengaburkan keberadaan ancaman siber di balik komunikasi yang tampak wajar (Alhuzali *et al*., 2025), terlebih karena pelaku ancaman kini kerap memanfaatkan *bot* otomatis dan entitas tiruan untuk menyebarkan informasi manipulatif secara masif (He *et al*., 2025). Oleh karena itu, mitigasi serangan ini memerlukan perubahan pendekatan dari sekadar ketergantungan pada filter sistem menuju pemahaman yang utuh atas pola manipulasi sosial. Pemahaman kognitif tersebut harus diperkuat dengan penerapan mekanisme pertahanan aktif, khususnya autentikasi dua faktor (2FA), guna memastikan integritas akun dari upaya pengambilalihan ilegal (Khadka & Ullah, 2025). Integrasi protokol keamanan proaktif ini bukan sekadar opsi, melainkan kebutuhan mendesak untuk mengatasi kelemahan metode kata sandi tradisional yang rentan terhadap eksploitasi (Yusop *et al*., 2025). Langkah preventif ini diharapkan mampu menutup celah kerentanan pada tingkat pengguna akhir dan meminimalkan risiko kebocoran data yang kerap tidak disadari oleh individu (Lallie *et al*., 2025). Sinergi antara kesadaran perilaku dan ketahanan teknis ini bersifat fundamental, mengingat faktor manusia selalu menjadi penentu utama dalam efektivitas arsitektur keamanan siber secara keseluruhan (Aljumaiah *et al*., 2025; Khadka & Ullah, 2025).

3 | METODE

3.1 Pendekatan dan Lokasi Kegiatan Pelaksanaan

kegiatan pengabdian kepada masyarakat ini menggunakan pendekatan aksi partisipatif (*participatory action research*) dengan menempatkan kelompok sasaran sebagai pihak yang terlibat langsung dalam seluruh rangkaian kegiatan. Program ini dilaksanakan pada 19 Agustus 2026 di SMPN 4 Pangalengan, Kabupaten Bandung, yang ditetapkan berdasarkan kesesuaiannya dengan tujuan program. Pemilihan lokasi dan mitra dilakukan menggunakan teknik *purposive sampling* dengan mempertimbangkan peningkatan akses internet di wilayah tersebut serta kerentanan siswa sekolah menengah pertama terhadap eksploitasi siber. Kegiatan ini melibatkan 59 siswa yang dipilih sebagai perwakilan untuk mendukung penguatan literasi digital di lingkungan sekolah.

3.2 Tahapan Kegiatan

Kegiatan pengabdian kepada masyarakat ini dilaksanakan secara sistematis melalui tiga tahapan utama: 1) tahap persiapan (analisis situasi), di mana tim pengabdian melakukan observasi awal dan berdiskusi dengan pihak sekolah

mengenai kejahatan siber, etika bermedia sosial, serta penyebaran berita bohong, yang hasilnya digunakan sebagai dasar penyusunan modul edukasi interaktif sesuai dengan kemampuan kognitif remaja; 2) tahap pelaksanaan (intervensi edukatif), yaitu kegiatan tatap muka selama 120 menit (pukul 08.00 hingga 10.00 WIB) yang diawali dengan pengisian instrumen evaluasi awal (*pretest*), dilanjutkan dengan pemaparan materi secara interaktif dan pembahasan studi kasus faktual mengenai etika bermedia sosial dan mitigasi perundungan siber (*cyberbullying*), pengenalan serta pencegahan modus *phishing* (rekayasa sosial), dan teknik verifikasi fakta untuk menekan penyebaran hoaks; serta 3) tahap evaluasi, yang dilakukan pada akhir kegiatan melalui pemberian evaluasi akhir (*posttest*) untuk mengukur pemahaman kognitif peserta terhadap materi yang telah disampaikan, disertai pengamatan respons siswa selama sesi tanya jawab partisipatif sebagai bentuk refleksi langsung.

3.3 Instrumen dan Analisis Data

Evaluasi keberhasilan program tidak hanya ditinjau dari tingkat partisipasi atau kehadiran peserta, tetapi juga dari peningkatan pemahaman kognitif yang diukur secara statistik. Instrumen evaluasi yang digunakan berupa 20 butir soal pilihan ganda (*multiple-choice questions*) yang identik untuk *pretest* dan *posttest* dengan rentang skor akhir 0 hingga 100. Data skor dari 59 responden dikumpulkan dan dianalisis menggunakan metode statistik deskriptif dan inferensial. Sebelum pengujian hipotesis, kelayakan distribusi data diperiksa menggunakan uji asumsi normalitas Shapiro-Wilk [cek metode: pastikan hasil uji Shapiro-Wilk ini turut dilaporkan secara singkat pada Bab 4 Hasil]. Selanjutnya, uji signifikansi dilakukan menggunakan *paired-sample t-test* melalui Google Colab untuk menguji perbedaan pemahaman secara statistik antara sebelum dan sesudah intervensi edukasi. Hasil analisis kemudian divisualisasikan dalam bentuk grafik distribusi kepadatan nilai, diagram pencar sebaran skor individu, dan grafik perbandingan kategori pemahaman guna memberikan gambaran yang jelas mengenai perubahan capaian peserta setelah kegiatan.

4 | HASIL DAN PEMBAHASAN

4.1 Hasil

Kegiatan pengabdian kepada masyarakat dilaksanakan di SMPN 4 Pangalengan dengan melibatkan 59 siswa sebagai peserta. Kegiatan dilakukan secara tatap muka melalui metode ceramah interaktif dan pembahasan studi kasus yang mencakup etika bermedia sosial, pengenalan ancaman kejahatan siber khususnya *phishing*, serta cara mengidentifikasi berita bohong (hoaks). Selama kegiatan berlangsung, siswa aktif mengikuti pemaparan materi dan diskusi, terutama ketika pemateri membedah contoh kasus penipuan digital yang dekat dengan keseharian remaja, sebagaimana didokumentasikan pada Gambar 1.








Gambar 1. Dokumentasi Pelaksanaan Sosialisasi Literasi Digital di SMPN 4 Pangalengan

Untuk mengukur efektivitas kegiatan secara kuantitatif, tim pengabdi memberikan evaluasi berupa *pretest* sebelum materi disampaikan dan *posttest* setelah seluruh rangkaian kegiatan selesai. Hasil pengolahan data dari 59 responden yang dirangkum pada Tabel 1 menunjukkan adanya peningkatan pemahaman siswa mengenai literasi digital dan keamanan siber, di mana nilai rata-rata kelas meningkat dari 65,76 pada *pretest* menjadi 74,58 pada *posttest*.

Tabel 1. Hasil Uji Statistik Pre-test dan Post-test

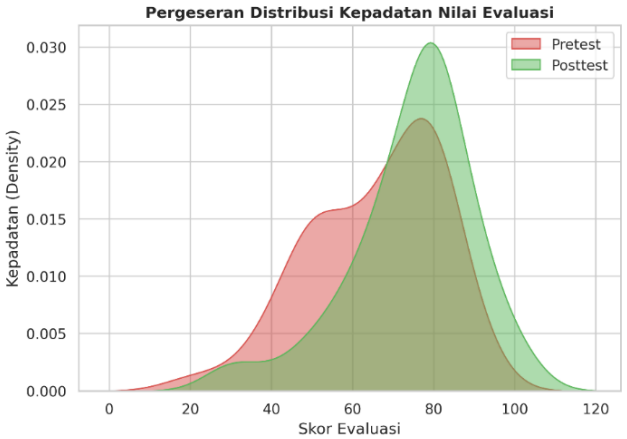
Parameter Uji	Pre-test	Post-test	Hasil Analisis
N (Jumlah Siswa)	59	59	*df* = 58
Nilai Minimum	20	30	Nilai *t* = -7,43
Nilai Maksimum	90	100	*p-value* = < 0,001
Rata-rata (*Mean*)	65,76	74,58	Beda Absolut = 8,81
Simpangan Baku (SD)	16,21	15,12	Cohen's *d* = 0,56

Tabel 2. Distribusi Kategori Pemahaman Siswa

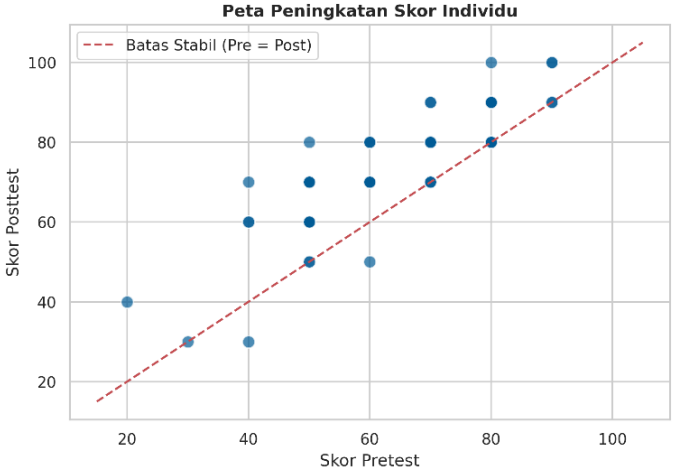
Kategori	Pre-test (N)	Pre-test (%)	Post-test (N)	Post-test (%)
Kurang (< 60)	17 Siswa	28,81%	6 Siswa	10,17%
Cukup (60-79)	20 Siswa	33,90%	18 Siswa	30,51%
Baik (≥ 80)	22 Siswa	37,29%	35 Siswa	59,32%
Total	59 Siswa	100%	59 Siswa	100%

Berdasarkan pengujian hipotesis pada ambang batas signifikansi α = 0,05, edukasi berbasis studi kasus terbukti efektif meningkatkan pemahaman kognitif siswa mengenai mitigasi *phishing*, hoaks, dan etika digital. Keberhasilan ini ditandai dengan peningkatan nilai rata-rata kelas sebesar 8,82 poin yang bermakna secara statistik ($t(58) = -7,43$; $p < 0,001$) dengan ukuran dampak sedang (*Cohen's d* = 0,56). Peningkatan tersebut didukung oleh relevansi materi dengan keseharian remaja, seperti pembedahan kasus penipuan tautan berkedok hadiah *game online*. Sebagaimana disajikan pada Tabel 2, pergeseran pemahaman juga terlihat secara linear dari penurunan jumlah siswa pada kategori Kurang (dari 28,81% menjadi 10,17%) dan peningkatan mayoritas peserta ke kategori Baik (mencapai 59,32% pascaintervensi). Kendati demikian, evaluasi *posttest* yang dilakukan segera setelah intervensi ini baru mengukur peningkatan kapasitas kognitif jangka pendek dan belum dapat diklaim sebagai perubahan perilaku daring secara permanen. Sebagai contoh, meskipun siswa menunjukkan pemahaman yang baik mengenai pentingnya autentikasi dua faktor (2FA) sebagai perlindungan teknis, ketiadaan survei lanjutan (*follow-up survey*) atau lembar komitmen pascakegiatan membuat tingkat adopsi praktik keamanan tersebut belum dapat dipastikan. Oleh karena itu, tindak lanjut berupa observasi berkala oleh guru atau penggunaan daftar periksa (*checklist*) keamanan akun sangat direkomendasikan untuk menjembatani kesenjangan antara pengetahuan kognitif dan pembentukan budaya aman berinternet secara berkelanjutan. Perubahan pemahaman siswa tersebut juga terkonfirmasi melalui analisis distribusi data secara visual. Berdasarkan kurva kepadatan nilai pada Gambar 2, puncak kurva *posttest* bergeser ke arah kanan, yang mengindikasikan bahwa skor siswa setelah mengikuti kegiatan secara umum lebih tinggi dibandingkan skor saat *pretest*. Sejalan dengan pergeseran distribusi tersebut, pemetaan perubahan skor masing-masing siswa melalui diagram pencar (*scatter plot*) pada Gambar 3 memperlihatkan bahwa sebagian besar titik observasi berada di atas garis referensi ($y = x$). Kondisi ini membuktikan bahwa peningkatan skor tidak hanya terpusat pada segelintir siswa, tetapi dialami secara merata oleh mayoritas peserta

yang mengikuti kegiatan.

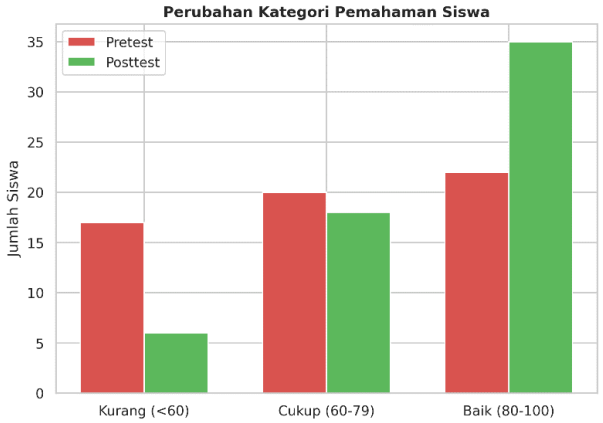


Gambar 2. Grafik Distribusi Kepadatan Nilai *Pretest* dan *Posttest* Siswa



Gambar 3. Peta Sebaran Peningkatan Skor Individu

Selain melalui distribusi skor kontinu, perubahan capaian edukasi juga tampak jelas pada visualisasi proporsi tingkat pemahaman siswa sebelum dan sesudah intervensi (Gambar 4). Setelah mengikuti kegiatan edukasi, proporsi siswa dalam kategori Kurang (skor < 60) mengalami penurunan yang nyata, diiringi dengan perpindahan sebagian besar siswa ke kategori Cukup (skor 60–79) dan kategori Baik (skor ≥ 80). Pergeseran proporsi ini memperkuat temuan bahwa intervensi yang diberikan mampu mengangkat tingkat pemahaman kelompok siswa yang semula berada pada kelompok rentan.



Gambar 4. Komparasi Kategori Tingkat Pemahaman Siswa Sebelum dan Sesudah Edukasi

4.2 Pembahasan

Peningkatan nilai rata-rata pada hasil evaluasi menunjukkan bahwa sosialisasi interaktif dapat membantu memperkuat pemahaman keamanan siber pada siswa sekolah menengah pertama. Sebelumnya, remaja diketahui masih rentan terhadap ancaman siber seperti *phishing* akibat kurangnya pengalaman serta kebiasaan berinteraksi dengan tautan mencurigakan tanpa melakukan verifikasi yang memadai (Arisanty *et al*., 2025; Pradipta *et al*., 2024). Melalui penyampaian materi yang dikaitkan langsung dengan kehidupan sehari-hari, seperti contoh penipuan berkedok hadiah *game online*, siswa dapat lebih mudah mengenali bentuk-bentuk ancaman yang mungkin mereka temui di platform daring. Pendekatan kontekstual tersebut mendorong siswa untuk lebih berhati-hati dan tidak langsung mempercayai informasi atau tautan yang diterima (Khomarudin *et al*., 2025; Manan *et al*., 2026), sehingga menjadi landasan penting dalam membangun pertahanan informasi (*information defense*) di lingkungan sekolah (Tsary & Muttaqin, 2026). Perubahan distribusi kategori pemahaman siswa juga mencerminkan peningkatan kesadaran mengenai etika bermedia sosial dan cara menghadapi berita bohong (hoaks). Rendahnya kemampuan dalam menyaring informasi dapat membuat remaja lebih mudah terlibat dalam penyebaran hoaks yang berpotensi memicu perpecahan sosial maupun merusak reputasi individu (Manuhutu *et al*., 2026; Soraya *et al*., 2026). Selama kegiatan berlangsung, siswa dibekali pemahaman mengenai pentingnya memeriksa kredibilitas sumber sebelum membagikan suatu konten kepada orang lain agar mampu membedakan informasi yang akurat dari konten yang bersifat manipulatif. Penggabungan pemahaman etika digital dan kemampuan berpikir kritis ini membantu siswa bersikap lebih selektif dalam menerima maupun menyebarkan informasi di lingkungan sekolah (Arisanty *et al*., 2025; Khomarudin *et al*., 2025). Secara keseluruhan, capaian kegiatan ini sejalan dengan temuan studi terdahulu yang menunjukkan bahwa pemberian edukasi keamanan siber secara terarah dapat membantu siswa menjadi lebih waspada dalam menggunakan teknologi digital (Akbar *et al*., 2026). Meskipun hasil evaluasi jangka pendek menunjukkan peningkatan yang positif, penerapan perilaku aman dalam kehidupan sehari-hari tetap menghadirkan tantangan tersendiri. Siswa perlu terus membiasakan diri menjaga kerahasiaan data pribadi dan mengaktifkan autentikasi dua faktor pada akun media sosial mereka (Adama *et al*., 2026; Nurrofi, 2026). Oleh karena itu, penguasaan literasi digital perlu diposisikan sebagai kompetensi dasar yang pengembangannya didukung melalui program edukasi yang berkelanjutan pada pendidikan formal (Akbar *et al*., 2026; Manuhutu *et al*., 2026).

5 | KESIMPULAN DAN REKOMENDASI

Kegiatan pengabdian kepada masyarakat melalui pendekatan aksi partisipatif di SMPN 4 Pangalengan efektif meningkatkan literasi digital dan pemahaman keamanan siber pada 59 siswa. Melalui sosialisasi interaktif dan bedah studi kasus kontekstual mengenai pencegahan *phishing*, etika bermedia sosial, serta verifikasi informasi, kegiatan ini menghasilkan peningkatan pemahaman kognitif yang signifikan. Keberhasilan tersebut dibuktikan secara kuantitatif dengan kenaikan nilai rata-rata kelas sebesar 8,82 poin, yakni dari 65,76 pada *pretest* menjadi 74,58 pada *posttest* ($t(58) = -7{,}43$; $p < 0{,}001$). Peningkatan capaian ini menunjukkan bahwa siswa memiliki kesiapan kognitif yang lebih baik untuk bersikap kritis sebelum berinteraksi dengan tautan mencurigakan atau membagikan konten di ruang digital. Meskipun demikian, pengukuran yang dilakukan segera setelah intervensi memiliki keterbatasan karena baru memotret penguasaan kognitif jangka pendek dan belum menjamin terbentuknya perilaku aman berinternet secara permanen. Guna menjaga keberlanjutan budaya keamanan siber dan perlindungan data pribadi, edukasi literasi digital perlu diintegrasikan secara berkesinambungan ke dalam kegiatan pembelajaran di sekolah. Sebagai tindak lanjut, pemangku kebijakan di sekolah direkomendasikan untuk menyusun modul pendampingan bagi guru, melaksanakan evaluasi berkala guna memantau retensi pemahaman dan penerapan praktik keamanan akun, serta menginisiasi kampanye verifikasi fakta yang melibatkan peran aktif siswa.

REFERENSI

Adama, V., Biddle, R., Arachchilage, N., & Lottridge, D. (2026). Confident yet concerned: Inconsistencies in computing students' attitudes on cybersecurity. *International Journal of Information Security*, *123*. https://doi.org/10.1007/s10207-026-01276-4

Akbar, F. N., Syifa, A., Utari, Faturahman, F., Rifai, A., Syahputra, R., Tamsar, R. A., Permana, D. A., Khaikal, M. D., & Rahman, M. R. F. (2026). Edukasi keamanan siber di SMK Kosgoro Bogor sebagai upaya peningkatan kesadaran dan tanggung jawab digital generasi muda. *KIAT: Kajian Ilmiah Pengabdian Masyarakat*, *2*(1), 41–47. https://doi.org/10.36350/kiat.v1i1.28

Al-kfairy, M., Alrabaee, S., Alfandi, O., Mohamed, A., & Khaddaj, S. (2025). Navigating ethical dimensions in the metaverse: Challenges, frameworks, and solutions. *IEEE Access*, *13*, 79996–80018. https://doi.org/10.1109/access.2025.3564498

Alhuzali, A., Alloqmani, A., Aljabri, M., & Alharbi, F. (2025). In-depth analysis of phishing email detection: Evaluating the performance of machine learning and deep learning models across multiple datasets. *Applied Sciences*, *15*(6), 3396. https://doi.org/10.3390/app15063396

Aljumaiah, O., Jiang, W., Addula, S. R., & Almaiah, M. A. (2025). Analyzing cybersecurity risks and threats in IT infrastructure based on NIST framework. *Journal of Cyber Security and Risk Auditing*, *2025*(2), 12–26. https://doi.org/10.63180/jcsra.thestap.2025.2.2

Arisanty, M., Riady, Y., Kharis, S. A. A., Permatasari, S. M., & Sukatmi, S. (2025). Cerdas dan aman bermedia digital: Peningkatan kesadaran keamanan siber di era hoaks dan phishing. *Jurnal Abdimas Patikala*, *4*(4), 1407–1418. https://doi.org/10.51574/patikala.v4i4.3282

Bhagaskoro, A., Pramadansyah, M. R., Adiputra, M. N., Setyawati, D., Putri, N., Sutiyo, & Utomo, R. G. (2023). Penyuluhan bahaya phising untuk meningkatkan kesadaran keamanan digital. *Jurnal Pemanfaatan Teknologi untuk Masyarakat (JAPATUM)*, *2022*(2), 2 [cek referensi: pastikan kesesuaian volume dan rentang halaman dengan DOI]. https://doi.org/10.59328/JAPATUM.2023.2.2.57

Blanc, S., Peiró, A. C., Benlloch-Dualde, J. V., Monteiro, A., & Grindei, L. (2025). Digital competence development in schools: A study on the association of problem-solving with autonomy and digital attitudes. *International Journal of STEM Education*, *12*(1). https://doi.org/10.1186/s40594-025-00534-6

Brissett, A., & Wall, J. (2025). Machine learning and watermarking for accurate detection of AI-generated phishing emails. *Electronics*, *14*(13), 2611. https://doi.org/10.3390/electronics14132611

Escoda, A. P., Fernández, E. O., & Otón, L. M. (2026). Enhancing teachers' digital competence for combating disinformation and fake news through the use of social media in classroom. *Journal of New Approaches in Educational Research*, *6*. https://doi.org/10.1007/s44322-026-00051-6

Haider, J., & Sundin, O. (2020). Information literacy challenges in digital culture: Conflicting engagements of trust and doubt. *Information, Communication & Society*, *25*(8), 1176–1191. https://doi.org/10.1080/1369118x.2020.1851389

He, Q., Zhang, S.-Y., Cai, Y., Yuan, W., Ma, L., & Yu, K. (2025). A survey on exploring real and virtual social network rumors: State-of-the-art and research challenges. *ACM Computing Surveys*, *57*(7), 1–37. https://doi.org/10.1145/3716498

Hossain, M., & Jabbari, J. (2026). 'Reading between the lies': Reading achievement, socioeconomic inequality, and adolescents' resistance to misinformation. *Social Science Research*, *139*, 103398. https://doi.org/10.1016/j.ssresearch.2026.103398

Khadka, K., & Ullah, A. B. (2025). Human factors in cybersecurity: An interdisciplinary review and framework proposal. *International Journal of Information Security*, *24*(3). https://doi.org/10.1007/s10207-025-01032-0

Khomarudin, A. N., Aulia, R., Jamaluddin, Novita, R., Ikhsan, M., Afif, M. N., & Suherlan, H. (2025). Penyuluhan internet sehat tentang bahaya phising dan dampak negatifnya bagi siswa SMK N 4 Payakumbuh. *Interaksi: Jurnal Pengabdian Kepada Masyarakat*, *2*(1), 16–22. https://doi.org/10.66341/interaksi.v2i1.254

Lallie, H. S., Thompson, A., Titis, E., & Stephens, P. (2025). Analysing cyber attacks and cyber security vulnerabilities in the university sector. *Computers*, *14*(2), 49. https://doi.org/10.3390/computers14020049

Ma, H., & Ismail, L. (2025). Bibliometric analysis and systematic review of digital competence in education. *Humanities and Social Sciences Communications*, *12*(1). https://doi.org/10.1057/s41599-025-04401-1

Manan, K. A., Ghani, M. M., Ahmed, I. S. Y., & Tajuddin, S. N. A. A. (2026). Digital literacy and scam susceptibility among youth: The mediating roles of risk awareness and digital responsibility. *Jurnal Komunikasi: Malaysian Journal of Communication*, *42*(2), 494–510. https://doi.org/10.17576/JKMJC-2026-4202-27

Manuhutu, M. A., Daharang, I., Sindi, Goklas, Marcello, Alberthus, & Orulin. (2026). Pengabdian masyarakat: Waspada phishing bagi kalangan pelajar. *Kesejahteraan Bersama: Jurnal Pengabdian dan Keberlanjutan Masyarakat*, *3*(3), 110–111. https://doi.org/10.62383/bersama.v3i3.3421

Nasr, N. R., Tu, C.-H., Werner, J., Bauer, T., Yen, C.-J., & Sujo–Montes, L. (2025). Exploring the impact of generative AI ChatGPT on critical thinking in higher education: Passive AI-directed use or human–AI supported collaboration? *Education Sciences*, *15*(9), 1198. https://doi.org/10.3390/educsci15091198

Nurrofi, N. (2026). Perlindungan privasi digital: Benteng utama keamanan di zaman internet. *Qolamuna: Keislaman, Pendidikan, Literasi dan Humaniora*, *3*(1), 89–98. https://jurnal.qolamuna.id/index.php/JQ/article/view/355

Opara, C., Modesti, P., & Golightly, L. (2025). Evaluating spam filters and stylometric detection of AI-generated phishing emails. *Expert Systems with Applications*, *276*, 127044. https://doi.org/10.1016/j.eswa.2025.127044

Pradana, D. W., & Amol, F. (2024). Etika teknologi: Kajian sistematis, trend dan potensi riset etika teknologi digital. *Journal of Information System, Graphics, Hospitality and Technology*, *6*(2), 51–57. https://doi.org/10.37823/insight.v6i2.405

Pradipta, V. D. A., Putra, V. F. F. G. E., Nugroho, R. E., Jap, D. C., Djwa, I. G., & Sundoro, B. T. (2024). Pencegahan risiko penyebaran phising dan hoaks dengan pembuatan video edukasi untuk siswa sekolah menengah pertama. *Prosiding KONSTELASI*, *1*(1), 59–68. https://ojs.uajy.ac.id/index.php/prosidingkonstelasi/article/view/8969

Primananda, M. A., Rasyad, P. A., Hibatullah, A., Gading, M., Hadhani, B., Tambunan, D., Rinanti, P., Harley, B. M., Zulfikar, F. R., Akbar, M. D., & Otniel, K. (2023). Bahaya phising di kalangan remaja melek internet kepada siswa/i SMA Pattimura Jakarta Selatan. *Jurnal Pengabdian Masyarakat Mandira Cendikia*, *2*(11), 88–99. https://journal.mandiracendikia.com/index.php/pkm/article/view/710

Rana, V., Verhoeven, B., & Sharma, M. (2025). Generative AI in design thinking pedagogy: Enhancing creativity, critical thinking, and ethical reasoning in higher education. *Journal of University Teaching and Learning Practice*, *22*(4). https://doi.org/10.53761/tjse2f36

Rodríguez-Díaz, M., & Rodríguez-Ferrándiz, R. (2026). Digital literacy and critical thinking in higher education: Gaps and training opportunities in the post-truth era. *Education Sciences*, *16*(5), 684. https://doi.org/10.3390/educsci16050684

Soraya, N. N., Juliastuti, R., & Mardiansyah, I. (2026). Pemberdayaan literasi digital berbasis partisipatif untuk menghadapi hoaks dan penipuan online. *Indonesian Engagement Journal*, *7*(1), 84–105. https://doi.org/10.21154/inej.v7i1.13306

Tondeur, J., Trevisan, O., Howard, S., & van Braak, J. (2025). Preparing preservice teachers to teach with digital technologies: An update of effective SQD-strategies. *Computers & Education*, *232*, 105262. https://doi.org/10.1016/j.compedu.2025.105262

Tsary, S. R., & Muttaqin, A. D. (2026). Edukasi literasi digital: Peningkatan kesadaran masyarakat dalam mengidentifikasi video hoaks berbasis artificial intelligence (AI) di Kelurahan Pucangsawit, Kota Surakarta. *AJAD Jurnal Pengabdian kepada Masyarakat*, *6*(2), 445–451. https://doi.org/10.59431/ajad.v6i2.869

Yaseen, H., Mohammad, A. S., Ashal, N., Abusaimeh, H., Ali, A. A. A., & Sharabati, A.-A. A. (2025). The impact of adaptive learning technologies, personalized feedback, and interactive AI tools on student engagement: The moderating role of digital literacy. *Sustainability*, *17*(3), 1133. https://doi.org/10.3390/su17031133

Yusop, M. I. M., Kamarudin, N. H., Suhaimi, N. H. S., & Hasan, M. K. (2025). Advancing passwordless authentication: A systematic review of methods, challenges, and future directions for secure user identity. *IEEE Access*, *13*, 13919–13943. https://doi.org/10.1109/access.2025.3528960