DOI: https://doi.org/10.31849/dinamisia.v10i5.34731

Introduction to Cybersecurity for Teachers and Students of SMA Plus Putra Melati, Jonggol, Regarding Digital Crime Threats

Pengenalan Keamanan Siber bagi Guru dan Siswa SMA Plus Putra Melati, Jonggol terhadap Ancaman Kejahatan Digital

Vina Ardelia Effendy*[1], Deni Utama[2], Muhammad Ridho Kurniawan Pratama[3], Prasetyo Wibowo Yunanto[4], Fuad Mumtas[5]
[1,2,3,4,5]Universitas Negeri Jakarta
E-mail: vinaardelia@unj.ac.id [1], deniutama@unj.ac.id [2], ridhopratama@unj.ac.id [3], prasetyo.wy@unj.ac.id [4], fuadmumtas@unj.ac.id [5]

Abstract

This community service activity aims to improve cybersecurity literacy and awareness at SMA Plus Putra Melati, Jonggol. The activity involved 20 students and two teachers as active participants whose understanding was evaluated. The implementation was carried out over two days through online sessions focusing on basic concepts, and offline sessions for hands-on practice in identifying digital threats and account protection. Actual evaluation results using pre-test and post-test showed increase in the average score, from 3,68 to 4,21. The main achievement was seen in the participants' improved practical ability to recognize malware, although theoretical understanding of cybersecurity still requires reinforcement. The tangible outputs of this community service activity are educational modules and digital account protection guidelines that have been handed over to the school to support the sustainability of cybersecurity practices in the educational environment.

Keywords*: Cybersecurity, Digital literacy, High school students, Phishing, Malware, Community service*

Abstrak

Kegiatan pengabdian kepada masyarakat ini bertujuan untuk meningkatkan literasi dan kesadaran keamanan siber di SMA Plus Putra Melati, Jonggol. Kegiatan ini melibatkan 20 siswa dan dua guru sebagai peserta aktif yang dievaluasi pemahamannya. Pelaksanaan dilakukan selama dua hari melalui sesi daring yang berfokus pada pemahaman konsep dasar, serta sesi luring untuk praktik langsung identifikasi ancaman digital dan perlindungan akun. Hasil evaluasi aktual menggunakan pre-test dan post-test menunjukkan adanya peningkatan skor rerata yakni dari 3,68 menjadi 4,21. Capaian utama terlihat pada peningkatan kemampuan praktis peserta dalam mengenali malware, meskipun pemahaman teoretis keamanan siber masih memerlukan penguatan. Luaran nyata dari kegiatan pengabdian ini adalah modul edukasi dan panduan perlindungan akun digital yang telah diserahkan kepada pihak sekolah guna mendukung keberlanjutan praktik keamanan siber di lingkungan pendidikan.

Kata kunci: *Keamanan siber, Literasi digital, Siswa sekolah menengah, Phishing, Malware, Pengabdian kepada masyarakat*

1. PENDAHULUAN

Penetrasi internet di kalangan remaja Indonesia terus meningkat secara signifikan. Menurut data BPS dari hasil pendataan Survei Susenas 2024, terdapat 72,78 persen penduduk Indonesia telah mengakses internet di tahun 2024 dan 69,21 persen di tahun 2023 (Direktorat Statistik Keuangan, 2025). Tingginya penggunaan internet ini menunjukkan bahwa masyarakat memiliki akses yang lebih luas terhadap sumber informasi dan menjadi indikator kesiapan suatu negara atau wilayah dalam menghadapi era transformasi digitalsementara laporan Digital 2024: Indonesia dari We Are Social, menempatkan Indonesia sebagai salah satu negara dengan rata-rata

DOI: https://doi.org/10.31849/dinamisia.v10i5.34731

penggunaan internet tertinggi di dunia, mencapai 7 jam 38 menit per hari (Social, 2026). Di lingkungan sekolah menengah, perangkat digital dan platform daring telah menjadi bagian tak terpisahkan dari kegiatan pembelajaran, komunikasi antarsiswa, serta akses informasi (Selwyn, 2016). Namun, tingginya intensitas penggunaan ini tidak diiringi oleh pemahaman keamanan siber yang memadai, sehingga siswa menjadi kelompok yang rentan terhadap berbagai bentuk kejahatan digital (Bada, 2019)

Ancaman siber yang paling umum dialami pelajar mencakup *phishing*, penggunaan kata sandi lemah, penyebaran *malware*, *cyberbullying*, dan kebocoran data pribadi. Studi Proofpoint (2024) melaporkan bahwa 84% organisasi di seluruh dunia mengalami setidaknya satu serangan *phishing* berhasil, dengan pengguna yang kurang teredukasi menjadi sasaran utama (Chavez, 2026). Di Indonesia, Badan Siber dan Sandi Negara (BSSN, 2026) mencatat lebih dari 400 juta anomali trafik siber sepanjang tahun 2022, yang sebagian besar menarget pengguna awam melalui rekayasa sosial dan tautan palsu.

Banyak remaja tidak sepenuhnya memahami risiko yang terkait dengan kegiatan *online*, termasuk *phishing*. Banyak yang tidak menyadari bahwa memberikan informasi pribadi secara sembarangan dapat berakibat pada pencurian identitas atau penipuan finansial (Zamachsari, 2021). Kondisi ini diperparah oleh kebiasaan penggunaan kata sandi yang lemah: survei NordPass menunjukkan bahwa kombinasi sederhana seperti "123456" dan tanggal lahir masih mendominasi pilihan kata sandi pengguna muda di Asia Tenggara (NordPass, 2026).

Selain itu, ancaman *malware* yang disebarkan melalui aplikasi APK palsu via WhatsApp semakin marak di Indonesia. Modus kejahatan siber menggunakan akun WhatsApp yang sebelumnya telah diretas untuk mendistribusikan lampiran berbahaya. Pesan dikirim dari kontak yang sudah ada di akun tersebut, yang meningkatkan kemungkinan penerima akan melihat file tersebut (Kaspersky, 2026). Pada saat bersamaan, *cyberbullying* menjadi ancaman sosial serius: laporan UNICEF 2019 mengungkapkan bahwa satu dari tiga remaja di 30 negara pernah menjadi korban perundungan daring, dengan dampak psikologis yang signifikan terhadap kesehatan mental dan prestasi akademik (UNICEF, 2026). Ketidakmampuan mengenali dan merespons ancaman-ancaman ini bukan semata masalah teknis, melainkan mencerminkan kesenjangan literasi keamanan digital yang mendasar (Hadlington, 2017)

Kesenjangan antara intensitas penggunaan teknologi dan tingkat literasi keamanan siber di kalangan pelajar mendorong perlunya intervensi edukasi yang terstruktur dan berbasis praktik. Pendekatan edukasi keamanan siber yang efektif perlu mengintegrasikan pemahaman konseptual dengan pengalaman praktik secara langsung. Pembelajaran berbasis pengalaman memungkinkan siswa berinteraksi langsung dengan simulasi ancaman dalam lingkungan yang aman, sehingga proses pembelajaran menjadi lebih bermakna dan kontekstual. Pendekatan ini dinilai lebih efektif dibandingkan metode ceramah semata dalam membentuk pemahaman jangka panjang (Khudin et al., 2026).

Pengetahuan mengenai keamanan siber sangat penting untuk melindungi aktivitas yang berkaitan dengan transaksi (Zwilling et al., 2022). Pengetahuan ini mencakup segala hal yang dipahami melalui pengalaman pribadi. Di sisi kelembagaan, sekolah menjadi ruang strategis untuk intervensi ini mengingat remaja menghabiskan sebagian besar waktunya di lingkungan tersebut, serta guru dapat berperan sebagai agen penguat literasi digital secara berkelanjutan (Derek et al., 2025).

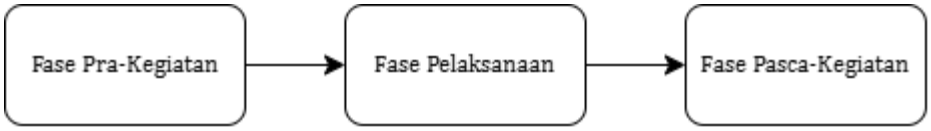
Berdasarkan identifikasi masalah dan kondisi mitra di atas, kegiatan pengabdian kepada masyarakat ini dilaksanakan dengan meningkatkan pemahaman siswa dan guru tentang ancaman siber umum (*phishing, malware, password lemah, cyberbullying*), melatih keterampilan praktis perlindungan akun (2FA, password kuat, verifikasi pesan), dan membangun kepercayaan diri dan kebiasaan digital aman yang berkelanjutan.

2. METODE

Kegiatan pengabdian kepada masyarakat ini dilaksanakan di SMA Plus Putra Melati, Kecamatan Jonggol, Kabupaten Bogor, pada 12 Juni 2026 secara daring dan 18 Juni 2026 secara

DOI: https://doi.org/10.31849/dinamisia.v10i5.34731

luring. Pelaksanaan berlangsung dalam dua hari: sesi pertama dilakukan secara daring selama ±3 jam melalui platform Zoom, dan sesi kedua dilakukan secara luring di ruang kelas sekolah selama ±4 jam. Peserta kegiatan ini sebanyak 20 siswa kelas X dan XI dan dua orang guru di SMA Plus Putra Melati yang dipilih oleh pihak sekolah. Rentang usia siswa berkisar antara 15–17 tahun. Kegiatan ini dilaksanakan dengan tiga fase: pra-kegiatan, pelaksanaan, dan pasca-kegiatan (Effendy et al., 2025), dapat dilihat pada Gambar 1.



Gambar 1. Tahapan Pelaksanaan Pengabdian kepada Masyarakat

1. Fase Pra-Kegiatan

Fase ini mencakup koordinasi awal dengan pihak sekolah. Tahap sosialisasi merupakan langkah awal untuk membangun pemahaman dan komitmen bersama antara tim pengusul dan mitra sasaran. Kegiatan sosialisasi dilakukan melalui koordinasi dengan pihak sekolah, guru, dan perwakilan siswa untuk menjelaskan tujuan, manfaat, dan rangkaian kegiatan pengabdian kepada masyarakat. Pada tahap ini juga dilakukan identifikasi awal tingkat pemahaman mitra terkait keamanan siber melalui diskusi dan pengisian kuesioner (*pre-test*). Sosialisasi bertujuan untuk menumbuhkan kesadaran awal mengenai pentingnya keamanan siber serta memastikan kesiapan mitra dalam mengikuti seluruh rangkaian kegiatan yang telah direncanakan (Afriyani et al., 2026).

2. Fase Pelaksanaan, mencakup kegiatan-kegiatan berikut:

a. Hari Pertama — Sesi Daring (±3 jam, 12 Juni 2026)

Sesi daring diselenggarakan melalui platform Zoom dan difokuskan pada pembangunan pemahaman konseptual. Materi yang disampaikan meliputi:

1. Konsep dasar keamanan siber: definisi *cybersecurity*, perbedaan *Threat*, *Vulnerability*, dan *Risk* dalam konteks digital;
2. Jejak digital dan implikasinya bagi reputasi serta privasi jangka panjang;
3. Pengenalan modus *phishing* melalui surel dan pesan instan, disertai kerangka kerja *STOP–THINK–VERIFY* sebagai panduan verifikasi pesan mencurigakan;
4. Risiko penggunaan kata sandi lemah dan berulang (*password reuse*), serta kriteria kata sandi yang kuat;
5. Pengenalan *malware* dan modus penyebaran file APK berbahaya melalui WhatsApp (contoh kasus: undangan pernikahan palsu dan notifikasi kurir paket);
6. Pemahaman *cyberbullying*, dampak psikologisnya terhadap korban, dan panduan respons etis berbasis prinsip *THINK* (*True, Helpful, Inspiring, Necessary, Kind*).

b. Hari Kedua — Sesi Luring (±4 jam, 18 Juni 2026)

Sesi luring dilaksanakan di ruang kelas dan berfokus pada praktik langsung dalam tiga tantangan terstruktur:

1. *2FA Security Challenge*: Peserta mempraktikkan aktivasi *Two-Factor Authentication* (2FA) pada akun Google masing-masing secara langsung di perangkat *smartphone*, dengan bimbingan fasilitator tahap per tahap.
2. *Phishing Detective Challenge*: Peserta disajikan sejumlah contoh tangkapan layar pesan dan tautan dari berbagai platform (WhatsApp, Gmail, Instagram), kemudian diminta mengidentifikasi ciri-ciri *phishing* dan memberi justifikasi atas penilaian mereka menggunakan kerangka *STOP–THINK–VERIFY*.
3. *Cyber Hygiene Action Plan*: Peserta menyusun rencana tindakan digital pribadi secara tertulis, mencakup langkah penggantian kata sandi lama, pengaktifan 2FA, dan komitmen kebiasaan digital aman yang akan diterapkan dalam kehidupan sehari-hari.

DOI: https://doi.org/10.31849/dinamisia.v10i5.34731

3. Fase Pasca-kegiatan
   a. Pendampingan dan Evaluasi

      Pendampingan dilakukan setelah kegiatan untuk memastikan bahwa siswa mampu menerapkan pemahaman keamanan siber secara konsisten. Tim pengusul melakukan pendampingan melalui diskusi lanjutan, tanya jawab, serta pemantauan sederhana terhadap pemahaman dan perilaku peserta. Evaluasi pelaksanaan program dilakukan melalui pengukuran post-test, observasi selama kegiatan, serta pengumpulan umpan balik dari mitra sasaran. Evaluasi ini bertujuan untuk menilai efektivitas metode yang digunakan, tingkat pencapaian luaran, serta mengidentifikasi kendala yang dihadapi selama pelaksanaan kegiatan (Ulfa & Syafitri, 2026).

   b. Keberlanjutan Program

      Untuk menjamin keberlanjutan program, tim pengusul menyerahkan modul dan materi edukasi keamanan siber kepada pihak sekolah sebagai bahan pembelajaran lanjutan. Guru didorong untuk mengintegrasikan materi keamanan siber ke dalam kegiatan pembelajaran atau kegiatan literasi sekolah. Selain itu, sekolah diharapkan dapat menunjuk perwakilan guru sebagai penggerak literasi keamanan digital agar dampak kegiatan dapat terus dirasakan setelah program selesai dilaksanakan.

Evaluasi kegiatan menggunakan instrumen kuesioner dengan skala Likert lima poin (1 = Sangat Tidak Setuju hingga 5 = Sangat Setuju) yang terbagi dalam dua tahap: pre-test (sebelum kegiatan) dan post-test (setelah kegiatan). Instrumen pre-test mencakup tujuh butir yang tersebar di empat domain. Skala Likert digunakan untuk menilai sikap, opini, dan persepsi responden untuk mengukur tingkat pemahaman mereka terhadap kegiatan ini. Tabel 1 berikut berisi penjelasan tentang 5 (lima) poin skala tersebut (Effendy et al., 2025).

Tabel 1. Kriteria Skala Likert

Bobot	Kriteria
1	Sangat Tidak Setuju
2	Tidak Setuju
3	Netral
4	Setuju
5	Sangat Setuju

Perlu ditekankan bahwa instrumen berskala Likert ini mengukur persepsi diri (*self-perceived competence*) peserta. Hasil interpretasi difokuskan pada pemahaman terhadap ancaman keamanan siber, panduan keterampilan praktis perlindungan akun digital, termasuk pembuatan kata sandi kuat, aktivasi *Two-Factor Authentication* (2FA), dan pemeriksaan kebocoran data; serta kewaspadaan dan kepercayaan diri siswa dalam merespons insiden siber yang umum terjadi di lingkungan sehari-hari.

Tabel 2. Indikator Kuesioner

Domain	Kode	Indikator
A. Pemahaman Dasar Keamanan Siber	A1	Definisi dan urgensi keamanan siber
	A2	Pembedaan *Threat*, *Vulnerability*, dan *Risk*
	A3	Dampak jangka panjang jejak digital

DOI: https://doi.org/10.31849/dinamisia.v10i5.34731

B. Pemahaman Ancaman Digital	B1	Mengenali ciri *phishing* (*STOP–THINK–VERIFY)*
	B2	Risiko password reuse, kriteria kata sandi kuat, dan penerapan *Two-Factor Authentication* (2FA)
	B3	Identifikasi *malware* dan APK palsu di WhatsApp
	B4	Respons bijak *cyberbullying* (prinsip *THINK*)

3. HASIL DAN PEMBAHASAN

Kegiatan pengabdian kepada masyarakat di SMA Plus Putra Melati berlangsung dalam dua sesi pada tanggal yang berbeda: sesi daring pada 12 Juni 2026 melalui platform Zoom selama ±3 jam, dan sesi luring pada 18 Juni 2026 di ruang kelas selama ±4 jam. Dari 20 siswa dan dua guru yang terdaftar sebagai peserta yang mengisi kuesioner evaluasi secara lengkap.

Pelaksanaan sesi daring mencakup enam topik yang disampaikan secara berurutan: (1) konsep dasar keamanan siber beserta pembedaan *threat*, *vulnerability*, dan *risk*; (2) jejak digital dan implikasinya bagi privasi jangka panjang; (3) pengenalan modus *phishing* disertai kerangka kerja *STOP–THINK–VERIFY*; (4) risiko *password reuse* dan kriteria *password* kuat; (5) pengenalan *malware* dan modus APK palsu via WhatsApp; serta (6) pemahaman *cyberbullying* dan prinsip *THINK*. Metode penyampaian melibatkan presentasi slide interaktif, studi kasus autentik, dan sesi tanya jawab. Setelah sesi daring, peserta mendapatkan jeda enam hari sebelum bertemu kembali pada sesi luring untuk melaksanakan tiga tantangan praktik terstruktur dapat dilihat pada Gambar 2.



Gambar 2. Kegiatan pengabdian masyarakat secara daring

Capaian pada sesi luring, peserta mempraktikkan aktivasi *Two-Factor Authentication* (2FA) pada akun Google masing-masing secara langsung menggunakan *smartphone* dengan pendampingan fasilitator. Seluruh peserta berhasil menyelesaikan proses aktivasi. Nilai pembelajaran yang dapat diambil, peserta menyadari bahwa manajemen akun masih buruk termasuk tidak memiliki informasi pemulihan merupakan kerentanan dalam keamanan siber.

Selanjutnya, tugas kedua terkait *Phishing Detective Challenge*. Peserta disajikan sejumlah tangkapan layar pesan serta tautan dari email dan indtagram. Peserta diminta mengidentifikasi

DOI: https://doi.org/10.31849/dinamisia.v10i5.34731

mana yang merupakan upaya *phishing* menggunakan kerangka *STOP–THINK–VERIFY*. Sesi ini mengungkap bahwa peserta memiliki kemampuan yang lebih baik dalam mengenali *phishing.*

Pada tugas ketiga *Cyber Hygiene Action Plan*. Setiap peserta melakukan Tindakan keamanan siber, seperti: mengganti kata sandi akun prioritas menjadi *password* kuat (minimal 12 karakter, kombinasi huruf besar-kecil, angka, dan simbol), mengaktifkan 2FA pada akun-akun penting, dan tidak mengunduh aplikasi dari sumber tidak resmi.

Kegiatan ini menghasilkan luaran yang diserahkan kepada pihak sekolah, meliputi: modul pelatihan keamanan siber dalam format dokumen, panduan aktivasi 2FA langkah per langkah dalam Bahasa Indonesia untuk akun Google. Seluruh materi ini secara resmi diserahkan kepada Kepala Sekolah pada 18 Juni 2026. Kegiatan luring dapat dilihat pada Gambar 3.



Gambar 3. Kegiatan pengabdian masyarakat secara luring

Evaluasi pemahaman peserta dilaksanakan menggunakan instrumen kuesioner berskala Likert lima poin yang tersebar dalam dua domain: Domain A (Pemahaman Dasar Keamanan Siber, tiga butir: A1, A2, A3) dan Domain B (Pemahaman Ancaman Digital, empat butir: B1, B2, B3, B4). Instrumen yang sama digunakan pada *pre-test* (sesi daring, 12 Juni 2026) dan *post-test* (sesi luring, 18 Juni 2026).

Kegiatan ini terdapat dua rangkaian tes untuk mengetahui tingkat pemahaman peserta. Berdasarkan hasil analisis data instrumen *pre-test* dan *post-test* pada kegiatan pengabdian masyarakat di SMA Plus Putra Melati, secara umum terjadi peningkatan rata-rata dari 3,68 pada *pre-test* menjadi 4,21 pada *post-test*. Masing-masing kelompok indikator memberikan gambaran pemahaman teoritis serta kapasitas praktis dari peserta. Berikut gambaran rata-rata nilai per indikator keamanan siber pada Tabel 3.

Tabel 3. Perbandingan Rerata Skor *Pre-Test* dan *Post-Test* per Indikator dan Domain

Domain	Kode	Indikator Pernyataan	*Pre-test*	*Post-test*	Rerata
Pemahaman Dasar Keamanan Siber	A1	Definisi dan urgensi keamanan siber	3,75	4,50	0,75
	A2	Pembedaan *Threat*, *Vulnerability*, *Risk*	3,75	3,75	0,00
	A3	Dampak jangka panjang jejak digital	3,75	4,25	0,50
Rerata Domain A			3,75	4,17	0,42
Pemahaman	B1	Mengenali ciri *phishing*	3,75	4,12	0,38

DOI: https://doi.org/10.31849/dinamisia.v10i5.34731

Domain	Kode	Indikator Pernyataan	*Pre-test*	*Post-test*	Rerata
Ancaman Digital		(*STOP–THINK–VERIFY*)			
	B2	Risiko *password reuse* dan *password* kuat	3,62	4,25	0,63
	B3	Identifikasi *malware* dan APK palsu WhatsApp	3,25	4,25	1,00
	B4	Respons bijak *cyberbullying* (prinsip *THINK*)	3,88	4,38	0,50
Rerata Domain B			3,62	4,25	0,62
Rata-rata keseluruhan			3,68	4,21	0,54

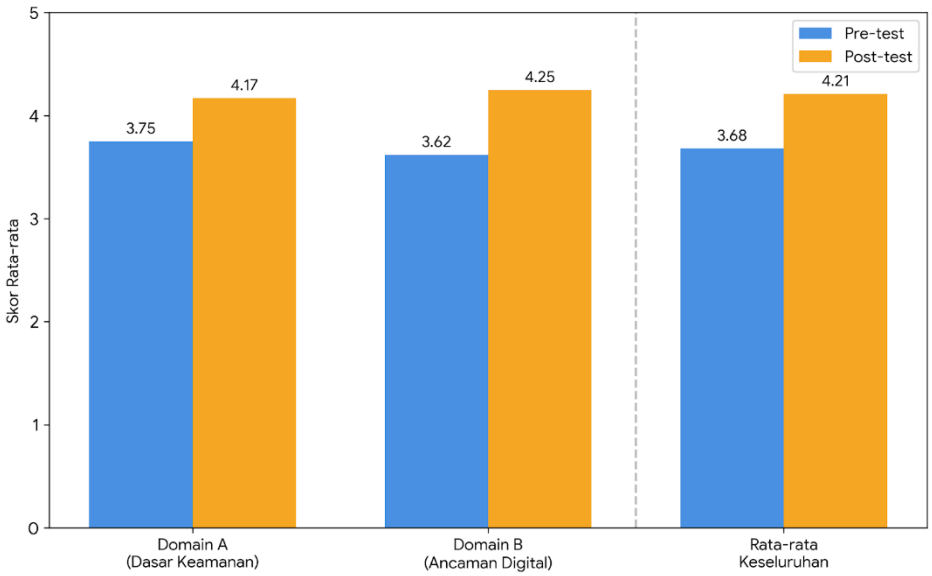
Secara keseluruhan, kegiatan edukasi keamanan siber ini menunjukkan hasil yang sangat positif dengan adanya peningkatan nilai rata-rata keseluruhan sebesar 0,54 poin, yaitu dari 3,68 pada *pre-test* menjadi 4,21 pada *post-test*. Peningkatan ini terdistribusi ke dalam dua area evaluasi utama, yakni Pemahaman Dasar Keamanan Siber (Domain A) dan Pemahaman Ancaman Digital (Domain B).

Pada Domain A yang mengukur Pemahaman Dasar Keamanan Siber, rata-rata skor peserta mengalami peningkatan sebesar 0,42 poin, bergerak dari angka 3,75 menjadi 4,17. Kenaikan paling signifikan di domain ini terlihat pada pemahaman peserta mengenai definisi dan urgensi keamanan siber (A1), yang melonjak 0,75 poin hingga mencapai skor tertinggi yakni 4,50. Selain itu, kesadaran mengenai dampak jangka panjang jejak digital (A3) juga menunjukkan tren positif dengan kenaikan 0,50 poin menjadi 4,25. Meski demikian, terdapat catatan khusus pada materi pembedaan konsep *Threat, Vulnerability*, dan *Risk* (A2). Pada indikator tersebut sama sekali tidak terjadi peningkatan, di mana nilai tertahan pada angka 3,75. Hal ini mengindikasikan bahwa istilah teknis dan konsep teoretis tersebut masih cukup sulit dipahami oleh peserta.

Sementara itu, Domain B yang membahas Pemahaman Ancaman Digital menunjukkan tingkat keberhasilan yang lebih tinggi dengan rata-rata peningkatan sebesar 0,62 poin, naik dari 3,62 menjadi 4,25. Seluruh indikator pada domain ini berhasil mengalami perbaikan. Lonjakan pemahaman paling tajam terjadi pada kemampuan identifikasi *malware* dan APK palsu WhatsApp (B3), dengan kenaikan sebesar 1,00 poin dari nilai awal terendah yakni 3,25 berhasil mengejar ke angka 4,25. Kesadaran peserta mengenai risiko *password reuse* dan pentingnya *password* kuat (B2) juga membaik dengan peningkatan sebesar 0,63 poin. Di samping itu, etika dan kewaspadaan bermedia sosial turut meningkat, yang ditunjukkan oleh naiknya skor indikator respons bijak terhadap *cyberbullying* (B4) sebesar 0,50 poin menjadi 4,38, serta kemampuan mengenali ciri *phishing* (B1) yang bertambah 0,38 poin menjadi 4,12.

Kegiatan ini memberikan dampak positif terutama dalam meningkatkan kewaspadaan serta kecakapan peserta terhadap ancaman digital yang bersifat praktis dan sering dijumpai sehari-hari. Akan tetapi, untuk pelaksanaan program ke depannya, diperlukan pendekatan atau metode pembelajaran yang lebih sederhana dan mudah dicerna agar materi-materi yang sifatnya konseptual, seperti perbedaan istilah dalam keamanan siber, dapat dipahami dengan sama baiknya oleh para peserta.

DOI: https://doi.org/10.31849/dinamisia.v10i5.34731



Gambar 4. Perbandingan rata-rata skor per domain keamanan siber

Melalui grafik perbandingan akhir di atas, kita dapat melihat dengan jelas perkembangan skor dari masing-masing area evaluasi. Pada Domain A, skor *pre-test* peserta bermula pada angka 3,75 yang sedikit lebih tinggi dibandingkan Domain B, dan kemudian mengalami peningkatan menjadi 4,17 pada saat *post-test*. Sebaliknya, Domain B yang awalnya memiliki skor *pre-test* lebih rendah yakni 3,62, justru berhasil menyalip dan memperoleh skor akhir *post-test* yang lebih tinggi dibandingkan Domain A, yaitu mencapai 4,25. Peningkatan drastis ini menunjukkan bahwa tingkat penyerapan materi praktis mengenai ancaman digital berjalan dengan sangat baik di kalangan peserta. Pencapaian positif dari kedua domain tersebut pada akhirnya saling melengkapi dan berkontribusi secara langsung terhadap kenaikan rata-rata keseluruhan program, yang bergerak naik dari 3,68 menjadi 4,21.

4. KESIMPULAN

Kegiatan pengabdian masyarakat mengenai edukasi keamanan siber di SMA Plus Putra Melati telah menunjukkan adanya peningkatan pemahaman peserta. Peningkatan yang paling menonjol terlihat pada domain pemahaman ancaman digital, khususnya pada kemampuan peserta dalam mengenali ancaman *malware* dan *file* APK palsu di WhatsApp. Sebaliknya, domain pemahaman dasar keamanan siber masih memerlukan penguatan. Hal ini terlihat jelas pada indikator yang membahas konsep teoretis mengenai pembedaan *Threat, Vulnerability*, dan *Risk*, di mana tidak terjadi peningkatan nilai sama sekali dari sebelum hingga sesudah pelatihan.

Pelaksanaan kegiatan ini juga memiliki beberapa keterbatasan, seperti durasi pelatihan yang cukup singkat yakni hanya dalam dua hari, serta instrumen evaluasi yang pengukurannya masih bergantung pada persepsi diri (*self-perceived*) dari para peserta. Sebagai langkah penyempurnaan ke depannya, pihak sekolah disarankan untuk melaksanakan tindak lanjut yang berfokus pada praktik keamanan akun secara langsung, pengadaan simulasi *phishing* secara berkala, serta pemberian pendampingan berkelanjutan oleh guru agar perilaku digital yang aman dapat menjadi kebiasaan sehari-hari para siswa.

DOI: https://doi.org/10.31849/dinamisia.v10i5.34731

UCAPAN TERIMA KASIH

Tim Pengabdian dengan tulus mengucapkan terima kasih kepada Fakultas Teknik, Universitas Negeri Jakarta selaku penyandang dana dan fasilitator program atas dukungan dana tersebut kami dapat melaksanakan seluruh rangkaian kegiatan pengabdian. Terima kasih turut disampaikan kepada SMA Plus Putra Melati, Jonggol selaku mitra pelaksana atas kerja sama, antusias, serta partisipasi aktif yang diberikan selama proses hingga kegiatan berlangsung.

DAFTAR PUSTAKA

Afriyani, F., Sari, D. k., Cahyani, S., & Heryati, A. (2026). Penguatan Ekonomi Kreatif UMKM Kopi "Borsalino" Melalui Inovasi Produk Dan Pemasaran Digital. *DINAMISIA: Jurnal Pengabdian Kepada Masyarakat, 10(1)*, 202-210. https://doi.org/10.31849/dinamisia.v10i1.29336

Bada, M. S. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv preprint arXiv*, 1901.02672.

BSSN. (2026, July 1). *Lanskap Keamanan Siber 2023*. Retrieved from EDUCSIRT: https://educsirt.kemendikdasmen.go.id/portal/berita/197

Chavez, P. (2026, 1 Juli). *Risky and They Know It: 96% of Risk-Taking Users Aware of the Dangers but Do It Anyway, 2024 State of the Phish Reveals*. Retrieved from Proofpoint: https://www.proofpoint.com/us/blog/security-awareness-training/2024-state-of-phish-report

Derek, S. V., Audita, S., Rahayu, E. D., & Nurhidayat, F. (2025). Peran Guru Dalam Meningkatkan Literasi Digital Di Kalangan Siswa. *Strategy Jurnal Inovasi Strategi dan Model Pembelajaran, 5(3)*, 281. https://doi.org/https://doi.org/10.51878/strategi.v5i3.6545

Direktorat Statistik Keuangan, T. I. (2025). *Statistik Telekomunikasi Indonesia 2024.* Jakarta: Badan Pusat Statistik.

Effendy, V. A., Sugiyanta, L., Idrus, A., Mumtas, F., Fahmi, R., & Utama, D. (2025). Introduction to Digital Marketing for Village Products to Encourage Local Community Business Innovation in Singasari Village, Jonggol. *Jurnal Pengabdian kepada Masyarakat, 10.55606/kreatif.v5i3.8386*, 568-569. https://doi.org/10.55606/kreatif.v5i3.8386

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon, 3(7)*, 2-4. https://doi.org/10.1016/j.heliyon.2017.e00346

Kaspersky. (2026, Juni 25). Retrieved from https://www.kaspersky.com/about/press-releases/kaspersky-uncovers-a-new-massive-campaign-spreading-malware-via-whatsapp

Khudin, F., Samudra, D. R., Fauzan, M., Utama, I., & Sarman. (2026). Pengembangan Modul Edukasi Interaktif Berbasis Web Untuk Deteksi Phishing Di MA Raudlatul Hidayah. *Journal of Artificial Intelligence and Digital Business (RIGGS), 4(4)*, 11878. https://doi.org/https://doi.org/10.31004/riggs.v4i4.5304

NordPass. (2026, July 1). *NordPass merilis 200 kata sandi paling umum tahun 2023.* Retrieved from Nord Security: https://nordsecurity.com/press-area/nordpass-released-the-200-most-common-passwords-of-2023

Selwyn, N. (2016). *Education and technology: Key issues and debates.* London: Bloomsbury Academic. https://doi.org/10.1007/s11159-022-09971-9

Social, W. A. (2026, Juli 1). *Digital 2024*. Retrieved from wearesocial.com: https://wearesocial.com/id/blog/2024/01/digital-2024/

Ulfa, M., & Syafitri, S. E. (2026). Pelatihan Pembuatan Digital Booklet Berbasis Canva untuk Meningkatkan Keterampilan Membuat Media Kreatifdi Era Digital Society 5,0 pada Guru Sekolah Dasar di Kabupaten Gayo Luwes. *DINAMISIA: Jurnal Pengabdian Kepada Masyarakat, 10(1)*, 17-22. https://doi.org/https://doi.org/10.31849/dinamisia.v9i6.29182

DOI: https://doi.org/10.31849/dinamisia.v10i5.34731

UNICEF. (2026, Juni 26). *Survei UNICEF*. Retrieved from UNICEF: https://www.unicef.org/press-releases/unicef-poll-more-third-young-people-30-countries-report-being-victim-online-bullying

Zamachsari, F. &. (2021). Penerapan Deep Learning dalam Deteksi Penipuan Transaksi Keuangan Secara Elektronik. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi), 5(2)*, 203-212. https://doi.org/10.29207/resti.v5i2.2952

Zwilling, M., Klien, G., Lesjak, D., & Wiechetek, L. (2022). Cyber Security Awareness,Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems, 62(1)*, 82-97. https://doi.org/10.1080/08874417.2020.1712269