

Sosialisasi dan Edukasi Keamanan Digital untuk Meningkatkan Kesadaran Siswa terhadap Ancaman Siber di SMP Muhammadiyah 1 Samarinda

Alvin Ari Pradhana^{1,*}, Muhammad Restu Al Hidayat², Trisna Aprilia³, Hiskya Harsyal Kila⁴, Vina Zahrotun Kamila⁵, Hario Jati Setyadi⁶, Akhmad Irsyad⁷, Islamiyah Islamiyah⁸, Muhammad Fawaz Saputra⁹, Amin Padmo Azam Masa¹⁰

^{1), 2), 3), 4), 5), 6), 7), 8), 9), 10)} Program Studi Sistem Informasi, Fakultas Teknik, Universitas Mulawarman

Jalan Sambaliung No. 9 Gunung Kelua, Samarinda, 75119

E-Mail : aplinnnn@gmail.com ¹⁾; hrestu24official@gmail.com ²⁾; trisnaaprilia245@gmail.com ³⁾;

hiskyakila@gmail.com ⁴⁾; vinakamila@ft.unmul.ac.id ⁵⁾; hariojati.setyadi@unmul.ac.id ⁶⁾;

akhmadirsyad@unmul.ac.id ⁷⁾; islamiyah@unmul.ac.id ⁸⁾; muhammadfawaz@unmul.ac.id ⁹⁾;

aminpadmo@unmul.ac.id ¹⁰⁾

ABSTRAK

Perkembangan teknologi digital membawa kemudahan sekaligus ancaman keamanan yang semakin meningkat, terutama bagi siswa SMP yang merupakan pengguna aktif internet namun memiliki literasi keamanan digital yang rendah. Kegiatan pengabdian kepada masyarakat ini bertujuan meningkatkan pemahaman dan kesadaran siswa SMP Muhammadiyah 1 Samarinda terhadap ancaman siber serta langkah-langkah perlindungan akun digital. Metode yang digunakan adalah sosialisasi interaktif dengan penyampaian materi mengenai phishing, aplikasi modifikasi berbahaya, teknik password kuat, Google Account Manager, verifikasi dua langkah, dan etika keamanan internet. Evaluasi dilakukan melalui pre-test dan post-test untuk mengukur peningkatan pemahaman siswa. Kegiatan dilaksanakan pada 24 Oktober 2025 dengan melibatkan 62 siswa dari seluruh tingkat kelas di sekolah. Hasil evaluasi menunjukkan peningkatan pemahaman siswa mengenai ancaman digital dan cara melindungi akun secara mandiri. Siswa mampu mengidentifikasi ciri-ciri phishing, memahami bahaya aplikasi modifikasi, dan menerapkan praktik keamanan dasar. Kegiatan ini berhasil membentuk kesadaran keamanan digital di lingkungan sekolah dan mendorong perilaku berinternet yang lebih aman, bijak, dan bertanggung jawab bagi siswa.

Kata Kunci – Keamanan Digital, Literasi Digital, Perlindungan Akun, Phising, Verifikasi Dua Langkah

ABSTRACT

The development of digital technology brings convenience as well as increasing security threats, especially for junior high school students who are active internet users but have low digital security literacy. This community service activity aims to increase the understanding and awareness of students at SMP Muhammadiyah 1 Samarinda regarding cyber threats and digital account protection measures. The method used was interactive socialization with material delivery on phishing, malicious modification applications, strong password techniques, Google Account Manager, two-step verification, and internet security ethics. Evaluation was conducted through pre-test and post-test to measure the increase in student understanding. The activity was carried out on October 24, 2025, involving 62 students from all grade levels at the school. Evaluation results showed an increase in student understanding of digital threats and how to protect accounts independently. Students were able to identify phishing characteristics, understand the dangers of modification applications, and apply basic security practices. This activity successfully built digital security awareness in the school environment and encouraged safer, wiser, and more responsible internet behavior among students.

Keywords – Digital Security, Digital Literacy, Account Protection, Phising, Two-Step Verification

1. PENDAHULUAN

Perkembangan teknologi digital telah memberikan banyak kemudahan bagi masyarakat, terutama bagi generasi yang tumbuh pada era internet. Namun, kemudahan tersebut tidak terlepas dari berbagai ancaman keamanan yang semakin meningkat, seperti phishing, aplikasi modifikasi berbahaya, pencurian data pribadi, hingga serangan yang menargetkan akun digital penting seperti Gmail, media sosial, dan aplikasi pembelajaran. Penelitian menunjukkan bahwa tingkat kesadaran keamanan digital di kalangan remaja masih rendah, khususnya dalam memahami ancaman seperti phishing, penyalahgunaan data pribadi, dan lemahnya pengelolaan kata sandi (Syakh Alam et al., 2025).

Siswa SMP sebagai pengguna aktif teknologi sering kali belum memahami risiko tersebut, sehingga menjadi kelompok yang paling rentan terhadap ancaman siber. Kurangnya literasi keamanan digital membuat siswa mudah

*) Correspondenting Author

tertipu oleh tautan palsu, iklan menyesatkan, atau pesan undian yang meminta login akun. Banyak dari mereka juga masih menggunakan password lemah, memakai password yang sama untuk banyak akun, serta belum mengaktifkan fitur keamanan tambahan seperti verifikasi dua langkah. Penelitian mengenai literasi dan keamanan digital semakin banyak dilakukan seiring meningkatnya penggunaan internet oleh pelajar di Indonesia, dengan temuan yang menunjukkan masih rendahnya tingkat pengetahuan, kepercayaan, dan kewaspadaan terhadap ancaman digital (Sanjaya et al., 2024). Ancaman social engineering yang menargetkan remaja semakin meningkat, memanfaatkan kurangnya pemahaman mereka terhadap pola-pola serangan siber (Yusuf Effendy & Oktiani, 2024).

Keamanan digital merupakan upaya untuk melindungi informasi, identitas, dan aktivitas pengguna dari berbagai ancaman siber yang memanfaatkan celah pada perangkat maupun perilaku pengguna (Saputra, 2023). Pada konteks siswa usia remaja, keamanan digital menjadi semakin penting karena mereka aktif menggunakan internet untuk belajar, berkomunikasi, hingga mengakses hiburan. Edukasi mengenai keamanan digital diperlukan untuk memastikan siswa mampu mengenali risiko serta menerapkan tindakan perlindungan yang tepat, terutama melalui strategi pendidikan kontekstual di lingkungan sekolah (Maisaroh et al., 2025). Dalam era cognitive warfare dan ancaman informasi yang semakin kompleks, literasi digital menjadi keterampilan fundamental yang harus dimiliki oleh generasi muda untuk membangun ketahanan informasi (Sugiarto, 2025).

Dalam memahami perilaku keamanan digital, Protection Motivation Theory (PMT) menjelaskan bahwa seseorang akan terdorong melakukan tindakan perlindungan apabila mereka memahami tingkat ancaman, merasa berisiko terkena ancaman, menyadari bahwa tindakan pencegahan itu efektif, serta memiliki kemampuan untuk melakukannya (Marikyan & Papagiannidis, 2025). Teori ini memberikan landasan konseptual untuk memahami bagaimana edukasi keamanan digital dapat mengubah perilaku siswa menuju praktik berinternet yang lebih aman.

Berdasarkan kondisi tersebut, program edukasi keamanan digital diperlukan sebagai langkah preventif untuk membekali siswa dengan pemahaman yang komprehensif mengenai ancaman siber dan strategi perlindungan akun. Kegiatan pengabdian kepada masyarakat ini bertujuan meningkatkan pemahaman dan kesadaran siswa SMP Muhammadiyah 1 Samarinda terhadap berbagai ancaman keamanan digital melalui sosialisasi interaktif, penyampaian materi edukatif, serta evaluasi pemahaman menggunakan pre-test dan post-test.

2. METODE

Kegiatan pengabdian kepada masyarakat ini dilaksanakan pada 24 Oktober 2025 di SMP Muhammadiyah 1 Samarinda, Jl. P. Hidayatullah Gg. Bakti No. 06, Kelurahan Pelabuhan, dengan melibatkan 62 siswa dari berbagai tingkat kelas yang didampingi oleh seorang guru pendamping. Pemilihan peserta dilakukan oleh pihak sekolah dengan mempertimbangkan keterwakilan dari setiap tingkat kelas agar materi yang disampaikan dapat menjangkau seluruh lapisan siswa di sekolah. Pelaksanaan kegiatan berlangsung pada pukul 08.00-09.30 WITA, dengan durasi yang disesuaikan agar tidak mengganggu jadwal pembelajaran reguler siswa.

A. Tahapan Pelaksanaan Kegiatan

Pelaksanaan kegiatan dirancang secara sistematis dengan beberapa tahapan yang telah disusun berdasarkan analisis kebutuhan dan karakteristik peserta. Setiap tahapan dirancang untuk memastikan materi keamanan digital dapat dipahami secara bertahap, mulai dari pengukuran pemahaman awal, penyampaian materi edukatif, hingga evaluasi akhir untuk mengukur efektivitas kegiatan. Tahapan pelaksanaan kegiatan adalah sebagai berikut :

a. Persiapan dan Koordinasi

Tim melakukan koordinasi dengan pihak sekolah untuk menentukan jadwal, ruangan, dan jumlah peserta. Persiapan materi presentasi, instrumen evaluasi (pre-test dan post-test), serta perlengkapan pendukung dilakukan sebelum pelaksanaan.

b. Pembukaan Kegiatan

Kegiatan dibuka oleh guru pendamping diikuti sambutan dari tim pengabdian. Siswa diberikan penjelasan singkat mengenai tujuan kegiatan dan garis besar materi yang akan disampaikan.

c. Pre-Test

Siswa mengerjakan pre-test untuk mengukur tingkat pemahaman awal mengenai keamanan digital. Pre-test terdiri dari lima soal pilihan ganda dan dua soal isian singkat yang mencakup topik phishing, password aman, verifikasi dua langkah, dan identifikasi situs berbahaya.

d. Penyampaian Materi

Materi disampaikan dalam tiga sesi utama. Sesi pertama berfokus pada pengenalan ancaman digital seperti phishing, aplikasi modifikasi, dan pencurian data pribadi. Sesi kedua membahas teknik mitigasi dasar dengan materi pembuatan password kuat yang mengacu pada standar keamanan terkini (Ariasa, 2025) dan praktik keamanan digital lainnya. Sesi ketiga berisi demonstrasi penggunaan Google Account Manager dan aktivasi verifikasi dua langkah yang mengadaptasi praktik keamanan yang telah terbukti efektif untuk melindungi akun pada layanan media sosial dan platform digital (Sari, 2025).

e. Post-Test dan Evaluasi

Setelah penyampaian materi, siswa mengerjakan post-test dengan soal yang sama untuk mengukur peningkatan pemahaman. Hasil pre-test dan post-test dibandingkan untuk menilai efektivitas kegiatan. Analisis perbandingan dilakukan segera setelah kegiatan untuk mengevaluasi sejauh mana tujuan pembelajaran telah tercapai dan mengidentifikasi area yang perlu mendapat perhatian khusus.

f. Sesi Tanya Jawab dan Penutupan

Kegiatan ditutup dengan sesi tanya jawab singkat untuk mengklarifikasi pemahaman siswa, dilanjutkan dengan penutupan resmi oleh guru pendamping. Sesi ini memberikan kesempatan bagi siswa untuk mendalami topik-topik tertentu yang masih memerlukan penjelasan lebih lanjut. Kegiatan diakhiri dengan harapan bahwa materi yang telah disampaikan dapat menjadi bekal bagi siswa dalam menjaga keamanan digital mereka di masa mendatang.

B. Metode Penyampaian

Metode yang digunakan dalam kegiatan ini dirancang untuk menciptakan pembelajaran yang aktif dan partisipatif, sehingga siswa tidak hanya menerima informasi secara pasif tetapi juga terlibat langsung dalam proses pembelajaran. Pendekatan multi-metode dipilih untuk mengakomodasi berbagai gaya belajar siswa dan memastikan materi keamanan digital dapat dipahami secara komprehensif. Adapun metode yang diterapkan adalah :

a. Penyampaian Interaktif

Materi disampaikan secara langsung dengan menggunakan media presentasi visual yang menarik dan mudah dipahami. Penyampaian dilakukan dengan gaya komunikasi dua arah, di mana siswa diajak untuk aktif merespons pertanyaan dan memberikan pendapat terkait topik yang sedang dibahas. Pendekatan ini bertujuan untuk menjaga keterlibatan siswa dan memastikan mereka memahami setiap konsep yang disampaikan.

b. Demonstrasi Praktis

Tim pengabdian menunjukkan langkah-langkah praktis penggunaan fitur keamanan akun Google secara detail, mulai dari cara mengakses pengaturan keamanan, mengaktifkan verifikasi dua langkah, hingga memeriksa aktivitas akun yang mencurigakan melalui Google Account Manager. Demonstrasi dilakukan menggunakan tampilan layar proyektor agar seluruh peserta dapat mengikuti setiap langkah dengan jelas, meskipun mereka tidak dapat mempraktikkan langsung pada perangkat mereka sendiri.

c. Diskusi Interaktif

Siswa diberikan kesempatan untuk bertanya dan berdiskusi mengenai pengalaman mereka terkait ancaman digital yang pernah mereka temui atau dengar. Sesi diskusi ini memungkinkan terjadinya pertukaran pengalaman antar siswa dan memberikan konteks nyata terhadap materi yang telah disampaikan. Diskusi juga berfungsi sebagai media untuk mengidentifikasi miskonsepsi atau kesalahpahaman siswa terkait keamanan digital, sehingga dapat diluruskan secara langsung oleh tim pengabdian.

d. Evaluasi Kuantitatif

Evaluasi dilakukan menggunakan pre-test dan post-test untuk mengukur peningkatan pemahaman siswa secara objektif. Instrumen evaluasi yang sama digunakan pada kedua tahap untuk memastikan validitas perbandingan hasil. Metode evaluasi ini memberikan data konkret mengenai efektivitas kegiatan dan membantu tim pengabdian dalam mengidentifikasi aspek materi yang telah berhasil dipahami serta aspek yang masih memerlukan penguatan.

C. Instrumen Evaluasi

Instrumen evaluasi yang digunakan terdiri dari tujuh butir soal yang mencakup aspek-aspek penting dalam keamanan digital. Soal-soal ini dirancang untuk mengukur pemahaman siswa secara komprehensif, baik dari segi pengetahuan teoritis maupun kemampuan aplikatif dalam menghadapi ancaman siber. Rincian instrumen evaluasi yang digunakan dalam kegiatan ini disajikan pada Tabel 1.

Tabel 1. Detail Instrumen Pre-Test dan Post-Test

No.	Deskripsi Soal	Jenis
1	Dari pernyataan berikut, manakah yang termasuk contoh phishing?	Pilihan Ganda
2	Password yang aman sebaiknya terdiri dari.....	Pilihan Ganda
3	Apa fungsi utama fitur 2-Step Verification (Verifikasi Dua Langkah)?	Pilihan Ganda
4	Salah satu tanda bahwa situs yang dikunjungi aman adalah.....	Pilihan Ganda
5	Dari pernyataan di bawah ini, mana yang merupakan cara melindungi akun Google?	Pilihan Ganda
6	Menurutmu, kenapa masih banyak orang yang jadi korban peretasan akun?	Isian
7	Langkah apa yang akan kamu lakukan untuk meningkatkan keamanan akunmu?	Isian

3. HASIL DAN PEMBAHASAN

Kegiatan sosialisasi dan edukasi keamanan digital dilaksanakan dengan lancar sesuai jadwal yang telah ditetapkan. Partisipasi siswa sangat antusias, terlihat dari keaktifan mereka dalam mengikuti setiap sesi kegiatan, mulai dari pre-test, penyampaian materi, hingga post-test dan sesi tanya jawab. Guru pendamping juga turut memberikan dukungan penuh selama kegiatan berlangsung. Selain itu, siswa menunjukkan ketertarikan tinggi terhadap materi yang disampaikan karena berkaitan langsung dengan aktivitas digital sehari-hari, khususnya dalam penggunaan media sosial dan layanan akun Google. Suasana pelaksanaan Sosialisasi dan Edukasi Keamanan Digital dapat dilihat pada Gambar 1 dan Gambar 2.



Gambar 1. Pelaksanaan Pre-Test oleh Peserta



Gambar 2. Penyampaian Materi Ancaman Siber

Siswa menunjukkan antusiasme tinggi dalam mengikuti seluruh rangkaian kegiatan, terlihat dari keaktifan mereka selama pre-test, penyampaian materi, hingga post-test dan sesi tanya jawab. Interaksi yang terbangun membuat proses pembelajaran lebih dinamis dan membantu meningkatkan pemahaman serta kesadaran siswa terhadap ancaman siber dalam aktivitas digital mereka. Kegiatan sosialisasi di akhiri dengan foto bersama seluruh peserta sebagaimana didokumentasikan pada Gambar 3.



Gambar 3. Foto Bersama Siswa SMP Muhammadiyah 1

A. Hasil Evaluasi Pre-Test dan Post-Test

Evaluasi pemahaman siswa dilakukan melalui pre-test sebelum penyampaian materi dan post-test setelah kegiatan berlangsung dengan melibatkan 62 orang peserta. Hasil evaluasi menunjukkan adanya perubahan tingkat pemahaman siswa terhadap keamanan digital, sebagaimana ditampilkan pada Tabel 2 dan Tabel 3. Rata-rata skor pre-test adalah 3,76 dari skala maksimal 5, sedangkan rata-rata skor post-test meningkat menjadi 4,15 yang menunjukkan peningkatan sebesar 0,39 poin atau 10,3%.

Tabel 2. Distribusi Hasil Pre-Test dan Post-Test

Kategori	Pre-Test		Post-Test		Perubahan (%)
	Jumlah Siswa	Persentase	Jumlah Siswa	Persentase	
Sangat Paham (4-5)	40	17,7%	49	79%	+14,5%
Cukup Paham (3)	11	17,7%	9	14,5	-3,2%
Belum Paham (1-2)	11	64,5%	4	6,5%	-11,2%

Tabel 3. Perubahan Pemahaman Siswa

Keterangan	Jumlah Siswa	Persentase
Meningkat	23 Orang	37,1%
Tetap	34 Orang	54,8%
Menurun	5 Orang	8,1%
Total	62 Orang	100%

Hasil pre-test menunjukkan bahwa tingkat pemahaman awal siswa mengenai keamanan digital masih bervariasi. Hal ini sejalan dengan temuan sebelumnya bahwa literasi digital pelajar di era teknologi masih perlu diperkuat, khususnya pada aspek keamanan dan etika digital (Yeyendra et al., 2024). Sebanyak 11 siswa (17,7%) berada pada kategori “Belum Paham”, 11 siswa (17,7%) pada kategori “Cukup Paham”, dan 40 siswa (64,5%) sudah berada pada kategori “Sangat Paham”, menunjukkan sebagian besar siswa telah memiliki pemahaman dasar, namun masih terdapat kelompok yang membutuhkan pendampingan lebih lanjut.

Hasil post-test menunjukkan peningkatan pemahaman yang signifikan setelah penyampaian materi. Jumlah siswa pada kategori “Sangat Paham” meningkat menjadi 49 orang (79,0%), sementara kategori “Belum Paham” menurun menjadi 4 orang (6,5%). Berdasarkan perubahan skor, 23 siswa (37,1%) mengalami peningkatan pemahaman, sedangkan sebagian besar lainnya mempertahankan skor tinggi mereka. Temuan ini mengindikasikan bahwa metode sosialisasi yang disertai contoh dan demonstrasi langsung efektif dalam memperkuat literasi keamanan digital siswa.

Meskipun mayoritas siswa menunjukkan peningkatan atau mempertahankan pemahaman yang baik, terdapat 5 siswa (8,1%) yang mengalami penurunan skor. Penurunan ini dapat disebabkan oleh berbagai faktor seperti kurangnya konsentrasi saat mengerjakan post-test, kesalahan dalam memahami soal, atau kelelahan setelah mengikuti kegiatan selama 90 menit. Namun, penurunan ini masih dalam batas wajar dan tidak mengurangi kesimpulan bahwa kegiatan secara keseluruhan berhasil meningkatkan pemahaman siswa terhadap keamanan digital.

B. Pembahasan Materi dan Respons Peserta

Berdasarkan hasil pengamatan selama kegiatan, siswa terlihat sangat antusias ketika materi dikaitkan langsung dengan pengalaman digital yang mereka temui sehari-hari. Adapun beberapa topik yang paling menarik perhatian siswa adalah :

a. Phising dan Social Engineering

Siswa sangat tertarik dengan contoh-contoh nyata kasus phishing, terutama yang melibatkan undian palsu, pesan dari “admin” aplikasi, dan tautan berbahaya di media sosial. Banyak siswa yang mengakui pernah menerima pesan serupa namun tidak menyadari bahwa itu merupakan upaya penipuan. Diskusi mengenai berbagai modus yang sering menyasar pengguna remaja juga memicu banyak pertanyaan dari peserta, karena mereka merasa situasi tersebut sangat dekat dengan aktivitas digital mereka sehari-hari.

b. Aplikasi Modifikasi (MOD)

Topik mengenai bahaya aplikasi modifikasi mendapat respons kuat dari siswa. Beberapa siswa mengaku pernah atau bahkan masih menggunakan aplikasi MOD karena fitur premium gratis, namun tidak menyadari risiko malware dan pencurian data yang menyertainya.

c. Verifikasi Dua Langkah (2FA)

Demonstrasi penggunaan Google Account Manager untuk mengecek aktivitas akun dan aktivasi verifikasi dua langkah sangat membantu siswa memahami cara melindungi akun mereka secara praktis. Evaluasi menunjukkan bahwa verifikasi dua langkah merupakan metode autentikasi yang efektif dalam meningkatkan keamanan akun digital (Aripadono et al., 2024). Implementasi fitur keamanan seperti verifikasi dua langkah terbukti dapat secara signifikan mengurangi risiko akses tidak sah terhadap akun pengguna (Herdiantoro & Islami, 2023). Meskipun siswa tidak dapat mempraktikkan langsung karena kebijakan sekolah yang melarang penggunaan ponsel, mereka terlihat antusias mencatat langkah-langkahnya (Rahman, 2024).

C. Dampak Kegiatan

Kegiatan ini memberikan beberapa dampak positif bagi peserta dan lingkungan sekolah. Pemanfaatan teknologi informasi dalam edukasi literasi digital terbukti efektif untuk meningkatkan keamanan data dan mencegah kejahatan siber di kalangan masyarakat, khususnya siswa (Rahman, 2024). Dampak konkret yang teridentifikasi meliputi :

a. Peningkatan Kesadaran Keamanan Digital

Siswa menjadi lebih waspada terhadap ancaman digital yang mereka hadapi sehari-hari dan memahami pentingnya melindungi data pribadi. Edukasi digital safety terbukti efektif dalam meningkatkan kecakapan bermedia digital siswa (Herawati et al., 2024).

b. Perubahan Perilaku Digital

Beberapa siswa menyatakan komitmen untuk mengubah password mereka menjadi lebih kuat dan mengaktifkan verifikasi dua langkah setelah pulang ke rumah. Peningkatan literasi keamanan digital dan kesadaran akan perlindungan data pribadi merupakan hasil langsung dari kegiatan sosialisasi yang terstruktur (Syafuddin, 2023).

c. Dukungan dari Pihak Sekolah

Pihak sekolah menyambut baik kegiatan ini dan menyatakan keinginan untuk melaksanakan kegiatan serupa secara berkala sebagai bagian dari program literasi digital sekolah.

D. Kendala dan Solusi

Beberapa kendala yang dihadapi selama pelaksanaan, terutama terkait kondisi ruangan dan keterbatasan perangkat siswa dalam mengikuti demonstrasi secara langsung, turut memengaruhi efektivitas kegiatan pada beberapa bagian. Adapun beberapa kendala yang muncul selama kegiatan yaitu :

a. Keterbatasan Ruangan

Ruangan yang memanjang dan sempit menyebabkan siswa di bagian belakang kesulitan melihat materi presentasi. Hal ini diatasi dengan penyesuaian posisi duduk dan pengaturan ulang tata letak presentasi.

b. Keterbatasan Praktik Langsung

Kebijakan sekolah yang melarang penggunaan ponsel membuat siswa tidak dapat mempraktikkan langsung pengaturan keamanan akun. Solusi yang diterapkan adalah demonstrasi visual yang detail dan pemberian panduan tertulis yang dapat dipraktikkan di rumah.

c. Keterbatasan Waktu

Durasi kegiatan yang relatif singkat (90 menit) membuat beberapa topik tidak dapat dibahas secara mendalam. Untuk kegiatan selanjutnya, disarankan penambahan waktu atau pembagian materi dalam beberapa sesi.

E. Relevansi dengan Penelitian Terdahulu

Hasil kegiatan ini sejalan dengan penelitian mengenai sosialisasi keamanan, etika, dan literasi digital yang menunjukkan bahwa pendekatan interaktif efektif dalam meningkatkan pemahaman siswa terhadap ancaman siber dan praktik keamanan digital (Fachruddin et al., 2023). Kegiatan ini membuktikan bahwa pendekatan edukatif yang melibatkan demonstrasi praktis dan evaluasi terstruktur efektif dalam meningkatkan literasi keamanan digital siswa, khususnya di tingkat sekolah menengah pertama.

4. KESIMPULAN

Kegiatan sosialisasi dan edukasi keamanan digital di SMP Muhammadiyah 1 Samarinda telah berhasil meningkatkan pemahaman dan kesadaran siswa terhadap ancaman siber serta langkah-langkah perlindungan akun digital. Peningkatan pemahaman siswa terlihat jelas dari hasil perbandingan pre-test dan post-test, di mana siswa mampu mengidentifikasi ciri-ciri phishing, memahami pentingnya password kuat dan verifikasi dua langkah, serta

mengenali tanda-tanda situs berbahaya. Metode sosialisasi interaktif dengan demonstrasi langsung terbukti efektif dalam menyampaikan materi keamanan digital kepada siswa SMP.

Kegiatan ini memberikan dampak positif dalam membentuk perilaku berinternet yang lebih aman, bijak, dan bertanggung jawab di kalangan siswa. Untuk kegiatan selanjutnya, disarankan untuk menambah durasi kegiatan agar materi dapat dibahas lebih mendalam, menyediakan kesempatan praktik langsung bagi siswa, serta melaksanakan kegiatan serupa secara berkala untuk memperkuat literasi keamanan digital di lingkungan sekolah. Kerja sama antara perguruan tinggi dan sekolah dalam program edukasi keamanan digital perlu terus ditingkatkan untuk membentuk budaya keamanan digital yang kuat sejak dini.

5. PENGAKUAN/ UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada SMP Muhammadiyah 1 Samarinda yang telah memberikan kesempatan dan dukungan penuh dalam pelaksanaan kegiatan pengabdian kepada masyarakat ini. Ucapan terima kasih juga disampaikan kepada Bapak Salman Anshori F., S.Sy., M.H. selaku Kepala Sekolah SMP Muhammadiyah 1 Samarinda atas penerimaan dan fasilitasi yang diberikan sehingga kegiatan dapat berjalan dengan baik. Terima kasih juga kepada Ibu Vina Zahrotun Kamila, S.Kom., M.Kom. selaku dosen pendamping yang telah memberikan bimbingan dan arahan selama pelaksanaan kegiatan, serta kepada Bapak Putut Pamilih Widagdo, S.Kom., M.Kom. selaku Koordinator Program Studi Sistem Informasi Fakultas Teknik Universitas Mulawarman sebagai penanggung jawab kegiatan.

Sebagai bentuk apresiasi dan penghargaan, kegiatan diakhiri dengan penyerahan cinderamata kepada pihak sekolah serta pemberian bingkisan kepada siswa teraktif yang berpartisipasi dalam kegiatan ini. Momen tersebut mencerminkan antusiasme peserta dan terjalannya kerja sama yang baik antara tim pengabdian dan pihak sekolah.

6. DAFTAR PUSTAKA

- Ariasa, K. (2025, May 15). Panduan Terbaru Membuat Password yang Aman dan Mudah Diingat (Berdasarkan Standar NIST 2025). *Teknologi Informasi & Komunikasi UNDIKSHA*.
- Aripadono, H. W., Haeruddin, & Cantra, K. (2024). Evaluation of Two-Factor Authentication (2FA) TOTP in Higher Education Using Vulnerability Assessment and CIA Triad. *Jurnal E-Komtek (Elektro-Komputer-Teknik)*, 8(2), 245–254. <https://doi.org/10.37339/e-komtek.v8i2.2113>
- Fachruddin, Sutoyo, M. A. H., Riyadi, W., & Arvita, Y. (2023). Sosialisasi Keamanan, Etika, Dan Literasi Bagi Siswa/I Sma Negeri 4 Kota Jambi. *Jurnal Pengabdian Masyarakat UNAMA*, 2(2), 45–50. <https://doi.org/10.33998/jpmu.2023.2.2.1404>
- Herawati, E. S. B., Mustofa, Z., Sari, M. N., Mirsa, N. R. P., Widiyan, A. P., & Astuti, Y. (2024). Edukasi Digital Safety Dalam Meningkatkan Kecakapan Bermedia Digital Siswa. *Lamahu: Jurnal Pengabdian Masyarakat Terintegrasi*, 3(1), 47–54. <https://doi.org/10.37905/ljpmu.v3i1.24090>
- Herdiantoro, H. R., & Islami, M. R. R. (2023). Implementasi Two-Factor Authentication (2FA) Dan Firewall Policies Dalam Mengamankan Website. *Jurnal Mahasiswa Ilmu Komputer*, 4(1), 1–9.
- Maisaroh, A. A., Sukriono, D., & Suhartono, E. (2025). Optimalisasi Literasi Digital dalam Materi Pertahanan dan Keamanan: Strategi Pendidikan Kontekstual di Sekolah. *Didaktika: Jurnal Kependidikan*, 14(2). <https://jurnaldidaktika.org>
- Marikyan, D., & Papagiannidis, S. (2025). *Protection Motivation Theory: A Review*. TheoryHub Book: Protection Motivation Theory. <https://open.ncl.ac.uk>
- Rahman, Z. A. (2024). Pemanfaatan Teknologi Informasi dalam Edukasi Literasi Digital untuk Peningkatan Keamanan Data dan Pencegahan Kejahatan Siber di Masyarakat Rawang Panca Arga. *Merkurius : Jurnal Riset Sistem Informasi Dan Teknik Informatika*, 2(6), 82–90. <https://doi.org/10.61132/mercurius.v2i6.399>
- Sanjaya, S., Fitriani, L. R., Hakim, M. A., Yasin, M. Y., & Maesaroh, S. S. (2024). Analisis Literasi Keamanan Digital Bagi Mahasiswa Universitas Pendidikan Indonesia Kampus Tasikmalaya: Tingkat Pengetahuan, Kepercayaan, dan Kewaspadaan. *INNOVATIVE: Journal Of Social Science Research*, 4, 8205–8216.
- Saputra, D. F. (2023). Literasi Digital Untuk Perlindungan Data Pribadi. *Jurnal Ilmu Kepolisian*, 17(3).
- Sari, A. P. (2025). Penerapan Autentikasi Dua Faktor (2FA) untuk Melindungi Data Pribadi pada Layanan Media Sosial. *ISSN: JURNAL STARDIA*, 1(1), 60–65. <https://journal.uici.ac.id>
- Sugiarto, E. C. (2025, July 7). *Ketahanan Informasi dan Literasi Digital di Era Cognitive Warfare*. Kementerian Sekretariat Negara Republik Indonesia.
- Syafuddin, K. (2023). Peningkatan Literasi Keamanan Digital Dan Perlindungan Data Pribadi Bagi Siswa Di Smpn 154 Jakarta. *Eastasouth Journal of Impactive Community Services*, 1(03), 122–133. <https://doi.org/10.58812/ejims.v1.i03>
- Syakh Alam, H., Agung Gede Adi Mega Putra, A., Agung Gede Bagus Abi Wiguna, A., Gede Ade Hendra Juniantara Putra, I., & Komang Swastika Adnyana, I. (2025). Peningkatan Literasi Dan Keamanan Digital Siswa SMP Negeri 3 Bangli Melalui Pelatihan Interaktif. *JOONG-KI: Jurnal Pengabdian Masyarakat*, 4(4).
- Yeyendra, Y., Hajar, I., Darmanto, D., & Junaidi, E. (2024). Profil Keterampilan Literasi Digital Siswa SMA di Era Teknologi Digital. *BIOLOGY AND EDUCATION JOURNAL*, 4, 111–119.

Yusuf Effendy, M., & Oktiani, H. (2024). Literasi Digital Keamanan Siber Pada Remaja Menghadapi Social Engineering. *Jurnal Wacana Publik*, 18(01), 35–42. <https://doi.org/10.37295/wp.v18i8.67>