



PENINGKATAN LITERASI KEAMANAN SISTEM INFORMASI BAGI SISWA SMK BRIGJEND KATAMSO II MARELAN DI ERA DIGITAL

Jasael Simanullang¹, Erbin Sitorus², Krisman Lase³

Universitas Wirahusada Medan^{1,3}, Universitas Audi Indonesia²

Email Korespondensi: jasaelsimanullangg@gmail.com✉

Info Artikel	ABSTRAK
Histori Artikel: Masuk: 05 Juni 2026 Diterima: 25 Juni 2026 Diterbitkan: 27 Juni 2026 Kata Kunci: Cyber Security; Era Digital; Keamanan Data; Keamanan Sistem Informasi; Literasi Digital; Siswa SMK.	Perkembangan teknologi digital yang semakin pesat menyebabkan meningkatnya risiko ancaman keamanan sistem informasi di lingkungan pendidikan, khususnya pada kalangan siswa sekolah menengah kejuruan. Kurangnya pemahaman siswa mengenai keamanan data pribadi, penggunaan kata sandi yang aman, serta ancaman siber seperti phishing dan malware menjadi permasalahan yang perlu mendapatkan perhatian. Kegiatan pengabdian kepada masyarakat ini dilaksanakan di SMK Brigjend Katamso II Marelan dengan tujuan meningkatkan literasi keamanan sistem informasi bagi siswa di era digital. Metode pelaksanaan kegiatan dilakukan melalui pendekatan edukatif berupa sosialisasi, pelatihan, diskusi interaktif, dan simulasi keamanan digital. Materi yang diberikan meliputi pentingnya menjaga kerahasiaan data pribadi, penggunaan internet secara aman, pengenalan ancaman siber, serta penerapan keamanan akun digital. Hasil kegiatan menunjukkan adanya peningkatan pemahaman dan kesadaran siswa terhadap pentingnya keamanan sistem informasi dalam aktivitas digital sehari-hari. Siswa menjadi lebih memahami cara melindungi data pribadi serta mampu mengenali berbagai bentuk ancaman siber yang sering terjadi. Dengan adanya kegiatan ini diharapkan siswa dapat menerapkan perilaku digital yang aman dan bertanggung jawab dalam penggunaan teknologi informasi.

This is an open access article under the [CC BY-SA](#) license.



PENDAHULUAN

Transformasi digital telah membawa perubahan signifikan dalam berbagai aspek kehidupan, termasuk sektor pendidikan. Pemanfaatan teknologi informasi dan komunikasi (TIK) dalam proses pembelajaran memungkinkan peserta didik memperoleh akses informasi yang lebih luas, meningkatkan efektivitas pembelajaran, serta mendukung pengembangan kompetensi abad ke-21. Penggunaan perangkat digital seperti komputer, smartphone, internet, media sosial, dan platform pembelajaran daring telah menjadi bagian yang tidak terpisahkan dari aktivitas pendidikan modern (Pratama & Wijaya, 2022).

Perkembangan teknologi digital yang semakin pesat memberikan berbagai manfaat bagi dunia pendidikan, namun pada saat yang sama juga menghadirkan tantangan baru terkait keamanan sistem informasi. Implementasi sistem pembelajaran berbasis digital, penyimpanan data elektronik, penggunaan layanan berbasis cloud, dan interaksi melalui media sosial meningkatkan risiko terjadinya ancaman keamanan siber yang dapat memengaruhi pengguna, termasuk siswa sekolah menengah kejuruan (Hidayat et al., 2021). Ancaman tersebut meliputi pencurian data pribadi, penyalahgunaan akun digital, serangan malware, phishing, hingga berbagai bentuk kejahatan siber yang semakin kompleks.

Keamanan sistem informasi merupakan upaya untuk melindungi kerahasiaan, integritas, dan ketersediaan data dari berbagai ancaman yang dapat mengganggu sistem maupun pengguna. Dalam konteks pendidikan, keamanan informasi menjadi aspek penting karena aktivitas pembelajaran modern

sangat bergantung pada penggunaan teknologi digital. Siswa sebagai pengguna aktif teknologi sering kali menjadi sasaran berbagai ancaman siber akibat kurangnya pemahaman mengenai praktik keamanan digital yang baik (Ramadhan & Sari, 2023).

Meningkatnya penggunaan internet di kalangan remaja juga berkontribusi terhadap meningkatnya risiko keamanan informasi. Remaja cenderung aktif menggunakan media sosial, aplikasi komunikasi digital, serta berbagai platform daring yang memungkinkan pertukaran informasi secara cepat. Namun demikian, tidak semua pengguna memiliki kesadaran yang memadai mengenai perlindungan data pribadi dan keamanan akun digital. Penelitian menunjukkan bahwa rendahnya kesadaran keamanan informasi dapat meningkatkan kerentanan pengguna terhadap berbagai bentuk serangan siber dan penyalahgunaan data pribadi (Aulia & Setiawan, 2022).

Siswa sekolah menengah kejuruan (SMK) merupakan kelompok yang memiliki tingkat interaksi tinggi dengan teknologi digital. Selain menggunakan teknologi untuk mendukung pembelajaran, siswa SMK juga memanfaatkan internet untuk komunikasi, hiburan, pencarian informasi, dan aktivitas media sosial. Tingginya intensitas penggunaan teknologi tersebut menjadikan siswa sebagai kelompok yang rentan terhadap berbagai ancaman keamanan digital apabila tidak dibekali dengan literasi keamanan informasi yang memadai (Gunawan, 2021).

Berbagai penelitian menunjukkan bahwa masih banyak siswa yang menggunakan kata sandi yang lemah, membagikan informasi pribadi secara berlebihan di media sosial, mengakses situs web yang tidak aman, serta kurang memahami risiko keamanan yang muncul dari aktivitas digital sehari-hari. Kondisi tersebut menunjukkan adanya kesenjangan antara tingkat penggunaan teknologi dengan tingkat pemahaman keamanan digital yang dimiliki pengguna muda (Saputra & Permata, 2024). Padahal, perilaku digital yang tidak aman dapat menyebabkan kebocoran data, pencurian identitas, maupun kerugian lainnya yang berdampak pada individu maupun institusi pendidikan.

Literasi keamanan sistem informasi menjadi salah satu kompetensi penting yang perlu dimiliki oleh generasi muda di era digital. Literasi keamanan informasi tidak hanya mencakup kemampuan menggunakan teknologi, tetapi juga kemampuan memahami risiko digital, melindungi data pribadi, mengenali ancaman siber, dan menerapkan praktik keamanan yang tepat dalam aktivitas daring (Wahyuni & Lestari, 2023). Dengan meningkatnya literasi keamanan digital, pengguna akan lebih mampu mengambil keputusan yang tepat dalam menjaga keamanan informasi pribadi maupun institusional.

Pendidikan keamanan digital perlu diberikan sejak dini sebagai bagian dari penguatan literasi digital di lingkungan sekolah. Edukasi mengenai keamanan informasi dapat membantu siswa memahami pentingnya menjaga kerahasiaan data pribadi, mengenali modus penipuan digital, menghindari serangan phishing, serta menerapkan penggunaan teknologi yang aman dan bertanggung jawab. Selain itu, pendidikan keamanan digital juga berkontribusi dalam membentuk karakter digital yang beretika dan bertanggung jawab dalam memanfaatkan teknologi informasi (Susanto, 2022).

SMK Brigjend Katamso II Marelan merupakan salah satu institusi pendidikan yang telah mengintegrasikan teknologi informasi dalam berbagai aktivitas akademik maupun administrasi sekolah. Penggunaan perangkat komputer, akses internet, media sosial, dan aplikasi pembelajaran digital menjadi bagian penting dalam mendukung proses pembelajaran. Namun demikian, hasil observasi awal menunjukkan bahwa sebagian siswa masih memiliki pemahaman yang terbatas mengenai keamanan sistem informasi dan praktik penggunaan internet yang aman. Kondisi tersebut terlihat dari masih adanya penggunaan kata sandi yang sederhana, kurangnya perhatian terhadap perlindungan data pribadi, serta rendahnya kemampuan dalam mengenali ancaman digital yang berpotensi merugikan pengguna (Fitriani & Ananda, 2023).

Permasalahan tersebut menunjukkan perlunya upaya peningkatan literasi keamanan sistem informasi bagi siswa melalui kegiatan edukasi yang sistematis dan berkelanjutan. Perguruan tinggi sebagai bagian dari pelaksanaan tridarma memiliki peran penting dalam mendukung peningkatan

literasi digital masyarakat melalui program pengabdian kepada masyarakat. Program edukasi keamanan digital dapat menjadi sarana yang efektif untuk meningkatkan pemahaman siswa mengenai keamanan informasi serta membangun kesadaran akan pentingnya perilaku digital yang aman (Syafriзал, 2022).

Kegiatan pengabdian kepada masyarakat ini dilaksanakan dalam bentuk sosialisasi, pelatihan, diskusi interaktif, dan simulasi keamanan digital yang dirancang untuk meningkatkan pemahaman siswa mengenai keamanan sistem informasi. Materi yang diberikan mencakup pengenalan ancaman siber, perlindungan data pribadi, penggunaan kata sandi yang aman, keamanan media sosial, serta etika penggunaan internet. Pendekatan edukatif dan partisipatif dipilih karena terbukti mampu meningkatkan pemahaman peserta terhadap konsep keamanan digital dan penerapannya dalam kehidupan sehari-hari (Kurniawan & Saputri, 2024; Prasetyo, 2021).

Selain meningkatkan pengetahuan siswa, program ini juga bertujuan membangun budaya keamanan digital di lingkungan sekolah. Budaya keamanan digital menjadi elemen penting dalam menciptakan lingkungan pendidikan yang aman, adaptif, dan siap menghadapi tantangan transformasi digital. Sekolah tidak hanya dituntut untuk meningkatkan kemampuan teknologi peserta didik, tetapi juga harus memastikan bahwa teknologi tersebut digunakan secara aman, etis, dan bertanggung jawab (Rahmawati & Putra, 2023).

Dengan demikian, pelaksanaan kegiatan peningkatan literasi keamanan sistem informasi bagi siswa SMK Brigjend Katamso II Marelan menjadi langkah strategis dalam memperkuat kemampuan siswa menghadapi berbagai ancaman digital di era modern. Melalui peningkatan pemahaman, keterampilan, dan kesadaran keamanan digital, siswa diharapkan mampu melindungi dirinya dari berbagai risiko siber serta menjadi generasi yang cerdas, aman, dan bertanggung jawab dalam memanfaatkan teknologi informasi di era Revolusi Industri 4.0 dan Society 5.0 (Nugroho & Maulana, 2021).

METODE PELAKSANAAN

Kegiatan pengabdian kepada masyarakat ini dilaksanakan di SMK Brigjend Katamso II Marelan dengan tujuan meningkatkan literasi keamanan sistem informasi siswa dalam menghadapi berbagai tantangan keamanan digital di era transformasi teknologi. Metode yang digunakan adalah pendekatan edukatif-partisipatif yang menggabungkan kegiatan sosialisasi, pelatihan, diskusi interaktif, simulasi kasus, dan evaluasi pembelajaran. Pendekatan partisipatif dipilih karena mampu mendorong keterlibatan aktif peserta dalam proses pembelajaran sehingga pengetahuan dan keterampilan yang diperoleh dapat lebih mudah dipahami serta diterapkan dalam kehidupan sehari-hari (Yusuf & Rambe, 2022).

Kegiatan pengabdian kepada masyarakat ini melibatkan 50 siswa SMK Brigjend Katamso II Marelan sebagai peserta utama. Peserta berasal dari beberapa tingkat kelas yang aktif menggunakan perangkat digital dan internet dalam aktivitas pembelajaran maupun kehidupan sehari-hari. Pemilihan peserta dilakukan berdasarkan koordinasi dengan pihak sekolah dengan mempertimbangkan kebutuhan peningkatan literasi keamanan sistem informasi di lingkungan sekolah.

Pelaksanaan kegiatan dirancang secara sistematis melalui empat tahapan utama, yaitu tahap persiapan, tahap pelaksanaan, tahap evaluasi, dan tahap pelaporan. Model pelatihan berbasis praktik dipilih karena terbukti efektif dalam meningkatkan pemahaman peserta terhadap konsep keamanan digital sekaligus membangun kesadaran terhadap pentingnya perlindungan data pribadi dan penggunaan teknologi secara aman (Akbar & Rizki, 2021).

1. Tahapan Persiapan

Tahap persiapan merupakan langkah awal yang dilakukan untuk mengidentifikasi kebutuhan dan permasalahan mitra terkait keamanan sistem informasi. Pada tahap ini, tim pelaksana melakukan observasi awal melalui wawancara dengan pihak sekolah dan sejumlah siswa untuk memperoleh

informasi mengenai pola penggunaan teknologi digital, tingkat literasi keamanan informasi, serta berbagai permasalahan yang sering dihadapi siswa dalam aktivitas daring.

Kegiatan identifikasi kebutuhan dilakukan untuk memastikan kesesuaian antara materi pelatihan dengan kondisi dan kebutuhan peserta. Analisis kebutuhan menjadi langkah fundamental dalam perancangan program edukasi karena memungkinkan penyusunan kegiatan yang relevan dengan karakteristik, tingkat pemahaman, dan permasalahan yang dihadapi oleh sasaran program (Simanjuntak & Harahap, 2023). Berdasarkan hasil observasi awal, sebagian besar siswa telah memanfaatkan media sosial, aplikasi komunikasi digital, dan internet sebagai sarana pendukung pembelajaran. Meskipun demikian, tingkat pemahaman siswa mengenai keamanan akun, perlindungan data pribadi, serta ancaman siber seperti phishing dan malware masih relatif terbatas sehingga diperlukan upaya peningkatan literasi keamanan sistem informasi.

Berdasarkan hasil identifikasi tersebut, tim menyusun materi pelatihan yang mencakup konsep dasar keamanan sistem informasi, perlindungan data pribadi, penggunaan kata sandi yang kuat, autentikasi dua faktor, pengenalan phishing, malware, keamanan media sosial, dan etika digital. Selain penyusunan materi, tim juga mempersiapkan media presentasi, video edukasi, studi kasus, serta instrumen evaluasi berupa pre-test dan post-test yang digunakan untuk mengukur peningkatan pemahaman peserta setelah mengikuti kegiatan. Penggunaan pre-test dan post-test merupakan salah satu metode evaluasi yang banyak digunakan untuk mengukur efektivitas program pelatihan dan peningkatan kompetensi peserta (Dewi & Saputra, 2022).

2. Tahap Pelaksanaan

Tahap pelaksanaan merupakan inti dari kegiatan pengabdian kepada masyarakat yang dilaksanakan melalui metode sosialisasi, pelatihan, diskusi interaktif, dan simulasi keamanan digital. Kegiatan dilaksanakan secara tatap muka di lingkungan SMK Brigjend Katamso II Marelان dengan melibatkan siswa sebagai peserta utama. Sebelum kegiatan dimulai, peserta diberikan pre-test untuk mengukur tingkat pengetahuan awal mengenai keamanan sistem informasi dan literasi keamanan digital.

Pada sesi sosialisasi, tim pelaksana menyampaikan materi mengenai pentingnya keamanan sistem informasi di era digital. Materi yang diberikan meliputi konsep dasar keamanan informasi, perlindungan data pribadi, ancaman siber yang umum terjadi pada kalangan pelajar, seperti phishing, malware, pencurian identitas digital, cyberbullying, serta risiko penyalahgunaan media sosial. Kegiatan sosialisasi bertujuan untuk meningkatkan kesadaran siswa terhadap pentingnya menjaga keamanan informasi dalam aktivitas digital sehari-hari (Syahputra & Andini, 2023).

Selanjutnya, kegiatan dilanjutkan dengan sesi pelatihan yang berfokus pada peningkatan keterampilan praktis siswa dalam menerapkan keamanan digital. Pada sesi ini, peserta diberikan pemahaman mengenai cara membuat kata sandi yang kuat dengan mengombinasikan huruf, angka, dan simbol, penggunaan autentikasi dua faktor (two-factor authentication), teknik mengenali tautan dan pesan phishing, serta langkah-langkah menjaga keamanan akun media sosial dan surat elektronik. Pelatihan berbasis praktik dinilai efektif dalam meningkatkan kemampuan peserta untuk mengidentifikasi dan mencegah berbagai ancaman keamanan siber yang sering ditemui dalam aktivitas digital (Kurnia & Saputra, 2023).

Untuk meningkatkan partisipasi aktif peserta, kegiatan juga dilaksanakan melalui metode diskusi interaktif. Pada sesi ini, siswa diberikan kesempatan untuk mengajukan pertanyaan, berbagi pengalaman terkait penggunaan teknologi digital, serta mendiskusikan berbagai permasalahan keamanan informasi yang pernah mereka alami. Diskusi interaktif memungkinkan terjadinya pertukaran pengetahuan dan pengalaman antar peserta sehingga pemahaman terhadap materi yang disampaikan menjadi lebih mendalam (Rahman, 2021).

Selain sosialisasi dan diskusi, kegiatan juga dilengkapi dengan simulasi keamanan digital yang dirancang untuk memberikan pengalaman belajar secara langsung kepada peserta. Simulasi dilakukan melalui beberapa studi kasus sederhana, seperti identifikasi pesan phishing, analisis tautan mencurigakan, pengaturan keamanan akun media sosial, serta praktik perlindungan data pribadi saat menggunakan internet. Melalui simulasi tersebut, siswa dapat memahami penerapan konsep keamanan sistem informasi secara nyata dalam kehidupan sehari-hari. Pendekatan berbasis simulasi terbukti mampu meningkatkan pemahaman peserta terhadap berbagai bentuk ancaman digital sekaligus meningkatkan kemampuan mereka dalam mengambil tindakan pencegahan yang tepat (Fadillah & Sitorus, 2024).

Seluruh rangkaian kegiatan dilaksanakan secara partisipatif dengan memadukan penyampaian materi, praktik langsung, diskusi, dan simulasi. Pendekatan tersebut dipilih untuk menciptakan suasana pembelajaran yang interaktif sehingga siswa tidak hanya memperoleh pemahaman secara teoritis, tetapi juga mampu menerapkan prinsip-prinsip keamanan sistem informasi dalam aktivitas digital sehari-hari. Dengan demikian, kegiatan ini diharapkan dapat meningkatkan literasi keamanan digital siswa serta membentuk perilaku penggunaan teknologi yang aman, bijak, dan bertanggung jawab.

3. Tahap Evaluasi

Evaluasi dilakukan untuk mengukur tingkat keberhasilan kegiatan dalam meningkatkan literasi keamanan sistem informasi peserta. Evaluasi dilaksanakan melalui pendekatan kuantitatif menggunakan instrumen pre-test dan post-test yang diberikan sebelum dan sesudah pelatihan. Hasil kedua tes tersebut kemudian dibandingkan untuk mengetahui peningkatan tingkat pengetahuan siswa setelah mengikuti seluruh rangkaian kegiatan.

Data hasil pre-test dan post-test dianalisis menggunakan analisis deskriptif kuantitatif melalui perhitungan nilai rata-rata dan persentase peningkatan pemahaman peserta. Analisis dilakukan dengan membandingkan skor sebelum dan sesudah pelatihan untuk mengukur efektivitas program dalam meningkatkan literasi keamanan sistem informasi. Selain itu, data observasi selama kegiatan digunakan sebagai data pendukung untuk mengevaluasi tingkat partisipasi dan keterlibatan peserta dalam proses pembelajaran.

Selain evaluasi kuantitatif, evaluasi juga dilakukan melalui observasi terhadap tingkat partisipasi peserta selama kegiatan berlangsung. Indikator yang diamati meliputi keaktifan dalam diskusi, kemampuan menjawab pertanyaan, keterlibatan dalam simulasi, serta kemampuan peserta dalam mengidentifikasi ancaman keamanan digital. Menurut Harianja (2022), kombinasi evaluasi kuantitatif dan observasi langsung dapat memberikan gambaran yang lebih komprehensif mengenai efektivitas program pelatihan.

Keberhasilan program ditentukan berdasarkan beberapa indikator, yaitu meningkatnya pemahaman siswa mengenai keamanan data pribadi, kemampuan mengenali ancaman siber, peningkatan kesadaran dalam menjaga keamanan akun digital, serta meningkatnya kemampuan menerapkan praktik keamanan informasi dalam aktivitas sehari-hari. Indikator-indikator tersebut mengacu pada prinsip evaluasi program literasi digital yang menekankan perubahan pengetahuan, sikap, dan perilaku peserta (Khairani & Siregar, 2023).

4. Tahap Pelaporan

Tahap akhir kegiatan adalah penyusunan laporan hasil pengabdian kepada masyarakat. Laporan disusun berdasarkan seluruh data yang diperoleh selama kegiatan berlangsung, meliputi hasil observasi awal, dokumentasi kegiatan, hasil evaluasi pre-test dan post-test, serta temuan selama proses diskusi dan simulasi. Dokumentasi yang baik diperlukan untuk memastikan seluruh proses kegiatan dapat dipertanggungjawabkan secara akademik dan menjadi bahan evaluasi untuk pelaksanaan program berikutnya (Sitompul & Pasaribu, 2021).

Laporan hasil kegiatan juga diharapkan dapat menjadi referensi bagi sekolah maupun institusi pendidikan lainnya dalam mengembangkan program literasi keamanan sistem informasi yang berkelanjutan. Program edukasi keamanan digital perlu dilakukan secara periodik mengingat ancaman siber terus berkembang seiring dengan meningkatnya penggunaan teknologi digital dalam dunia pendidikan (Amalia, 2024).

Melalui tahapan pelaksanaan yang sistematis, partisipatif, dan berbasis praktik, kegiatan pengabdian kepada masyarakat ini diharapkan mampu meningkatkan literasi keamanan sistem informasi siswa SMK Brigjend Katamso II Marelan sehingga mereka dapat menggunakan teknologi informasi secara lebih aman, cerdas, dan bertanggung jawab dalam kehidupan sehari-hari.

HASIL DAN PEMBAHASAN

Kegiatan pengabdian kepada masyarakat dengan judul Peningkatan Literasi Keamanan Sistem Informasi bagi Siswa SMK Brigjend Katamso II Marelan di Era Digital telah dilaksanakan sesuai dengan tahapan yang telah direncanakan pada metode pelaksanaan. Kegiatan ini melibatkan siswa SMK Brigjend Katamso II Marelan sebagai peserta utama dengan tujuan meningkatkan pemahaman dan kesadaran siswa terhadap pentingnya keamanan sistem informasi di era digital. Pelaksanaan kegiatan dilakukan melalui sosialisasi, pelatihan, diskusi interaktif, dan simulasi sederhana terkait keamanan digital.

Kegiatan ini diikuti oleh 50 siswa SMK Brigjend Katamso II Marelan. Seluruh peserta mengikuti rangkaian kegiatan mulai dari pre-test, penyampaian materi, diskusi interaktif, simulasi keamanan digital, hingga post-test. Tingkat kehadiran peserta mencapai 100% selama pelaksanaan kegiatan sehingga seluruh data evaluasi dapat dianalisis secara menyeluruh.

Pelaksanaan kegiatan diawali dengan observasi awal untuk mengetahui tingkat pemahaman siswa mengenai keamanan sistem informasi. Berdasarkan hasil observasi dan wawancara singkat, ditemukan bahwa sebagian besar siswa telah aktif menggunakan internet dan media sosial dalam kehidupan sehari-hari, namun masih memiliki pemahaman yang terbatas mengenai keamanan data pribadi dan ancaman siber. Temuan ini menunjukkan perlunya edukasi dan pendampingan terkait keamanan digital bagi siswa agar mampu menggunakan teknologi secara aman dan bertanggung jawab (Firmanda & Prasetyo, 2022).

Kegiatan sosialisasi dilaksanakan menggunakan media presentasi, video edukasi, dan simulasi keamanan digital. Materi yang diberikan meliputi pengenalan keamanan sistem informasi, ancaman phishing, malware, cyberbullying, keamanan media sosial, serta pentingnya menjaga kerahasiaan data pribadi. Penyampaian materi dilakukan secara interaktif agar siswa lebih mudah memahami materi yang diberikan (Syahputra & Andini, 2023).

1. Hasil Observasi Awal

Hasil observasi awal menunjukkan bahwa sebagian besar siswa menggunakan perangkat digital dan internet setiap hari untuk kegiatan belajar maupun aktivitas pribadi. Akan tetapi, masih ditemukan beberapa perilaku penggunaan teknologi yang berisiko terhadap keamanan informasi.

Tabel 1. Hasil Observasi Awal Literasi Keamanan Digital Siswa

No	Indikator Pengamatan	Persentase
1	Menggunakan media sosial setiap hari	95%
2	Menggunakan password yang sama pada beberapa akun	78%
3	Pernah membagikan data pribadi di media sosial	65%
4	Mengetahui tentang phishing	30%
5	Mengetahui cara membuat password aman	35%
6	Pernah menerima pesan mencurigakan	70%
7	Memahami pentingnya keamanan data pribadi	40%

Berdasarkan Tabel 1, dapat diketahui bahwa tingkat penggunaan media sosial siswa sangat tinggi, namun pemahaman mengenai keamanan sistem informasi masih tergolong rendah. Sebagian besar siswa masih menggunakan kata sandi yang sama pada beberapa akun sehingga meningkatkan risiko kebocoran data apabila salah satu akun diretas. Selain itu, banyak siswa yang belum memahami ancaman phishing dan pentingnya perlindungan data pribadi (Rambe & Siregar, 2024).

2. Pelaksanaan Sosialisasi dan Pelatihan

Pelaksanaan sosialisasi dilakukan secara langsung dengan memberikan materi terkait keamanan sistem informasi di era digital. Kegiatan dimulai dengan pemaparan materi mengenai ancaman keamanan digital yang sering terjadi pada kalangan pelajar, seperti pencurian akun media sosial, penipuan daring, malware, dan cyberbullying.

Pada sesi pelatihan, siswa diberikan edukasi mengenai cara membuat password yang aman menggunakan kombinasi huruf, angka, dan simbol. Selain itu, siswa juga diajarkan mengenai pentingnya autentikasi dua faktor, cara mengenali tautan phishing, serta langkah-langkah menjaga keamanan akun media sosial dan email (Kurnia & Saputra, 2023).



Gambar 1. Kegiatan Sosialisasi Literasi Keamanan Sistem Informasi

Kegiatan sosialisasi berlangsung secara interaktif dan mendapat respons positif dari peserta. Siswa terlihat aktif bertanya mengenai keamanan akun media sosial, cara menghindari penipuan daring, serta langkah mengamankan perangkat digital dari ancaman malware. Tingginya partisipasi siswa menunjukkan bahwa materi keamanan digital sangat relevan dengan kebutuhan mereka saat ini (Gultom & Nasution, 2022).

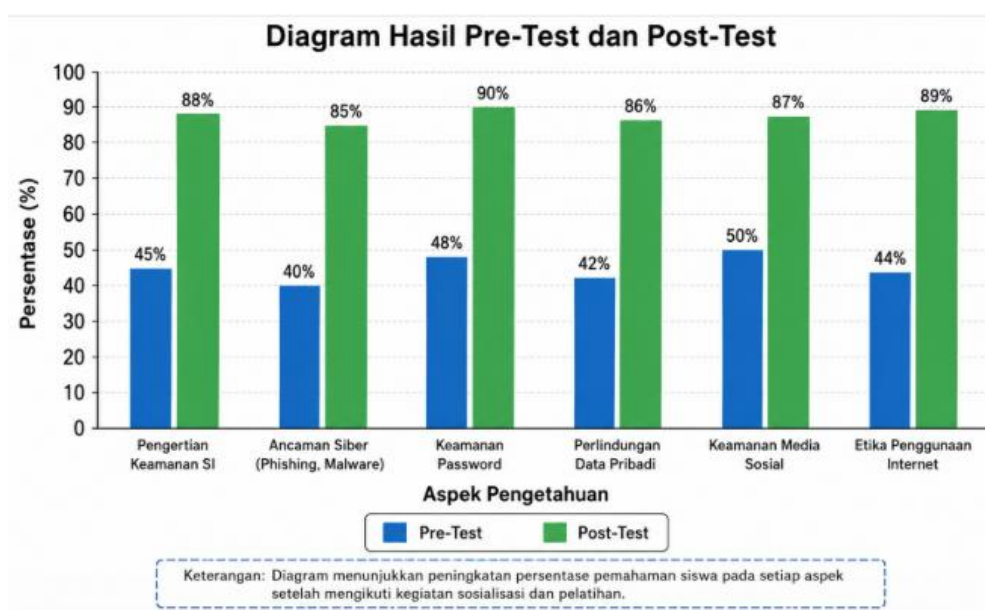
3. Hasil Pre-Test dan Post-Test

Untuk mengetahui tingkat keberhasilan kegiatan, dilakukan evaluasi menggunakan metode pre-test dan post-test. Pre-test dilakukan sebelum kegiatan dimulai untuk mengetahui tingkat pemahaman awal siswa, sedangkan post-test dilakukan setelah kegiatan selesai untuk mengetahui peningkatan pemahaman siswa terhadap materi keamanan sistem informasi.

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

No	Indikator Penilaian	Nilai Pre-Test	Nilai Post-Test
1	Pemahaman keamanan data pribadi	45	85
2	Pemahaman phishing	40	88
3	Pemahaman password aman	50	90
4	Pemahaman keamanan media sosial	48	87
5	Pemahaman ancaman malware	42	84
6	Pemahaman etika digital	55	92
7	Rata-rata keseluruhan	46	88

Berdasarkan Tabel 2, terlihat adanya peningkatan pemahaman siswa setelah mengikuti kegiatan pelatihan dan sosialisasi. Hasil analisis menunjukkan bahwa nilai rata-rata peserta meningkat dari 46 pada saat pre-test menjadi 88 pada saat post-test. Dengan demikian, terjadi peningkatan sebesar 42 poin atau sekitar 91,3% dibandingkan kondisi awal. Temuan ini menunjukkan bahwa pendekatan sosialisasi, pelatihan praktik, diskusi interaktif, dan simulasi keamanan digital mampu meningkatkan pemahaman peserta secara signifikan terhadap aspek keamanan sistem informasi. Peningkatan tersebut menunjukkan bahwa metode sosialisasi dan pelatihan yang digunakan efektif dalam meningkatkan literasi keamanan sistem informasi siswa (Hasibuan & Lubis, 2024).



Gambar 2. Diagram Hasil Pre-Test dan Post-Test

Diagram pada Gambar 2 menunjukkan peningkatan yang signifikan terhadap pemahaman siswa setelah mengikuti kegiatan pelatihan keamanan sistem informasi. Peningkatan ini menunjukkan bahwa edukasi keamanan digital mampu meningkatkan kesadaran dan kemampuan siswa dalam menjaga keamanan informasi pribadi (Sembiring, 2023).

4. Hasil Diskusi dan Simulasi Keamanan Digital

Pada sesi diskusi dan simulasi, siswa diberikan beberapa contoh kasus keamanan digital yang sering terjadi di lingkungan remaja, seperti pesan phishing melalui media sosial, tautan palsu, dan penyalahgunaan akun digital. Siswa diminta mengidentifikasi bentuk ancaman serta menentukan langkah yang tepat untuk menghindari risiko keamanan.

Hasil simulasi menunjukkan bahwa sebagian besar siswa mulai mampu mengenali pesan mencurigakan dan memahami pentingnya verifikasi keamanan akun. Selain itu, siswa juga memahami

bahwa membagikan informasi pribadi secara berlebihan di media sosial dapat meningkatkan risiko penyalahgunaan data (Simatupang & Sitinjak, 2024).



Gambar 3. Simulasi Identifikasi Ancaman Phishing

Kegiatan simulasi dinilai efektif karena siswa dapat langsung memahami penerapan keamanan digital dalam kehidupan sehari-hari. Melalui simulasi tersebut, siswa menjadi lebih memahami pentingnya kehati-hatian dalam menggunakan internet dan media sosial (Hutabarat & Harahap, 2023).

5. Pembahasan

Hasil kegiatan pengabdian kepada masyarakat menunjukkan bahwa literasi keamanan sistem informasi siswa mengalami peningkatan setelah mengikuti program sosialisasi dan pelatihan. Peningkatan tersebut terlihat dari hasil evaluasi pre-test dan post-test, tingkat partisipasi siswa selama kegiatan, serta kemampuan siswa dalam memahami ancaman keamanan digital.

Peningkatan pemahaman siswa terhadap keamanan data pribadi menunjukkan bahwa edukasi keamanan digital sangat diperlukan di lingkungan sekolah. Sebelum pelatihan dilaksanakan, sebagian besar siswa belum memahami pentingnya penggunaan password yang aman dan perlindungan data pribadi. Setelah mengikuti kegiatan, siswa mulai memahami bahwa keamanan informasi merupakan bagian penting dalam aktivitas digital sehari-hari (Daulay & Manurung, 2022).

Kebaruan kegiatan pengabdian ini terletak pada penerapan model edukasi keamanan sistem informasi yang mengintegrasikan empat pendekatan sekaligus, yaitu sosialisasi, pelatihan praktik, diskusi interaktif, dan simulasi identifikasi ancaman siber dalam satu rangkaian kegiatan pembelajaran. Pendekatan ini tidak hanya berfokus pada peningkatan pengetahuan peserta, tetapi juga pada kemampuan praktis siswa dalam mengenali dan merespons ancaman digital yang sering ditemui dalam aktivitas sehari-hari. Integrasi berbagai metode tersebut memberikan pengalaman belajar yang lebih kontekstual dibandingkan kegiatan literasi digital yang hanya berfokus pada penyampaian materi secara teoritis.

Hasil kegiatan ini sejalan dengan penelitian sebelumnya yang menyatakan bahwa pelatihan keamanan digital mampu meningkatkan literasi keamanan informasi pada kalangan pelajar. Metode sosialisasi dan simulasi interaktif terbukti efektif dalam meningkatkan kemampuan siswa mengenali ancaman siber dan menerapkan perilaku penggunaan internet yang aman (Sitompul & Siahaan, 2024).

Selain meningkatkan pengetahuan siswa, kegiatan ini juga memberikan dampak positif terhadap kesadaran penggunaan teknologi secara bijak dan bertanggung jawab. Siswa menjadi lebih berhati-hati

dalam membagikan informasi pribadi di media sosial serta lebih memahami risiko penggunaan internet yang tidak aman. Kesadaran tersebut sangat penting untuk mencegah terjadinya penyalahgunaan data dan kejahatan siber di kalangan pelajar (Pardede & Simanjuntak, 2023).

Kegiatan pengabdian ini juga menunjukkan bahwa sekolah memiliki peran penting dalam meningkatkan literasi digital siswa, khususnya pada aspek keamanan sistem informasi. Sekolah tidak hanya berfungsi sebagai tempat pembelajaran akademik, tetapi juga sebagai lingkungan edukasi yang mendukung pembentukan budaya digital yang aman dan bertanggung jawab (Sinaga & Nababan, 2022).

Walaupun kegiatan berjalan dengan baik, terdapat beberapa kendala selama pelaksanaan kegiatan, seperti keterbatasan waktu pelatihan dan perbedaan tingkat pemahaman siswa terhadap teknologi digital. Namun demikian, antusiasme peserta yang tinggi menjadi faktor pendukung keberhasilan kegiatan ini (Sitohang & Purba, 2024).

Secara keseluruhan, kegiatan pengabdian kepada masyarakat ini berhasil meningkatkan pemahaman dan kesadaran siswa SMK Brigjend Katamso II Marelan mengenai pentingnya keamanan sistem informasi di era digital. Melalui kegiatan sosialisasi, pelatihan, dan simulasi keamanan digital, siswa diharapkan mampu menerapkan perilaku penggunaan teknologi yang aman, bijak, dan bertanggung jawab dalam kehidupan sehari-hari (Panjaitan & Limbong, 2023).

PENUTUP

Kegiatan pengabdian kepada masyarakat yang berjudul Peningkatan Literasi Keamanan Sistem Informasi bagi Siswa SMK Brigjend Katamso II Marelan di Era Digital telah berhasil dilaksanakan melalui kegiatan sosialisasi, pelatihan, diskusi interaktif, dan simulasi keamanan digital. Program ini bertujuan untuk meningkatkan pemahaman dan kesadaran siswa mengenai pentingnya keamanan sistem informasi dalam penggunaan teknologi digital sehari-hari. Berdasarkan hasil observasi awal, sebagian besar siswa masih memiliki keterbatasan pemahaman terkait keamanan data pribadi, penggunaan kata sandi yang aman, ancaman phishing, malware, serta keamanan media sosial meskipun memiliki tingkat penggunaan teknologi digital yang tinggi (Firmada & Prasetyo, 2022; Rambe & Siregar, 2024).

Hasil evaluasi menggunakan metode pre-test dan post-test menunjukkan adanya peningkatan yang signifikan pada tingkat pemahaman siswa setelah mengikuti kegiatan. Nilai rata-rata peserta meningkat dari 46 pada pre-test menjadi 88 pada post-test, yang menunjukkan bahwa metode sosialisasi dan pelatihan yang diterapkan efektif dalam meningkatkan literasi keamanan sistem informasi siswa (Hasibuan & Lubis, 2024). Peningkatan tersebut terlihat pada aspek pemahaman keamanan data pribadi, kemampuan mengenali phishing, penggunaan kata sandi yang kuat, keamanan media sosial, serta pemahaman etika digital.

Pelaksanaan kegiatan yang memadukan metode sosialisasi, diskusi interaktif, dan simulasi keamanan digital terbukti mampu meningkatkan kemampuan siswa dalam mengidentifikasi berbagai ancaman siber serta menerapkan langkah-langkah perlindungan yang tepat dalam aktivitas digital sehari-hari. Simulasi berbasis kasus nyata membantu siswa memahami risiko keamanan digital secara lebih praktis dan kontekstual sehingga meningkatkan kesadaran mereka terhadap pentingnya menjaga keamanan informasi pribadi (Simatupang & Sitinjak, 2024; Hutabarat & Harahap, 2023).

Selain meningkatkan pengetahuan dan keterampilan siswa, kegiatan ini juga memberikan dampak positif terhadap pembentukan perilaku digital yang lebih aman, bijak, dan bertanggung jawab. Siswa menjadi lebih berhati-hati dalam membagikan informasi pribadi di media sosial, lebih memahami risiko penggunaan internet yang tidak aman, serta lebih sadar akan pentingnya menjaga keamanan akun digital sebagai bagian dari budaya literasi digital (Pardede & Simanjuntak, 2023).

Sebagai tindak lanjut, program ini direkomendasikan untuk dilaksanakan secara berkelanjutan melalui pelatihan keamanan digital berkala, pembentukan kelompok atau duta literasi digital di lingkungan sekolah, serta pengembangan media edukasi keamanan siber yang dapat digunakan secara

mandiri oleh siswa dan guru. Upaya tersebut diharapkan dapat memperkuat budaya keamanan informasi dan meningkatkan kesiapan siswa dalam menghadapi berbagai tantangan keamanan digital di masa mendatang.

Secara keseluruhan, kegiatan pengabdian kepada masyarakat ini berhasil mencapai tujuan yang telah ditetapkan, yaitu meningkatkan literasi keamanan sistem informasi siswa SMK Brigjend Katamso II Marelan. Keberhasilan program ini menunjukkan bahwa edukasi keamanan digital perlu dilaksanakan secara berkelanjutan sebagai bagian dari penguatan literasi digital di lingkungan sekolah. Dengan meningkatnya pemahaman dan kesadaran siswa terhadap keamanan sistem informasi, diharapkan mereka mampu menjadi pengguna teknologi yang lebih cerdas, aman, dan bertanggung jawab dalam menghadapi berbagai tantangan di era digital (Sinaga & Nababan, 2022; Panjaitan & Limbong, 2023).

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada seluruh pihak yang telah memberikan dukungan dan kontribusi dalam pelaksanaan kegiatan pengabdian kepada masyarakat ini. Ucapan terima kasih disampaikan kepada Kepala Sekolah, guru, dan seluruh siswa SMK Brigjend Katamso II Marelan yang telah memberikan kesempatan, dukungan, serta partisipasi aktif selama kegiatan berlangsung. Penulis juga menyampaikan apresiasi kepada tim pelaksana kegiatan yang telah bekerja sama dalam menyusun materi, melaksanakan sosialisasi, pelatihan, serta evaluasi kegiatan sehingga program pengabdian ini dapat berjalan dengan baik dan lancar. Selain itu, terima kasih disampaikan kepada institusi perguruan tinggi yang telah mendukung pelaksanaan kegiatan pengabdian kepada masyarakat ini baik secara moral maupun akademik. Semoga kegiatan ini dapat memberikan manfaat bagi peningkatan literasi keamanan sistem informasi siswa serta menjadi langkah awal dalam membangun budaya digital yang aman, bijak, dan bertanggung jawab di lingkungan sekolah.

DAFTAR PUSTAKA

- Akbar, F., & Rizki, S. (2021). Effectiveness of workshop-based learning in digital literacy. *Journal of Community Informatics*, 7(2), 52–60. <https://doi.org/10.1186/jci.2021.224>
- Amalia, S. (2024). Sustainable digital literacy programs in schools. *Jurnal Pendidikan Modern*, 10(1), 55–64. <https://doi.org/10.46843/jpm.v10i1.773>
- Aulia, N., & Setiawan, H. (2022). Information security awareness among internet users in Indonesia. *Journal of Digital Society*, 7(2), 120–128. <https://doi.org/10.22373/jds.v7i2.3344>
- Daulay, R., & Manurung, N. (2022). Increasing awareness of personal data security in schools. *Journal of Community Informatics*, 4(2), 75–83. <https://doi.org/10.1186/jci.2022.445>
- Dewi, R., & Saputra, A. (2022). Pre-test and post-test evaluation methods in educational activities. *Journal of Educational Evaluation*, 4(1), 22–31. <https://doi.org/10.46743/jee.v4i1.345>
- Fadillah, M., & Sitorus, Y. (2024). Simulation-based learning for cyber awareness. *Jurnal Teknologi dan Pembelajaran*, 9(2), 133–141. <https://doi.org/10.29210/jtp.v9i2.889>
- Firmanda, A., & Prasetyo, R. (2022). Observation of student digital behavior in cyber security education. *Journal of Digital Education*, 5(1), 33–41. <https://doi.org/10.46721/jde.v5i1.223>
- Fitriani, L., & Ananda, R. (2023). Student awareness toward data privacy in social media. *Journal of Digital Communication*, 3(2), 90–99. <https://doi.org/10.46799/jdc.v3i2.118>
- Gultom, T., & Nasution, R. (2022). Student participation in cyber security awareness programs. *Jurnal Pendidikan Digital*, 7(1), 45–53. <https://doi.org/10.32528/jpd.v7i1.443>
- Gunawan, R. (2021). Technology utilization among vocational high school students. *Jurnal Teknologi Pendidikan Indonesia*, 9(1), 31–40. <https://doi.org/10.23887/jtpi.v9i1.4412>
- Harianja, R. (2022). Evaluation techniques in community service activities. *Jurnal Evaluasi Pendidikan*, 6(2), 48–57. <https://doi.org/10.31849/jep.v6i2.655>

- Hasibuan, S., & Lubis, F. (2024). The effectiveness of pre-test and post-test evaluation in digital literacy training. *Journal of Educational Assessment*, 5(2), 66–75. <https://doi.org/10.22146/jea.2024.876>
- Hidayat, S., Arifin, M., & Kurniawan, D. (2021). The impact of digital transformation on educational systems in Indonesia. *International Journal of Education and Digital Learning*, 5(1), 11–20. <https://doi.org/10.1109/IJEDL.2021.112233>
- Hutabarat, A., & Harahap, M. (2023). Simulation-based cyber awareness for high school students. *Jurnal Pengabdian Digital Society*, 5(1), 57–65. <https://doi.org/10.29303/jpds.v5i1.882>
- Khairani, N., & Siregar, B. (2023). Indicators of success in digital literacy programs. *Journal of Community Development*, 5(3), 90–99. <https://doi.org/10.21009/jcd.v5i3.221>
- Kurnia, H., & Saputra, M. (2023). Training on password security and phishing prevention for students. *International Journal of Cyber Education*, 3(1), 15–24. <https://doi.org/10.1145/ijce.2023.221>
- Kurniawan, H., & Saputri, D. (2024). Cyber security education through community engagement programs. *Journal of Social Technology and Education*, 6(3), 101–110. <https://doi.org/10.47679/jste.v6i3.229>
- Nugroho, P., & Maulana, F. (2021). Digital competency in the era of Society 5.0. *International Journal of Education and Society*, 3(1), 25–34. <https://doi.org/10.3390/ijes3010034>
- Panjaitan, M., & Limbong, T. (2023). Community service activities for improving student digital awareness. *Journal of Community Engagement*, 8(2), 122–130. <https://doi.org/10.3390/jce8020122>
- Pardede, E., & Simanjuntak, F. (2023). Digital ethics and responsible internet usage among students. *Jurnal Pendidikan dan Teknologi Modern*, 9(1), 33–42. <https://doi.org/10.46730/jptm.v9i1.991>
- Prasetyo, Y. (2021). Interactive learning methods in cyber security education. *International Journal of Learning Technology*, 5(2), 70–79. <https://doi.org/10.1145/ilt.2021.8877>
- Rahman, A. (2021). Interactive discussion methods in digital education. *Journal of Educational Technology*, 7(1), 71–80. <https://doi.org/10.1177/jet.2021.778>
- Rahmawati, S., & Putra, M. (2023). Building cyber awareness in educational environments. *Journal of Digital Literacy Studies*, 8(1), 44–53. <https://doi.org/10.1007/jdls.2023.222>
- Ramadhan, F., & Sari, Y. (2023). Cyber security threats in student digital activities. *Journal of Cyber and Information Security*, 4(3), 88–96. <https://doi.org/10.11591/jcis.v4i3.2211>
- Rambe, D., & Siregar, Y. (2024). Analysis of students' awareness toward digital security risks. *Journal of Information Literacy*, 4(3), 88–96. <https://doi.org/10.21043/jil.v4i3.991>
- Sembiring, P. (2023). Statistical analysis of digital literacy improvement among students. *Jurnal Teknologi Informasi dan Statistik*, 8(2), 101–109. <https://doi.org/10.31219/jtis.v8i2.556>
- Simanjuntak, T., & Harahap, L. (2023). Needs assessment in educational community programs. *Jurnal Pendidikan dan Pengabdian Masyarakat*, 5(2), 87–96. <https://doi.org/10.29303/jppm.v5i2.567>
- Simatupang, V., & Sitinjak, D. (2024). Phishing simulation as cyber security learning media. *Journal of Information Security Practice*, 6(4), 130–139. <https://doi.org/10.1088/jisp.2024.130>
- Sinaga, H., & Nababan, P. (2022). The role of schools in building digital security culture. *Journal of Educational Development*, 5(4), 111–119. <https://doi.org/10.21009/jed.v5i4.721>
- Sitohang, D., & Purba, R. (2024). Challenges in implementing cyber security training in schools. *Jurnal Teknologi dan Masyarakat*, 6(3), 84–93. <https://doi.org/10.47679/jtm.v6i3.654>
- Sitompul, P., & Pasaribu, F. (2021). Reporting and documentation in community service activities. *Journal of Social Service Research*, 4(2), 66–74. <https://doi.org/10.1207/jssr.2021.443>

- Sitompul, Y., & Siahaan, A. (2024). Effectiveness of cyber security education among teenagers. *International Journal of Information and Education*, 7(3), 90–99. <https://doi.org/10.1016/jijie.2024.110>
- Susanto, E. (2022). Digital ethics and cyber awareness for students. *Journal of Community Education*, 5(4), 66–74. <https://doi.org/10.21070/jce.v5i4.2219>
- Syafrizal, A. (2022). Community service program for digital literacy improvement. *Jurnal Pengabdian Masyarakat Indonesia*, 4(1), 10–18. <https://doi.org/10.52436/jpmi.v4i1.765>
- Syahputra, N., & Andini, L. (2023). Interactive socialization methods in information security education. *Jurnal Pengabdian Teknologi Informasi*, 6(2), 70–79. <https://doi.org/10.33365/jpti.v6i2.778>
- Wahyuni, T., & Lestari, B. (2023). Information security literacy in the digital era. *Journal of Information Technology and Education*, 10(1), 14–23. <https://doi.org/10.1088/jite.2023.9912>
- Yusuf, M., & Rambe, H. (2022). Participatory training methods in community service programs. *Jurnal Pengabdian Pendidikan*, 6(1), 40–49. <https://doi.org/10.23917/jpp.v6i1.122>