

Enhancing Students' Digital Security Awareness through Data Protection and Phishing Prevention Education in a Secondary Education Institution

Peningkatan Kesadaran Keamanan Digital Siswa melalui Edukasi Perlindungan Data dan Pencegahan Phishing di Lembaga Pendidikan Menengah

***Wahyu Hidayat, Syahid Nur Wahid, Asmaul Husnah Nasrullah.**

Universitas Negeri Makassar, Indonesia

ARTICLE INFO

Article History

Received: October 07, 2025

Revise: November 10, 2025

Accepted: November 26, 2025

Corresponding author:

Email: wahyu.hidayat@unm.ac.id

DOI: doi.org/10.61220/sipakatau

Copyright © 2025 The Authors



*This is an open access article under the
CC BY-SA license*

ABSTRACT

Cybersecurity threats such as personal data breaches and phishing attacks are increasing alongside the widespread adoption of digital technologies among adolescents. This community engagement program aims to enhance digital literacy and cybersecurity awareness among students in a secondary education institution through education on personal data protection and phishing prevention. The activities included awareness sessions, training workshops, phishing simulations, and guided mentoring, using a participatory approach involving lecturers, university students, teachers, and learners. Evaluation results indicate a substantial improvement in participants' understanding: over 75% of students were able to identify common phishing indicators, and 80% of teachers demonstrated an understanding of basic digital security principles. This initiative contributes to fostering a safer digital literacy culture and strengthening the technology-based learning ecosystem within secondary education.

Keywords: digital security, personal data protection, phishing, digital literacy

ABSTRAK

Ancaman keamanan siber seperti pencurian data pribadi dan phishing semakin meningkat seiring dengan meluasnya penggunaan teknologi digital di kalangan remaja. Program pengabdian ini bertujuan meningkatkan literasi digital dan kesadaran keamanan siber bagi siswa pada sebuah lembaga pendidikan menengah melalui edukasi perlindungan data pribadi dan pencegahan phishing. Kegiatan dilakukan melalui sosialisasi, pelatihan, simulasi phishing, serta pendampingan intensif dengan pendekatan partisipatif yang melibatkan dosen, mahasiswa, guru, dan siswa. Hasil evaluasi menunjukkan peningkatan signifikan pada pemahaman peserta: lebih dari 75% siswa mampu mengidentifikasi ciri umum phishing, dan 80% guru memahami prinsip dasar keamanan digital. Program ini berkontribusi dalam membangun budaya literasi digital yang aman dan mendukung penguatan ekosistem pembelajaran berbasis teknologi di lingkungan pendidikan menengah.

Kata kunci: keamanan digital, perlindungan data pribadi, phishing, literasi digital

1. PENDAHULUAN

Seiring pesatnya pertumbuhan teknologi digital dan penggunaan *internet* di kalangan remaja, khususnya siswa sekolah menengah atas, kesadaran akan pentingnya perlindungan data pribadi menjadi sebuah kebutuhan mendesak yang harus segera diatasi. Remaja usia sekolah saat ini sangat akrab dengan dunia digital, namun mereka belum sepenuhnya menyadari risiko keamanan digital yang mengancam, khususnya *phishing*. *Phishing* merupakan ancaman digital paling umum di kalangan siswa yang menyebabkan pencurian informasi pribadi seperti data pribadi, akun sosial media, bahkan data keuangan. Situasi ini diperparah dengan minimnya edukasi formal yang terintegrasi di sekolah terkait perlindungan data pribadi (1).

Kegiatan ini akan dilakukan di SMA yang terletak di kawasan urban dengan jumlah siswa sekitar 500 siswa dan tenaga pendidik sebanyak 35 orang. Lokasi sekolah yang strategis di perkotaan menunjukkan potensi besar untuk perkembangan literasi digital siswa. Namun, penguasaan teknologi informasi dan komunikasi (TIK) para

siswa ini belum diimbangi dengan pemahaman keamanan digital yang memadai. Siswa SMA memiliki kecenderungan tinggi terhadap perilaku digital yang berisiko seperti membuka tautan sembarangan dan berbagi data pribadi tanpa memahami risikonya (2).

Kondisi eksisting sekolah mitra menunjukkan bahwa siswa cenderung menggunakan perangkat digital secara intensif untuk pembelajaran daring dan komunikasi sehari-hari. Sebagian besar siswa menggunakan smartphone dan komputer pribadi tanpa perlindungan yang cukup. Pemahaman siswa terhadap ancaman phishing dan data pribadi relatif rendah. Akibatnya, siswa rentan menjadi korban pencurian identitas, eksploitasi informasi pribadi, dan kejahatan *cyber* lainnya (3).

Berdasarkan survei awal terhadap mitra, ditemukan bahwa 70% siswa kurang memahami bagaimana cara mengenali dan menghindari situs *phishing*. Kondisi ini diperparah oleh kurangnya sosialisasi dan edukasi dari pihak sekolah mengenai pentingnya perlindungan data pribadi (4,5). Kondisi ini diperparah dengan belum maksimalnya implementasi regulasi keamanan digital yang efektif di lingkungan pendidikan.

Tujuan utama kegiatan PKM ini adalah meningkatkan literasi dan kesadaran siswa terhadap pentingnya perlindungan data pribadi serta mengenali dan menghindari ancaman phishing.

Secara spesifik, kegiatan ini bertujuan untuk:

1. Memberikan edukasi tentang konsep dasar perlindungan data pribadi.
2. Mengenalkan berbagai bentuk ancaman phishing yang dapat terjadi di dunia digital.
3. Membekali siswa dengan keterampilan teknis dalam mengidentifikasi dan menghindari serangan *phishing*.
4. Memberdayakan sekolah melalui pelatihan guru sebagai fasilitator keamanan digital di lingkungan sekolah.

Kegiatan ini relevan dengan Indikator Kinerja Utama (IKU) Perguruan Tinggi yang berfokus pada peningkatan kualitas pendidikan melalui program pengabdian yang berdampak langsung pada masyarakat (6,7). Fokus kegiatan pengabdian ini adalah untuk mewujudkan komunitas sekolah yang tanggap terhadap ancaman keamanan digital melalui kegiatan yang terintegrasi, interaktif, dan praktis. Pelaksanaan kegiatan ini akan diselenggarakan dengan pendekatan partisipatif, melibatkan siswa dalam simulasi *phishing*, penyuluhan interaktif, dan pelatihan keterampilan praktis. Hasil akhir kegiatan diharapkan mampu membentuk generasi muda yang tidak hanya kompeten dalam penggunaan teknologi, namun juga kritis dan aman dalam menghadapi berbagai ancaman keamanan siber, terutama *phishing*.

Tingkat literasi digital kalangan siswa Sekolah Menengah Atas (SMA) masih tergolong rendah, khususnya terkait kesadaran terhadap pentingnya perlindungan data pribadi dan ancaman *phishing*. Situasi ini dipengaruhi oleh beberapa faktor dan dipecah dalam beberapa sub permasalahan antar lain, kurangnya kesadaran pentingnya perlindungan data pribadi serta rendahnya pemahaman tentang ancaman *phishing*.

Berdasarkan observasi awal dan studi pendukung, siswa SMA umumnya belum memahami secara mendalam pentingnya menjaga kerahasiaan data pribadi mereka di ruang digital. Sebagian besar siswa menggunakan smartphone dan komputer pribadi tanpa proteksi yang memadai, dengan sebanyak 60% siswa tidak memiliki pengaturan keamanan tambahan di akun-akun digital mereka (3). Sekolah belum memiliki kurikulum atau program khusus yang terintegrasi yang membahas tentang perlindungan data pribadi dan *cyber security* secara mendalam dan komprehensif. Penelitian Wijayanto (2024) menemukan bahwa kurang dari 20% sekolah memiliki modul khusus terkait perlindungan data pribadi (8).

Phishing masih menjadi ancaman dominan yang dialami oleh siswa, yang kerap kali berujung pada pencurian informasi pribadi atau bahkan perundungan daring. Studi Surbakti (2024) menunjukkan sekitar 65% siswa belum mampu mengidentifikasi tautan atau email yang bersifat *phishing* (1). Siswa SMA mayoritas menggunakan teknologi informasi untuk pendidikan dan interaksi sosial, tetapi tidak dibekali keterampilan teknis yang cukup untuk menangkal ancaman digital (9). Bukan hanya pada siswa, tetapi juga tenaga pendidik yang masih dinilai belum memiliki wawasan yang memadai tentang ancaman digital, sehingga kurang mampu memberikan pendampingan optimal terhadap siswa. Menurut penelitian Harahap et al. (2023), hanya sekitar 30% tenaga pengajar yang pernah mengikuti pelatihan keamanan digital (9).

Dengan mengatasi beberapa sub permasalahan ini, diharapkan tercipta lingkungan sekolah yang memiliki budaya sadar terhadap pentingnya perlindungan data pribadi dan keamanan digital. Hal ini akan berkontribusi positif dalam menciptakan ekosistem digital yang aman dan terjamin bagi seluruh komunitas sekolah. Untuk mengatasi permasalahan rendahnya tingkat literasi digital siswa terkait perlindungan data pribadi dan ancaman *phishing*, serangkaian solusi yang komprehensif dirancang agar mampu memberikan dampak yang signifikan bagi mitra sasaran. Solusi ini mencakup upaya edukasi, penguatan kapasitas tenaga pendidik, pengembangan kebijakan sekolah, serta implementasi teknologi yang mendukung ekosistem digital yang aman.

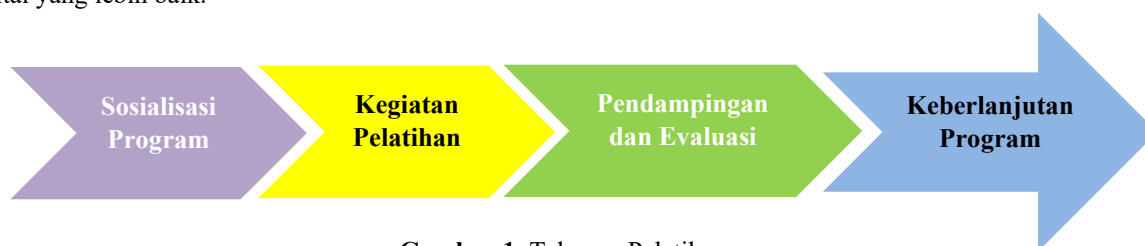
Langkah pertama dalam meningkatkan kesadaran siswa adalah melalui penyuluhan interaktif yang berfokus pada edukasi mengenai konsep dasar perlindungan data pribadi, potensi risiko kebocoran data, serta cara-cara praktis dalam menjaga informasi pribadi di dunia digital. Penyuluhan ini akan dilaksanakan dalam bentuk seminar interaktif yang menghadirkan pakar di bidang keamanan siber serta praktisi IT yang memiliki pengalaman dalam menangani kasus kebocoran data. Selain itu, akan dilakukan kampanye digital di lingkungan sekolah, baik secara

daring melalui media sosial maupun secara luring melalui pemasangan poster dan infografis yang mengedukasi siswa tentang pentingnya menjaga privasi mereka secara digital.

Materi yang disampaikan dalam penyuluhan akan mencakup bahaya dari penggunaan kata sandi yang lemah, pentingnya menghindari berbagi informasi sensitif di media sosial, serta perlindungan terhadap aplikasi dan perangkat yang digunakan dalam aktivitas sehari-hari. Sebagai pelengkap, siswa akan diberikan modul edukatif dalam bentuk brosur digital dan video pendek yang menjelaskan langkah-langkah pengamanan data pribadi. Target utama dari solusi ini adalah meningkatkan pemahaman siswa minimal sebesar 80% mengenai pentingnya perlindungan data pribadi serta menanamkan kebiasaan yang lebih aman dalam berinternet.

2. METODE

Program PKM Perlindungan Data Pribadi dan Pengenalan Ancaman Phishing kepada Siswa Sekolah Menengah Atas akan dilaksanakan melalui serangkaian tahapan yang sistematis guna memastikan efektivitas dalam meningkatkan literasi digital siswa dan tenaga pendidik. Metode pelaksanaan dirancang untuk memberikan pemahaman yang komprehensif melalui sosialisasi, pelatihan, penerapan teknologi, pendampingan, evaluasi, serta memastikan keberlanjutan program di lingkungan sekolah mitra. Setiap tahapan dirancang dengan mempertimbangkan tingkat pemahaman awal siswa serta kesiapan sekolah dalam mengadopsi praktik keamanan digital yang lebih baik.



Gambar 1. Tahapan Pelatihan

2.1 Sosialisasi Program

Tahap awal dalam pelaksanaan program ini adalah sosialisasi yang bertujuan untuk memberikan pemahaman mendalam mengenai pentingnya perlindungan data pribadi dan ancaman phishing kepada seluruh pihak yang terlibat, termasuk kepala sekolah, guru, dan siswa. Sosialisasi akan dilakukan melalui pertemuan formal dengan pihak sekolah untuk membahas tujuan program, manfaat yang akan diperoleh, serta strategi implementasi yang akan diterapkan. Dalam tahap ini, pihak sekolah diberikan kesempatan untuk menyampaikan pandangan serta kesiapan mereka dalam mendukung pelaksanaan program. Selanjutnya, akan dilakukan penyuluhan awal kepada siswa dan tenaga pendidik dengan menghadirkan pakar di bidang keamanan digital yang akan memberikan wawasan tentang ancaman dunia maya dan bagaimana cara menghadapinya.

Untuk mengetahui tingkat pemahaman awal siswa dan tenaga pendidik mengenai topik ini, kuesioner pre-test akan diberikan guna mengukur sejauh mana mereka sudah memahami konsep perlindungan data pribadi dan pencegahan phishing. Data yang diperoleh dari kuesioner ini akan menjadi dasar untuk menyusun strategi pembelajaran yang lebih efektif dan disesuaikan dengan kebutuhan sekolah mitra. Sosialisasi ini juga mencakup distribusi materi edukatif dalam bentuk infografis dan video pendek yang dirancang agar mudah dipahami oleh siswa.

2.2 Pelatihan Keamanan Digital

Setelah tahap sosialisasi, program ini akan dilanjutkan dengan pelatihan intensif yang bertujuan untuk membekali siswa dan tenaga pendidik dengan keterampilan teknis dalam mengidentifikasi dan mencegah ancaman phishing serta menjaga keamanan data pribadi. Pelatihan ini dilakukan dengan pendekatan teoritis dan praktis, di mana peserta akan diberikan modul pembelajaran yang mencakup topik tentang bagaimana menjaga data pribadi, membuat kata sandi yang kuat, serta mengaktifkan fitur keamanan seperti autentikasi dua faktor. Selain itu, simulasi phishing juga akan diterapkan dengan menyajikan contoh nyata dari email atau situs web phishing agar siswa dan guru dapat secara langsung berlatih mengenali pola serangan yang sering digunakan oleh penipu daring.

Pelatihan ini juga mencakup workshop interaktif yang memberikan kesempatan kepada siswa untuk membuat konten edukatif digital seperti video pendek atau poster kampanye yang berisi pesan tentang pentingnya menjaga keamanan digital. Pendekatan ini bertujuan untuk melibatkan siswa secara aktif dalam menyebarkan informasi tentang ancaman phishing kepada teman sebaya mereka. Bagi guru, pelatihan ini tidak hanya berfokus pada pemahaman dasar keamanan digital tetapi juga mencakup bagaimana mereka dapat mengintegrasikan materi ini dalam pembelajaran sehari-hari sehingga siswa dapat terus mendapatkan edukasi mengenai keamanan digital secara berkelanjutan.

2.3 Pendampingan dan Evaluasi

Setelah pelaksanaan sosialisasi, pelatihan, dan penerapan teknologi, program ini akan memasuki tahap pendampingan yang bertujuan untuk memastikan bahwa materi yang diberikan dapat diimplementasikan dengan baik oleh siswa dan tenaga pendidik. Dalam tahap ini, akan dibentuk kelompok literasi digital yang terdiri dari siswa dan guru sebagai agen perubahan yang bertugas untuk menyebarkan informasi mengenai keamanan digital kepada komunitas sekolah. Kelompok ini akan mendapatkan bimbingan secara berkala agar dapat menjadi sumber informasi terpercaya bagi siswa lainnya.

Evaluasi program akan dilakukan melalui beberapa metode, termasuk pengukuran hasil pelatihan dengan membandingkan hasil pre-test dan post-test yang diberikan kepada peserta. Selain itu, survei umpan balik juga akan dilakukan untuk mengukur sejauh mana siswa dan guru merasa terbantu dengan program ini serta untuk mengidentifikasi aspek mana yang perlu diperbaiki. Dari hasil evaluasi ini, rekomendasi akan diberikan kepada pihak sekolah mengenai strategi keberlanjutan yang dapat diterapkan agar literasi digital tetap menjadi bagian dari budaya sekolah.

Dalam perencanaan dan implementasinya, program ini mengikuti prinsip-prinsip dasar pengabdian kepada masyarakat sebagaimana ditegaskan oleh Khasanah et al. (2024), yang menekankan pentingnya proses identifikasi kebutuhan mitra, pemilihan metode edukasi yang tepat, serta pelaksanaan kegiatan berbasis partisipatif untuk meningkatkan kebermanfaatan program. Pendekatan ini memastikan bahwa kegiatan pengabdian tidak hanya bersifat seremonial, tetapi benar-benar memberikan dampak nyata melalui kolaborasi, asesmen kebutuhan, dan pendampingan berkelanjutan sesuai kerangka metodologi pengabdian masyarakat berbasis teori dan implementasi.

2.4 Keberlanjutan Program

Agar program ini dapat memberikan dampak jangka panjang, berbagai strategi keberlanjutan akan diterapkan di sekolah mitra. Salah satu strategi utama adalah penyusunan Standar Operasional Prosedur (SOP) Keamanan Digital Sekolah yang mencakup langkah-langkah yang harus diambil oleh siswa dan guru dalam melindungi data pribadi mereka. SOP ini akan menjadi pedoman resmi bagi seluruh komunitas sekolah dalam menghadapi ancaman phishing dan kejahatan digital lainnya.

Selain itu, sekolah didorong untuk mengintegrasikan materi keamanan digital ke dalam kurikulum Teknologi Informasi dan Komunikasi (TIK) agar siswa terus mendapatkan edukasi yang relevan seiring dengan perkembangan teknologi. Program ini juga akan memastikan bahwa komunitas keamanan digital yang telah dibentuk di sekolah dapat terus berjalan dengan dukungan dari tenaga pendidik yang telah mendapatkan pelatihan. Dengan demikian, program ini tidak hanya berdampak dalam jangka pendek tetapi juga memberikan manfaat jangka panjang bagi lingkungan sekolah.

2.5 Partisipasi Mitra dalam Program

Dalam pelaksanaan program ini, mitra sekolah akan berperan aktif di setiap tahapan. Kepala sekolah akan memberikan dukungan dalam bentuk kebijakan yang memfasilitasi pelaksanaan program, sementara guru akan berpartisipasi dalam pelatihan serta mendampingi siswa dalam kegiatan komunitas literasi digital. Siswa juga akan dilibatkan secara aktif dalam setiap tahapan, baik sebagai peserta pelatihan maupun sebagai agen perubahan yang akan menyebarkan kesadaran tentang keamanan digital di lingkungan sekolah mereka.

Pelaksanaan program ini akan didukung oleh tim pengabdian yang terdiri dari dosen dan mahasiswa dengan peran yang sesuai dengan kompetensinya. Dosen ahli di bidang keamanan digital akan bertanggung jawab dalam menyusun materi pelatihan dan memberikan pendampingan teknis. Mahasiswa informatika akan mengembangkan teknologi pendukung seperti dashboard monitoring, selain itu siswa dan mahasiswa akan membantu dalam penyebaran kampanye digital dan edukasi berbasis media sosial.

Dalam pelaksanaan program ini, mitra sekolah akan berperan aktif di setiap tahapan. Kepala sekolah akan memberikan dukungan dalam bentuk kebijakan yang memfasilitasi pelaksanaan program, sementara guru akan berpartisipasi dalam pelatihan serta mendampingi siswa dalam kegiatan komunitas literasi digital. Siswa juga akan dilibatkan secara aktif dalam setiap tahapan, baik sebagai peserta pelatihan maupun sebagai agen perubahan yang akan menyebarkan kesadaran tentang keamanan digital di lingkungan sekolah mereka. Pelaksanaan program ini akan didukung oleh tim pengabdian yang terdiri dari dosen dan mahasiswa dengan peran yang sesuai dengan kompetensinya. Dosen ahli di bidang keamanan digital akan bertanggung jawab dalam menyusun materi pelatihan dan memberikan pendampingan teknis. Mahasiswa informatika akan mengembangkan teknologi pendukung seperti dashboard monitoring, selain itu siswa dan mahasiswa akan membantu dalam penyebaran kampanye digital dan edukasi berbasis media sosial.

3. HASIL DAN PEMBAHASAN

Untuk mengatasi permasalahan rendahnya tingkat literasi digital siswa terkait perlindungan data pribadi dan ancaman phishing, serangkaian solusi yang komprehensif dirancang agar mampu memberikan dampak yang signifikan bagi mitra sasaran. Solusi ini mencakup upaya edukasi, penguatan kapasitas tenaga pendidik, pengembangan kebijakan sekolah, serta implementasi teknologi yang mendukung ekosistem digital yang aman.

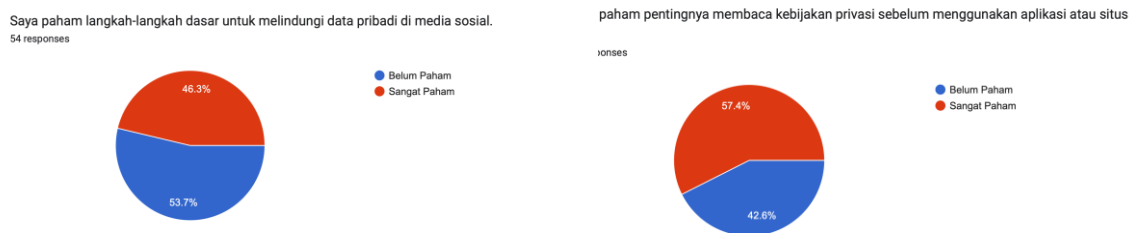
3.1 Sosialisasi Program

Tahap awal dalam pelaksanaan program ini adalah sosialisasi yang bertujuan untuk memberikan pemahaman mendalam mengenai pentingnya perlindungan data pribadi dan ancaman phishing kepada seluruh pihak yang terlibat, termasuk kepala sekolah, guru, dan siswa. Sosialisasi akan dilakukan melalui pertemuan formal dengan pihak sekolah untuk membahas tujuan program, manfaat yang akan diperoleh, serta strategi implementasi yang akan diterapkan. Dalam tahap ini, pihak sekolah diberikan kesempatan untuk menyampaikan pandangan serta kesiapan mereka dalam mendukung pelaksanaan program. Selanjutnya, akan dilakukan penyuluhan awal kepada siswa dan tenaga pendidik dengan menghadirkan pakar di bidang keamanan digital yang akan memberikan wawasan tentang ancaman dunia maya dan bagaimana cara menghadapinya.



Gambar 2. Sosialisasi Program

Untuk mengetahui tingkat pemahaman awal siswa dan tenaga pendidik mengenai topik ini, kuesioner pre-test akan diberikan guna mengukur sejauh mana mereka sudah memahami konsep perlindungan data pribadi dan pencegahan phishing. Data yang diperoleh dari kuesioner ini akan menjadi dasar untuk menyusun strategi pembelajaran yang lebih efektif dan disesuaikan dengan kebutuhan sekolah mitra. Sosialisasi ini juga mencakup distribusi materi edukatif dalam bentuk infografis dan video pendek yang dirancang agar mudah dipahami oleh siswa.



Gambar 3. Hasil Pelaksanaan Pre-Test

Dari hasil pre-tes yang dilakukan terlihat bahwa sebagian dari peserta belum mengetahui konsep perlindungan data pribadi dan pencegahannya. oleh karena itu kegiatan pelatihan ini dapat meningkatkan pemahaman siswa dan guru terkait perlindungan data pribadi dan teknik pencegahan phishing.

3.2 Pelatihan Keamanan Digital

Setelah tahap sosialisasi, program ini akan dilanjutkan dengan pelatihan intensif yang bertujuan untuk membekali siswa dan tenaga pendidik dengan keterampilan teknis dalam mengidentifikasi dan mencegah

ancaman phishing serta menjaga keamanan data pribadi. Pelatihan ini dilakukan dengan pendekatan teoritis dan praktis, di mana peserta akan diberikan modul pembelajaran yang mencakup topik tentang bagaimana menjaga data pribadi, membuat kata sandi yang kuat, serta mengaktifkan fitur keamanan seperti autentikasi dua faktor. Selain itu, simulasi phishing juga akan diterapkan dengan menyajikan contoh nyata dari email atau situs web phishing agar siswa dan guru dapat secara langsung berlatih mengenali pola serangan yang sering digunakan oleh penipu daring.



Gambar 4. Hasil Pelaksanaan Pre-Test

Pelatihan ini juga mencakup workshop interaktif yang memberikan kesempatan kepada siswa untuk membuat konten edukatif digital seperti video pendek atau poster kampanye yang berisi pesan tentang pentingnya menjaga keamanan digital. Pendekatan ini bertujuan untuk melibatkan siswa secara aktif dalam menyebarkan informasi tentang ancaman phishing kepada teman sebaya mereka. Bagi guru, pelatihan ini tidak hanya berfokus pada pemahaman dasar keamanan digital tetapi juga mencakup bagaimana mereka dapat mengintegrasikan materi ini dalam pembelajaran sehari-hari sehingga siswa dapat terus mendapatkan edukasi mengenai keamanan digital secara berkelanjutan.



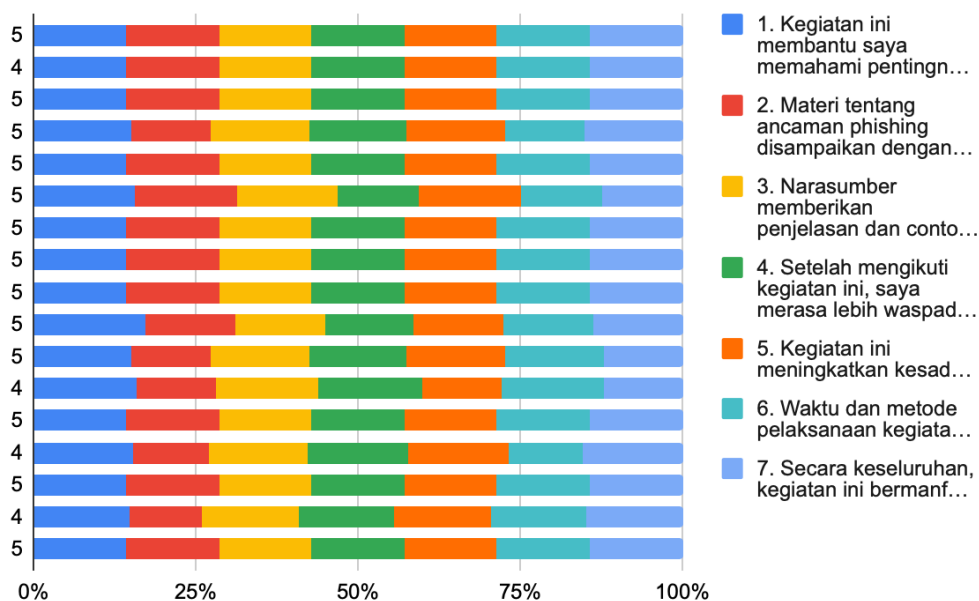


Gambar 4. Hasil Pelaksanaan Pre-Test

3.3 Pendampingan dan Evaluasi

Setelah pelaksanaan sosialisasi, pelatihan, dan penerapan teknologi, program ini akan memasuki tahap pendampingan yang bertujuan untuk memastikan bahwa materi yang diberikan dapat diimplementasikan dengan baik oleh siswa dan tenaga pendidik. Dalam tahap ini, akan dibentuk kelompok literasi digital yang terdiri dari siswa dan guru sebagai agen perubahan yang bertugas untuk menyebarkan informasi mengenai keamanan digital kepada komunitas sekolah. Kelompok ini akan mendapatkan bimbingan secara berkala agar dapat menjadi sumber informasi terpercaya bagi siswa lainnya.

Evaluasi program akan dilakukan melalui beberapa metode, termasuk pengukuran hasil pelatihan dengan membandingkan hasil pre-test dan post-test yang diberikan kepada peserta. Selain itu, survei umpan balik juga akan dilakukan untuk mengukur sejauh mana siswa dan guru merasa terbantu dengan program ini serta untuk mengidentifikasi aspek mana yang perlu diperbaiki. Dari hasil evaluasi ini, rekomendasi akan diberikan kepada pihak sekolah mengenai strategi keberlanjutan yang dapat diterapkan agar literasi digital tetap menjadi bagian dari budaya sekolah.



Gambar 4. Hasil Pelaksanaan Pre-Test

Berdasarkan hasil post test kegiatan sosialisasi perlindungan data pribadi dan teknik pencegahan phishing, dapat disimpulkan bahwa kegiatan ini berjalan dengan sangat baik dan efektif. Mayoritas peserta memberikan

nilai tinggi (4 dan 5) pada seluruh indikator, yang menunjukkan bahwa kegiatan ini berhasil meningkatkan pemahaman peserta tentang pentingnya perlindungan data pribadi. Materi mengenai ancaman phishing dinilai disampaikan dengan jelas, relevan, dan mudah dipahami oleh peserta, sementara narasumber dianggap mampu memberikan penjelasan serta contoh yang aplikatif. Selain itu, kegiatan ini juga terbukti meningkatkan kesadaran dan kewaspadaan peserta terhadap ancaman phishing serta mendorong perilaku yang lebih protektif terhadap keamanan data pribadi. Aspek waktu dan metode pelaksanaan kegiatan pun dinilai memadai, menandakan bahwa durasi, cara penyampaian, dan interaksi selama kegiatan berlangsung dengan efektif. Secara keseluruhan, kegiatan sosialisasi ini dinilai sangat bermanfaat dan memberikan dampak positif terhadap peningkatan pengetahuan dan kesadaran peserta mengenai keamanan data pribadi di era digital.

3.4 Keberlanjutan Program

Agar program ini dapat memberikan dampak jangka panjang, berbagai strategi keberlanjutan akan diterapkan di sekolah mitra. Salah satu strategi utama adalah penyusunan Standar Operasional Prosedur (SOP) Keamanan Digital Sekolah yang mencakup langkah-langkah yang harus diambil oleh siswa dan guru dalam melindungi data pribadi mereka. SOP ini akan menjadi pedoman resmi bagi seluruh komunitas sekolah dalam menghadapi ancaman phishing dan kejahatan digital lainnya.

Selain itu, sekolah didorong untuk mengintegrasikan materi keamanan digital ke dalam kurikulum Teknologi Informasi dan Komunikasi (TIK) agar siswa terus mendapatkan edukasi yang relevan seiring dengan perkembangan teknologi. Program ini juga akan memastikan bahwa komunitas keamanan digital yang telah dibentuk di sekolah dapat terus berjalan dengan dukungan dari tenaga pendidik yang telah mendapatkan pelatihan. Dengan demikian, program ini tidak hanya berdampak dalam jangka pendek tetapi juga memberikan manfaat jangka panjang bagi lingkungan sekolah.

4. KESIMPULAN DAN SARAN

Pelaksanaan Program Kemitraan Masyarakat (PKM) yang berfokus pada *Perlindungan Data Pribadi dan Pengenalan Ancaman Phishing kepada Siswa Sekolah Menengah Atas* memberikan dampak yang signifikan terhadap peningkatan literasi digital dan kesadaran keamanan siber di lingkungan sekolah mitra. Kegiatan ini dirancang sebagai bentuk respons terhadap rendahnya tingkat pemahaman siswa dan guru mengenai pentingnya perlindungan data pribadi serta tingginya risiko serangan phishing yang menyasar pengguna muda di dunia digital. Melalui pendekatan partisipatif yang melibatkan dosen, mahasiswa, guru, dan siswa, program ini berhasil menciptakan proses pembelajaran yang interaktif dan aplikatif. Tahapan kegiatan yang meliputi sosialisasi, pelatihan keamanan digital, simulasi phishing, dan pendampingan memberikan pengalaman langsung kepada peserta untuk memahami ancaman siber sekaligus melatih keterampilan teknis dalam menghindarinya. Pelatihan tersebut tidak hanya memperkenalkan konsep dasar perlindungan data pribadi, tetapi juga mengajarkan praktik nyata seperti pembuatan kata sandi yang kuat, penerapan autentikasi dua faktor, serta cara mengenali ciri-ciri email atau tautan phishing.

Hasil evaluasi menunjukkan adanya peningkatan yang nyata pada tingkat pemahaman siswa dan tenaga pendidik setelah mengikuti seluruh rangkaian kegiatan. Berdasarkan perbandingan hasil pre-test dan post-test, sebagian besar siswa menunjukkan peningkatan kemampuan dalam mengenali potensi serangan phishing dengan tingkat keberhasilan mencapai lebih dari 75 persen. Selain itu, lebih dari 80 persen guru peserta pelatihan dinilai mampu memahami dan mengajarkan kembali konsep-konsep keamanan digital kepada siswa, sehingga terbentuk kelompok fasilitator keamanan digital di sekolah mitra.

Capaian tersebut menegaskan bahwa kegiatan ini tidak hanya memberikan edukasi jangka pendek, tetapi juga menanamkan kebiasaan baru yang lebih aman dan bertanggung jawab dalam penggunaan teknologi digital. Sekolah mitra kini memiliki sumber daya manusia yang lebih siap dalam menghadapi ancaman keamanan siber serta telah memiliki panduan digital dan modul pembelajaran yang dapat dijadikan referensi berkelanjutan. Program ini juga menjadi langkah strategis dalam memperkuat peran perguruan tinggi sebagai agen pemberdayaan masyarakat di bidang literasi digital, sejalan dengan Indikator Kinerja Utama (IKU) yang menekankan kontribusi nyata perguruan tinggi terhadap peningkatan kualitas pendidikan dan ketahanan digital masyarakat.

Secara keseluruhan, kegiatan PKM ini telah berhasil mewujudkan lingkungan sekolah yang lebih sadar terhadap pentingnya perlindungan data pribadi serta mampu menciptakan budaya keamanan digital yang tangguh. Dampak positif yang dihasilkan menunjukkan bahwa pendekatan kolaboratif antara akademisi, tenaga pendidik, dan siswa merupakan strategi efektif dalam membangun kesadaran dan kompetensi digital yang berkelanjutan di era transformasi teknologi informasi saat ini.

Berdasarkan hasil pelaksanaan program dan evaluasi yang telah dilakukan, terdapat beberapa hal yang perlu diperhatikan untuk mendukung keberlanjutan dan peningkatan kualitas kegiatan serupa di masa mendatang. Sekolah mitra diharapkan dapat melanjutkan upaya literasi digital dengan mengintegrasikan materi keamanan siber ke dalam kurikulum Teknologi Informasi dan Komunikasi (TIK) maupun kegiatan ekstrakurikuler. Dengan

demikian, pemahaman siswa terhadap perlindungan data pribadi dan ancaman phishing tidak berhenti pada kegiatan pelatihan semata, tetapi menjadi bagian dari proses pembelajaran yang berkelanjutan di lingkungan sekolah.

Selain itu, pelatihan dan pendampingan lanjutan bagi guru perlu terus dilakukan secara periodik. Hal ini penting agar tenaga pendidik selalu memperoleh pembaruan informasi terkait tren dan bentuk-bentuk ancaman siber yang terus berkembang. Dengan adanya pelatihan berkelanjutan, guru dapat terus berperan sebagai fasilitator keamanan digital yang mampu membimbing siswa dalam menerapkan perilaku berinternet yang aman dan bertanggung jawab.

Pihak sekolah juga disarankan untuk memperkuat kebijakan internal terkait keamanan digital melalui penyusunan dan penerapan *Standard Operating Procedure* (SOP) Keamanan Digital Sekolah. Dokumen ini akan menjadi pedoman resmi bagi seluruh warga sekolah dalam melindungi data pribadi, menangani potensi insiden siber, serta memastikan bahwa setiap aktivitas digital di lingkungan sekolah dilakukan dengan aman dan sesuai prinsip perlindungan privasi. Selanjutnya, keberhasilan program ini diharapkan dapat direplikasi dan diperluas ke sekolah-sekolah lain, khususnya di wilayah yang memiliki tingkat literasi digital yang masih rendah. Kolaborasi antara perguruan tinggi, sekolah, dan lembaga pemerintah akan menjadi langkah strategis untuk memperluas dampak positif dari kegiatan ini, sekaligus membangun ekosistem pendidikan yang tanggap terhadap ancaman digital.

Dengan penerapan saran-saran tersebut, diharapkan upaya peningkatan literasi digital dan kesadaran keamanan siber di kalangan pelajar dapat terus berlanjut, memberikan manfaat jangka panjang, serta mendukung terciptanya generasi muda yang cerdas, kritis, dan bertanggung jawab dalam menghadapi perkembangan teknologi informasi di era digital.

UCAPAN TERIMA KASIH

Program Kemitraan Masyarakat (PKM) ini dapat terlaksana berkat dukungan pendanaan dari Universitas Negeri Makassar melalui Dana PNPB Tahun 2025. Penulis menyampaikan apresiasi kepada SMK Negeri 2 Kabupaten Gowa sebagai mitra kegiatan atas kerja sama dan keterlibatannya selama proses pelaksanaan program. Terima kasih juga ditujukan kepada seluruh guru, siswa, serta tim dosen dan mahasiswa Jurusan Teknik Informatika dan Komputer, Fakultas Teknik UNM, yang telah berkontribusi dalam penyusunan materi, pelatihan, dan evaluasi kegiatan. Dukungan dari berbagai pihak tersebut sangat berperan dalam keberhasilan pelaksanaan program yang berfokus pada peningkatan literasi digital dan kesadaran terhadap keamanan siber di lingkungan sekolah.

REFERENSI

- Adani DW, Nurhayati I, Mirati RE. The Importance of Security Awareness of Phishing in Indonesia: a Systematic Literature Review. ResearchGate Preprint.2023.
- Ali R, Hussain A, Kumar P. Assessing the Efficacy of Security Awareness Training in Mitigating Phishing Attack: a review. ResearchGate Preprint.2024.
- Candra Wulan PID, Perdana DP, Fauzi R, Pormes R. Edukasi undang undang informasi dan transaksi elektronik serta perlindungan data pribadi dari kejahatan digital di Desa Kirig Kudus. KACANEGARA. 2023 May 2;6(2):185.
- Harahap SZ, Juledi AP, Munthe IR, Nasution M, Irmayani D. e-ISSN : 2808-4047 Universitas Labuhanbatu. 2023; Khasanah, U., Trisnawati, S. N. I., Isma, A., Alanur, S. N., Maida, A. N., Nainiti, N. P. P. E., Amin, L. H., Aryawati, N. P. A., Murwati, M., Bangu, B., & Maulida, C. (2024). Metodologi Pengabdian Kepada Masyarakat: Teori dan Implementasi. *Penerbit Tahta Media*. Retrieved from <https://tahtamedia.co.id/index.php/issj/article/view/1066>
- Nasution M, Juledi AP, Hrahap SZ, Irmayani D, Munthe IR. e-ISSN : 2808-4047 Universitas Labuhanbatu. 2024; Reyner A, Ujianto T. Sosialisasi Keamanan Digital Kepada Siswa Berkebutuhan Khusus Di Sekolah Inklusi Pkbn House Of Knowledge. 2024;3(2).
- Sapriadi S, Eko Syaputra A, Septi Eirlangga Y, Hariani Manurung K, Hayati N. Sosialisasi dan Pelatihan Secure Computer dalam Meningkatkan Kesadaran Siswa terhadap Keamanan Data. jmi. 2023 Dec 6;38–43.
- Surbakti FPS. Edukasi Keamanan Siber Berdigital dengan Aman. Pri Abd:JPM. 2024 Dec 1;4(4):868–78.
- Syaddan S. Sosialisasi Keamanan Data di Dunia Siber untuk Meningkatkan Kewaspadaan SMK 1 Negeri Tarakan Terhadap Ancaman Cybercrime. arch. 2024 Jun 13;3(2):289–99.
- Tandirerung VA, Riana T. Mangesa, Syahrul. Pengenalan Cyber Security Bagi Siswa Sekolah Menengah Atas. TEKNOVOKASI. 2023 May 15;1(2):89–94.
- Wijayanto A. Mengenal Cybersecurity: Perlindungan Data Pribadi Dan Privasi Di Sma Negeri 1 Samboja. 2024;3(2).