



## **Edukasi Keamanan Siber sebagai Upaya Preventif terhadap Ancaman Phishing pada Siswa SMA Islam Tambora Jakarta Barat**

*(Cybersecurity Education as a Preventive Measure Against Phishing Threats Among Students of SMA Islam Tambora Jakarta Barat)*

**Muhammad Patria<sup>1\*</sup>, Dea Andini Andriati<sup>2</sup>, Haryo Kusumo Wicaksono<sup>3</sup>, Muhammad Yusril Rapsanjani<sup>4</sup>, Tia Amelia Azmi<sup>5</sup>, Muhammad Fauzan Arbah<sup>6</sup>, M Sirojul Anam<sup>7</sup>**

<sup>1,2,3,4,5,6,7</sup>Teknik Informatika, Fakultas Teknik dan Informatika, Universitas Dian Nusantara, Jakarta

\*email: [muhammad.patria@undira.ac.id](mailto:muhammad.patria@undira.ac.id)

Diterima: 02 Februari 2026, Diperbaiki: 24 Februari 2026, Disetujui: 25 Februari 2026

**Abstract.** *The rapid development of digital technology has increased internet usage among students while also expanding exposure to cybersecurity threats such as phishing. This community service activity aimed to enhance the digital security awareness and understanding of twelfth-grade students at SMA Islam Tambora as a preventive measure against phishing threats. The program employed a participatory-educational approach consisting of three stages: preparation, socialization, and evaluation. A total of 11 students participated, with pre-test and post-test instruments used to measure improvements in understanding phishing concepts, account security practices, and personal data protection. The results showed an increase in the average score from 60 in the pre-test to 88 in the post-test, with 90.9% of participants demonstrating significant improvement. Questionnaire evaluation also indicated highly positive responses regarding material clarity and program relevance. These findings suggest that interactive and practice-based cybersecurity education is effective in strengthening students' digital security literacy and fostering safer online behavior. The program has potential to be replicated as a model for digital literacy reinforcement in secondary education.*

**Keywords:** cybersecurity education, phishing, digital literacy, personal data protection, high school students

**Abstrak.** Perkembangan teknologi digital meningkatkan intensitas penggunaan internet di kalangan pelajar, namun juga memperluas risiko ancaman siber seperti *phishing*. Kegiatan Pengabdian kepada Masyarakat ini bertujuan meningkatkan pemahaman dan kesadaran keamanan digital siswa kelas XII SMA Islam Tambora sebagai upaya preventif terhadap ancaman *phishing*. Metode pelaksanaan menggunakan pendekatan partisipatif-edukatif melalui tiga tahap, yaitu persiapan, sosialisasi, dan evaluasi. Kegiatan diikuti oleh 11 siswa dengan instrumen evaluasi berupa *pre-test* dan *post-test* untuk mengukur peningkatan pemahaman terkait konsep *phishing*, praktik keamanan akun, dan perlindungan data pribadi. Hasil menunjukkan rata-rata skor meningkat dari 60 pada *pre-test* menjadi 88 pada *post-test*, dengan 90,9% peserta mengalami peningkatan signifikan. Evaluasi kuesioner juga menunjukkan respons sangat positif terhadap kejelasan materi dan manfaat kegiatan. Temuan ini menunjukkan bahwa edukasi keamanan siber berbasis interaktif dan praktik langsung efektif dalam meningkatkan literasi keamanan digital siswa serta membentuk perilaku digital yang lebih aman. Program ini berpotensi direplikasi sebagai model penguatan literasi digital di tingkat pendidikan menengah.

**Kata kunci:** edukasi keamanan siber, penipuan digital, literasi digital, perlindungan data pribadi, SMA

### **PENDAHULUAN**

Perkembangan pesat teknologi digital telah mendorong penggunaan internet

secara masif di berbagai kelompok usia, termasuk pelajar sekolah menengah



Lisensi  
Lisensi Internasional Creative Commons Attribution-ShareAlike 4.0.

(Muhtada et al., 2025; Pane, 2021). Sementara akses digital membawa manfaat dalam pembelajaran dan komunikasi, hal ini juga memperluas permukaan ancaman siber seperti *phising*, yang menggunakan teknik rekayasa sosial untuk mencuri data pribadi dan kredensial akses (Hendrawan et al., 2025). Fenomena ini merupakan bagian dari tantangan keaman digital yang lebih luas, di mana literasi kewanitaan siber menjadi krusial untuk melindungi individu dari eksploitasi digital (Hendrawan et al., 2025; Patria, 2025; Wanayumini et al., 2025). Ancaman *social engineering* dan *phishing* kini menjadi perhatian penting dalam studi keaman siber karena kompleksitas yang terus berkembang (Eriana et al., 2025; Pane, 2021).

Literatur pendidikan dan keaman informasi menekankan bahwa literasi digital yang mencakup pemahaman risiko, prinsip privasi, serta strategi mitigasi ancaman siber dapat meningkatkan kesadaran dan kemampuan pelajar untuk mengamankan diri dari berbagai bentuk kejahatan siber yang semakin canggih (Arifin et al., 2024; Muhtada et al., 2025). Pendidikan yang terstruktur dan kontekstual, termasuk penggunaan simulasi dan praktik aplikasi, terbukti memperkuat kemampuan peserta didik dalam melindungi data mereka sendiri serta memahami aspek autentikasi dan identitas digital (Patria, 2025; Wahyuni et al., 2025).

Meskipun demikian, masih terdapat gap signifikan antara penetrasi penggunaan internet di kalangan siswa dan kesiapan mereka dalam menghadapi serangan siber secara preventif. Studi kasus pada institusi pendidikan menunjukkan bahwa banyak siswa memiliki keterbatasan dalam praktik keaman digital yang lebih mendalam, termasuk kemampuan deteksi tanda-tanda tautan berbahaya atau pengelolaan kredensial secara aman, meskipun mereka sudah memiliki literasi dasar terkait teknologi (Arsyad et al., 2024)

Kondisi tersebut juga tercermin pada lingkungan pendidikan tingkat menengah,

termasuk di SMA Islam Tambora (NPSN 20101348) yang berlokasi di Kecamatan Tambora, Kota Jakarta Barat. Sekolah dengan akreditasi B ini memiliki sekitar 159 peserta didik yang secara aktif memanfaatkan teknologi digital dalam proses pembelajaran maupun interaksi sosial. Hasil identifikasi awal kegiatan pengabdian menunjukkan bahwa pemahaman siswa terkait praktik keaman digital dasar, seperti pengelolaan kata sandi yang kuat dan kemampuan mengenali tautan phishing, masih memerlukan penguatan lebih lanjut melalui pendekatan edukatif yang sistematis.

Profil mitra ini menunjukkan ruang yang strategis untuk intervensi edukasi keaman siber berskala sekolah karena karakteristik penggunaan internet oleh siswa dan kebutuhan akan literasi digital yang lebih komprehensif. Hal ini sejalan dengan penelitian yang menunjukkan kebutuhan penguatan kompetensi digital secara kontekstual bagi pelajar sekolah menengah untuk menanggulangi ancaman siber yang semakin canggih dan bervariasi (Isnawati et al., 2021). Urgensi tersebut menjadi semakin relevan terutama bagi siswa kelas XII yang berada pada fase transisi menuju pendidikan tinggi maupun dunia kerja, di mana interaksi digital akan semakin luas dan kompleks, baik dalam proses pendaftaran, komunikasi profesional, transaksi daring, maupun pengelolaan identitas digital pribadi. Oleh karena itu, pembekalan literasi keaman siber pada tahap ini tidak hanya bersifat preventif jangka pendek, tetapi juga menjadi fondasi kesiapan digital dalam menghadapi dinamika kehidupan setelah lulus sekolah.

Beragam studi pengabdian dan riset pendidikan keaman siber di lingkungan sekolah juga menunjukkan bahwa program literasi keaman digital dapat meningkatkan kemampuan siswa dalam memitigasi risiko siber (Rahman, 2024). Misalnya, pelatihan interaktif yang

mencakup penyampaian materi, simulasi, dan evaluasi *pre-post* intervensi menunjukkan peningkatan signifikansi dalam penguasaan praktik aman digital, seperti pengenalan phishing dan pengaturan privasi akun (Novantara & Suwandi, 2025).

Meskipun beberapa kajian sebelumnya telah mengevaluasi program literasi keamanan digital di sekolah, sebagian besar fokusnya adalah pada deskripsi tingkat kesadaran atau pemahaman yang bersifat umum tanpa mengukur secara terstruktur perubahan pengetahuan dan praktik sebelum dan setelah intervensi pendidikan (Ayuningtyas et al., 2025). Kesenjangan ini menunjukkan kebutuhan penelitian yang tidak hanya mendeskripsikan fenomena tetapi juga mengevaluasi dampak praktik edukasi secara kuantitatif untuk menghasilkan rekomendasi implementasi yang lebih evidensial (Wijayanto et al., 2026).

Dengan mempertimbangkan kebutuhan mitra dan gap penelitian tersebut, kegiatan Pengabdian kepada Masyarakat (PkM) ini dirancang untuk mengimplementasikan pendidikan keamanan siber sebagai upaya preventif terhadap ancaman phishing pada siswa SMA Islam Tambora. Program ini memadukan penyampaian materi kontekstual, diskusi interaktif, studi kasus nyata, dan evaluasi hasil untuk mengukur

perubahan pemahaman dan praktik keamanan digital peserta didik secara empiris. Diharapkan kegiatan ini akan memberikan kontribusi pada pengembangan model edukasi keamanan digital yang relevan untuk konteks pendidikan menengah di Indonesia. Adapun tujuan kegiatan ini adalah meningkatkan pemahaman siswa mengenai ancaman *phishing*, memperkuat praktik keamanan akun dan perlindungan data pribadi, serta membangun kesadaran perilaku digital yang aman sebagai bekal menghadapi pendidikan tinggi dan dunia kerja.

### METODE KEGIATAN

Kegiatan Pengabdian kepada Masyarakat ini dilaksanakan di SMA Islam Tambora yang berlokasi di Kecamatan Tambora, Kota Jakarta Barat. Sasaran kegiatan adalah siswa kelas XII, yang berada pada fase transisi menuju pendidikan tinggi maupun dunia kerja. Karakteristik peserta menunjukkan intensitas penggunaan perangkat digital yang tinggi, baik untuk pembelajaran, komunikasi sosial, maupun akses layanan daring. Kondisi ini menjadikan siswa kelas XII sebagai kelompok strategis dalam penguatan literasi keamanan siber, khususnya dalam menghadapi ancaman *phishing* dan risiko penyalahgunaan data pribadi.



**Gambar 1.** Tahapan Pelaksanaan Kegiatan Pengabdian kepada Masyarakat.

Pendekatan yang digunakan dalam kegiatan ini adalah pendekatan partisipatif-edukatif, di mana tim pelaksana berperan sebagai fasilitator pembelajaran, sementara siswa sebagai mitra kegiatan ditempatkan sebagai subjek utama yang aktif dalam proses identifikasi masalah, diskusi, dan praktik penerapan keamanan digital. Model ini menekankan interaksi dua arah, pembelajaran berbasis pengalaman, serta penguatan kesadaran melalui refleksi bersama. Dengan pendekatan ini, proses transfer pengetahuan tidak bersifat satu arah, melainkan mendorong keterlibatan aktif peserta dalam memahami dan menerapkan prinsip keamanan digital dalam konteks keseharian mereka.

Pelaksanaan kegiatan dirancang dalam tiga tahap sistematis, yaitu tahap persiapan, tahap sosialisasi, dan tahap evaluasi, yang saling terintegrasi untuk memastikan efektivitas program secara menyeluruh.

Tahap persiapan meliputi koordinasi dengan pihak sekolah, penentuan jadwal kegiatan, identifikasi kebutuhan mitra melalui komunikasi awal, serta penyusunan materi edukasi yang kontekstual dan relevan dengan karakteristik peserta. Pada tahap ini, tim juga menyusun instrumen evaluasi berupa *pre-test* dan *post-test* untuk mengukur tingkat pemahaman awal dan perubahan pemahaman setelah intervensi. Materi yang disiapkan mencakup pengenalan ancaman *phishing*, praktik pengelolaan kata sandi yang kuat, penggunaan autentikasi dua faktor (2FA), serta simulasi identifikasi tautan mencurigakan.

Tahap sosialisasi merupakan inti pelaksanaan kegiatan yang dilakukan melalui metode presentasi interaktif, diskusi kasus nyata, serta praktik langsung. Penyampaian materi dilakukan secara komunikatif dengan melibatkan siswa dalam studi kasus berbasis contoh pesan atau tautan yang menyerupai serangan *phishing*. Peserta diajak untuk mengidentifikasi indikator bahaya,

mendiskusikan risiko yang mungkin terjadi, serta mempraktikkan langkah-langkah preventif seperti pembuatan kata sandi kuat dan aktivasi autentikasi dua faktor pada akun digital. Pendekatan ini bertujuan untuk mengintegrasikan pemahaman konseptual dengan pengalaman praktis sehingga terjadi internalisasi pengetahuan secara lebih mendalam.

Tahap evaluasi dilakukan untuk mengukur efektivitas kegiatan melalui perbandingan hasil *pre-test* dan *post-test* yang diberikan kepada peserta. Instrumen evaluasi dirancang untuk mengukur peningkatan pemahaman terkait konsep *phishing*, praktik keamanan akun, dan kesadaran terhadap perlindungan data pribadi. Indikator keberhasilan program ditetapkan apabila minimal 80% peserta menunjukkan peningkatan skor pemahaman setelah kegiatan berlangsung. Selain itu, evaluasi juga dilengkapi dengan umpan balik peserta terhadap materi dan metode penyampaian untuk mengetahui tingkat penerimaan serta relevansi program.

Hasil evaluasi yang menunjukkan peningkatan pemahaman dan respons positif dari peserta menjadi dasar untuk menilai efektivitas pendekatan partisipatif yang digunakan. Penguatan literasi keamanan digital melalui metode interaktif dan praktik langsung terbukti mampu meningkatkan kesadaran siswa terhadap ancaman *phishing* serta mendorong penerapan perilaku digital yang lebih aman.

## **HASIL DAN PEMBAHASAN**

Kegiatan Pengabdian kepada Masyarakat ini dihadiri oleh 11 siswa kelas XII SMA Islam Tambora. Peserta merupakan siswa yang berada pada fase akhir pendidikan menengah dan akan segera memasuki jenjang pendidikan tinggi maupun dunia kerja. Dengan karakteristik penggunaan teknologi digital yang aktif dalam aktivitas akademik dan sosial, kelompok ini menjadi sasaran strategis dalam penguatan literasi keamanan siber

sebagai bekal menghadapi dinamika interaksi digital yang semakin kompleks.

Tahap persiapan diawali dengan koordinasi antara tim fasilitator dan pihak sekolah, khususnya kepala sekolah, untuk menyampaikan tujuan, ruang lingkup, serta rencana pelaksanaan kegiatan sosialisasi. Koordinasi ini bertujuan memastikan

kesesuaian materi dengan kebutuhan siswa serta penjadwalan kegiatan yang tidak mengganggu aktivitas pembelajaran. Selain itu, pada tahap ini tim juga menyiapkan instrumen evaluasi berupa *pre-test* dan *post-test* serta materi presentasi yang kontekstual dengan isu keamanan digital terkini.



**Gambar 2.** Sambutan Baik dari Pihak Kepala Sekolah dan Guru.

Pihak kepala sekolah dan guru menyambut baik pelaksanaan kegiatan ini sebagai bagian dari penguatan literasi digital di lingkungan sekolah. Materi dan susunan acara sosialisasi turut diinformasikan secara terbuka kepada pihak sekolah dan guru agar terdapat keselarasan antara program pengabdian dan visi pembelajaran sekolah. Dukungan ini menunjukkan adanya kolaborasi positif antara perguruan tinggi dan sekolah dalam membangun kesadaran keamanan digital

bagi siswa.

Tahap sosialisasi diawali dengan pemberian kuis singkat sebagai *pre-test* untuk mengukur tingkat pemahaman awal peserta sebelum menerima materi. Setelah itu, fasilitator memulai pemaparan materi edukasi keamanan digital secara interaktif. Tujuan utama kegiatan ini adalah meningkatkan kesadaran dan membentuk perilaku digital yang lebih aman melalui pemahaman risiko serta praktik perlindungan data pribadi.



**Gambar 3.** Pemaparan Materi oleh Fasilitator.

Materi yang disampaikan mencakup berbagai ancaman siber yang relevan

dengan kehidupan sehari-hari siswa, seperti phishing melalui pesan atau email,

penipuan telepon, aplikasi palsu, penyalahgunaan OTP, serta investasi bodong. Selain itu, dipaparkan pula ancaman modern seperti QRIS palsu, RFID *skimming*, dan manipulasi konten menggunakan teknologi *deepfake*. Fasilitator memberikan panduan praktis

mengenai cara mengenali ciri-ciri serangan, mengelola kata sandi yang kuat, mengaktifkan autentikasi dua faktor, serta melindungi data pribadi agar terhindar dari kerugian finansial maupun penyalahgunaan identitas digital.



**Gambar 4.** Materi Sosialisasi.

Selama kegiatan berlangsung, siswa menunjukkan antusiasme yang tinggi. Hal ini terlihat dari keaktifan peserta dalam mengajukan pertanyaan, berdiskusi mengenai kasus nyata, mengikuti praktik dengan serius, serta berbagi pengalaman

pribadi terkait kejadian penipuan digital yang pernah mereka temui. Di akhir sesi, peserta juga memberikan umpan balik positif terhadap materi dan metode penyampaian yang dinilai relevan dengan kebutuhan mereka.



**Gambar 5.** Foto Kegiatan Sosialisasi.

Pada tahap evaluasi, peserta diminta kembali menjawab kuis sebagai *post-test* untuk mengukur perubahan pemahaman setelah mengikuti kegiatan. Evaluasi ini

dilakukan secara langsung untuk memastikan peningkatan pengetahuan dan kesadaran peserta terhadap praktik keamanan digital.

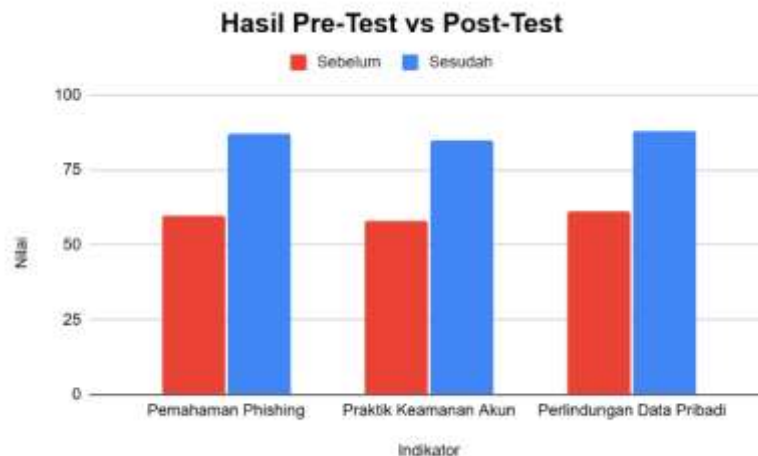


**Gambar 6.** Peserta Nilai *Post-Test* Tertinggi.

Sebagai bentuk apresiasi dan motivasi, diberikan penghargaan kepada

peserta dengan kombinasi nilai post-test tertinggi dan waktu pengerjaan tercepat. Pemberian apresiasi ini bertujuan

mendorong semangat belajar sekaligus memperkuat partisipasi aktif dalam kegiatan edukatif.



**Gambar 6.** Hasil *Pre-Test* dan *Post-Test*.

Berdasarkan hasil pengolahan data, rata-rata skor pre-test peserta adalah 60 dari skala 100. Setelah mengikuti sosialisasi, rata-rata skor post-test meningkat menjadi 88. Dari 11 peserta, sebanyak 10 siswa (90,9%) menunjukkan peningkatan skor di atas 20 poin, sementara 1 siswa menunjukkan peningkatan moderat. Hasil ini melampaui indikator keberhasilan yang telah ditetapkan dalam metode kegiatan, yaitu minimal 80% peserta mengalami peningkatan pemahaman. Secara umum,

data ini menunjukkan bahwa intervensi edukatif yang dilakukan efektif dalam meningkatkan literasi keamanan digital siswa.

Selain pengukuran kognitif melalui kuis, tim juga menyebarkan kuesioner evaluasi untuk menilai persepsi peserta terhadap keseluruhan kegiatan. Kuesioner diisi oleh seluruh 11 peserta dan mencakup aspek kejelasan materi, relevansi topik, metode penyampaian, serta manfaat kegiatan.

**Tabel 1.** Hasil Penilaian Evaluasi Kegiatan.

Aspek Penilaian	Sangat Baik	Baik	Cukup	Kurang
Kejelasan Materi	73%	27%	0	0
Relevansi Materi dengan Kebutuhan	82%	18%	0	0
Metode Penyampaian	64%	36%	0	0
Manfaat Kegiatan Secara Keseluruhan	82%	18%	0	0

Hasil kuesioner menunjukkan bahwa mayoritas peserta menilai kegiatan berada pada kategori sangat baik, terutama dalam aspek relevansi dan manfaat kegiatan. Hal ini mengindikasikan bahwa materi yang disampaikan sesuai dengan kebutuhan siswa serta mampu memberikan pemahaman yang aplikatif.

Peningkatan skor *pre-test* dan *post-test* yang signifikan menunjukkan bahwa

pendekatan partisipatif dan praktik langsung efektif dalam memperkuat literasi keamanan digital siswa. Hasil ini sejalan dengan temuan Arsyad et al. (2024) yang menunjukkan bahwa program literasi digital berbasis edukasi kontekstual mampu meningkatkan kesadaran remaja terhadap ancaman phishing. Demikian pula, Hendrawan et al. (2025) menegaskan bahwa intervensi edukatif yang disertai

evaluasi terstruktur dapat meningkatkan pemahaman siswa terkait keamanan siber secara signifikan. Pendekatan interaktif yang digunakan dalam kegiatan ini juga sejalan dengan Ayuningtyas et al. (2025) yang menekankan bahwa metode edukasi interaktif lebih efektif dalam membentuk kesadaran dan perubahan perilaku digital dibandingkan pendekatan satu arah.

Partisipasi aktif siswa dalam diskusi dan praktik turut memperkuat internalisasi konsep keamanan digital sehingga pemahaman tidak hanya bersifat teoritis, tetapi juga aplikatif. Hal ini didukung oleh Novantara & Suwandi (2025) yang menunjukkan bahwa pelatihan keamanan digital berbasis praktik mampu meningkatkan ketahanan digital siswa secara lebih komprehensif. Selain itu, Wijayanto et al. (2026) dalam kegiatan pelatihan dan simulasi serangan siber pada siswa SMK menemukan bahwa pengalaman langsung melalui simulasi dapat memperdalam pemahaman serta meningkatkan kesiapsiagaan terhadap potensi serangan digital.

Dukungan pihak sekolah dan kolaborasi antara fasilitator dan mitra juga menjadi faktor penting dalam keberhasilan kegiatan. Arifin et al. (2024) dan Wanayumini et al. (2025) menegaskan bahwa program pengabdian literasi digital yang melibatkan sinergi antara perguruan tinggi dan sekolah mampu membangun kesadaran keamanan digital secara lebih sistematis dan berkelanjutan. Dalam konteks ini, pendekatan partisipatif yang diterapkan juga konsisten dengan model penguatan literasi digital berbasis komunitas sebagaimana dikemukakan oleh Patria (2025), yang menekankan pentingnya keterlibatan aktif peserta dalam proses pembelajaran.

Secara keseluruhan, hasil kegiatan menunjukkan bahwa program edukasi keamanan siber ini efektif dalam meningkatkan kesadaran dan pemahaman siswa terhadap ancaman phishing serta praktik perlindungan data pribadi. Temuan

ini memperkuat urgensi penguatan literasi keamanan digital di tingkat pendidikan menengah sebagaimana diuraikan oleh Muhtada et al. (2025), Eriana et al. (2025), dan Wahyuni et al. (2025), yang menyatakan bahwa edukasi preventif merupakan langkah strategis dalam membangun ketahanan digital generasi muda di tengah meningkatnya kompleksitas ancaman siber. Dengan demikian, kegiatan ini tidak hanya memberikan dampak pada peningkatan skor evaluasi, tetapi juga berkontribusi pada penguatan budaya keamanan digital di lingkungan sekolah.

## **SIMPULAN DAN SARAN**

Kegiatan Pengabdian kepada Masyarakat berupa edukasi keamanan siber pada siswa kelas XII SMA Islam Tambora telah dilaksanakan secara sistematis melalui tahapan persiapan, sosialisasi, dan evaluasi dengan pendekatan partisipatif-edukatif. Pelaksanaan kegiatan menunjukkan bahwa kolaborasi yang baik antara tim fasilitator dan pihak sekolah menjadi faktor pendukung keberhasilan program. Hasil evaluasi kuantitatif memperlihatkan adanya peningkatan signifikan pada tingkat pemahaman peserta terkait konsep *phishing*, praktik keamanan akun, serta kesadaran terhadap perlindungan data pribadi. Rata-rata skor peserta meningkat dari 60 pada *pre-test* menjadi 88 pada *post-test*, dengan 90,9% peserta mengalami peningkatan skor di atas 20 poin. Capaian tersebut melampaui indikator keberhasilan yang telah ditetapkan dan menunjukkan bahwa pendekatan pembelajaran interaktif dan berbasis praktik efektif dalam memperkuat literasi keamanan digital siswa. Selain peningkatan aspek kognitif, respons positif peserta terhadap kejelasan materi, relevansi topik, serta metode penyampaian menunjukkan bahwa kegiatan ini tidak hanya meningkatkan pemahaman, tetapi juga membangun kesadaran dan sikap proaktif dalam menghadapi risiko digital.

Dengan demikian, program ini terbukti berkontribusi sebagai upaya preventif terhadap ancaman *phishing* sekaligus sebagai fondasi kesiapan digital bagi siswa yang berada pada fase transisi menuju pendidikan tinggi maupun dunia kerja.

Berdasarkan hasil tersebut, disarankan agar penguatan literasi keamanan digital tidak berhenti pada satu kegiatan sosialisasi, melainkan diintegrasikan secara berkelanjutan dalam program sekolah, baik melalui kegiatan pembinaan siswa, literasi digital berkala, maupun kolaborasi lanjutan dengan perguruan tinggi. Pengembangan program serupa dengan cakupan peserta yang lebih luas juga perlu dipertimbangkan untuk membangun budaya keamanan digital secara kolektif di lingkungan sekolah. Selain itu, pada implementasi selanjutnya, evaluasi dapat diperluas dengan pengukuran dampak jangka menengah untuk melihat keberlanjutan perubahan perilaku digital siswa. Melalui langkah-langkah tersebut, edukasi keamanan siber diharapkan menjadi bagian integral dari upaya membentuk generasi muda yang cakap, bertanggung jawab, dan tangguh dalam menghadapi dinamika ekosistem digital yang terus berkembang.

#### UCAPAN TERIMAKASIH

Penulis menyampaikan terima kasih kepada Kepala Sekolah dan seluruh Guru SMA Islam Tambora atas kesempatan dan dukungan yang diberikan dalam pelaksanaan kegiatan Pengabdian kepada Masyarakat ini. Dukungan tersebut sangat berarti bagi kelancaran dan keberhasilan kegiatan.

#### DAFTAR PUSTAKA

Arifin, M., Helmi, F., & Dharmawan, J. (2024). Peningkatan Literasi Digital Melalui Sosialisasi Pentingnya Pemahaman Kejahatan Siber Di Kalangan Pelajar SMAN 1 Gayam. *Rampa' Naong Jurnal Pengabdian Kepada Masyarakat*, 2(2), 1-7.

<https://doi.org/10.24929/rn.v2i2.3625>

Arsyad, A. A. J., Tamrin, U., Lande, J. P., & Umar, N. (2024). Meningkatkan Kesadaran Remaja Terhadap Phishing Melalui Literasi Digital: Studi Kasus di SMK Darussalam Makassar. *Jurnal Pengabdian Literasi Digital Indonesia*, 3(2), 60-71. <https://doi.org/10.57119/abdimas.v3i2.122>

Ayuningtyas, F., Sakti, M., & Nidatya, N. (2025). Peningkatan Kesadaran Literasi Digital Bagi Remaja Melalui Program Edukasi interaktif. *Jurnal Abdimas Ilmiah Citra Bakti*, 6(1), 201-212. <https://doi.org/10.38048/jailcb.v6i1.4442>

Eriana, E. S., Zein, A., Wati, F. E., & Buminata, M. S. A. (2025). Sosialisasi Keamanan Digital Untuk Mengatasi Phishing Dan Apk Berbahaya. *Attamkiim: Jurnal Pengabdian Masyarakat*, 2(1), 85-90. <https://doi.org/10.62070/attamkiim.v2i1.248>

Hendrawan, F. R., Rahma, D. W., Ramadhan, Y. Z., Siregar, S. D., Naufal, F., Marza, M., & Muhtar, A. Y. (2025). Peningkatan Literasi Digital dalam Keamanan Siber bagi Siswa SMK Telekomunikasi Telesandi Bekasi. *SOROT: Jurnal Pengabdian Kepada Masyarakat*, 4(2), 74-79. <https://doi.org/10.32699/sorot.v4i2.9534>

Isnawati, I., Zamhari, A., Yusuf, M., & Sujoko, I. (2021). Strengthening Digital Literacy toward Students in Facing Education Era 4.0. *Proceedings of the 3rd International Colloquium on Interdisciplinary Islamic Studies, ICIIS 2020, 20-21 October 2020, Jakarta, Indonesia*. Proceedings of the 3rd International Colloquium on Interdisciplinary

- Islamic Studies, ICIIS 2020, 20-21 October 2020, Jakarta, Indonesia. <https://doi.org/10.4108/eai.20-10-2020.2305174>
- Muhtada, D., Irawaty, I., & Puteri, D. S. (2025). Cybercrime Prevention for Students in TPQ Darul Muayyad Gunungpati. *Jurnal Panjar: Pengabdian Bidang Pembelajaran*, 5(2), 40-48. <https://doi.org/10.15294/panjar.v5i2.33509>
- Novantara, P., & Suwandi, F. F. (2025). Pelatihan Literasi Keamanan Digital dan Dasar Cyber Security untuk Siswa SMK sebagai Upaya Penguatan Ketahanan Digital Masyarakat. *Sinergi Dan Transformasi Dalam Pengabdian Kepada Masyarakat*, 1(2), 199-205. <https://doi.org/10.33020/sentraabdimas.v1i2.1007>
- Pane, C. G. G. (2021). EDUKASI KEPADA SISWA SMA NEGERI 1 MIMIKA UNTUK MENGATASI ANCAMAN MEDIA ONLINE PADA DATA PRIBADI. *KONSTELASI: Konvergensi Teknologi Dan Sistem Informasi*, 1(2), 412-418. <https://doi.org/10.24002/konstelasi.v1i2.4166>
- Patria, M. (2025). Improving Digital Literacy of The Elderly Through a Participation-Based Approach: Service Program at Bekasi Elderly School. *TAAWUN*, 5(01), 66-80. <https://doi.org/10.37850/taawun.v5i01.873>
- 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>
- Wahyuni, P., Candra, O., Utami, W. L., & Sari, F. W. (2025). Transformasi Pembelajaran Abad 21: Literasi Digital, Keamanan Siber, dan Etika Digital untuk Siswa SMA: Penelitian. *Jurnal Pengabdian Masyarakat Dan Riset Pendidikan*, 4(2), 12164-12170. <https://doi.org/10.31004/jerkin.v4i2.3622>
- Wanayumini, Muhammad Azwar Al Ayyub, Dini Farhatun, Triana Puspa Handayani, M Yoggi Saputra, & Mhd Fauzan Yafi. (2025). Pengabdian Masyarakat dalam Pengenalan Dunia Cyber untuk Membangun Kesadaran Literasi Digital Bagi Siswa SMA N 1 Ujung Padang: Pengabdian. *Jurnal Pengabdian Masyarakat Dan Riset Pendidikan*, 4(2), 7615-7619. <https://doi.org/10.31004/jerkin.v4i2.3054>
- Wijayanto, A., Abdillah, M. F., Maulidah, A. A., Maynardian, A., Madina, G. N., Wijaya, A., Gerungan, R. A. C., Najha, N., Ahsani, A. Z., Ramadhan, S. M., Triwahyudi, R. D., & Zistafa, E. R. (2026). Peningkatan Kesadaran Keamanan Siber Siswa SMK Melalui Pelatihan Dan Simulasi Serangan Dalam Lingkungan Virtual. *BERBAKTI: Jurnal Pengabdian Kepada Masyarakat*, 3(3), 278-285. <https://doi.org/10.30822/hj4rr981>