Sarwahita : Jurnal Pengabdian Kepada Masyarakat
DOI : doi.org/10.21009/sarwahita.231.7

Edukasi Keamanan Informasi untuk Mendukung Penguatan Literasi Digital Siswa SMA Negeri 8 Tangerang

Mega Kartika Sari[1*], Bhustomy Hakim[2], Evasaria Magdalena Sipayung[3], Marta Lenah Haryanti[4], Puguh Hiskiawan[5], Ozmar Azhari[6], Merryana Lestari[7], Gregorius Ivan Pamungkas Triwibowo[8]

Fakultas Teknologi dan Desain, Universitas Bunda Mulia, Kampus Serpong, Jl. Jalur Sutera Barat Kav. 7–9, Alam Sutera, Tangerang 15143, Indonesia

[*]*Corresponding Author Email*: *msari@bundamulia.ac.id

Received : 2 July 2026
Revised : 27 July 2026
Accepted : 30 July 2026
Online : 30 July 2026
Published : 30 July 2026

Sarwahita
Volume 23, Issue 1 (2026)
P-ISSN : 0216-7484
E-ISSN : 2597-8926

Abstract

The rapid development of digital technology has not been fully accompanied by adequate information security literacy among students. This condition makes students more vulnerable to cyber threats such as phishing, fake applications, and the risks associated with using public Wi-Fi networks. This community service program aimed to provide information security education to students of SMA Negeri 8 Tangerang as an effort to support the strengthening of digital literacy and awareness of information security risks in daily activities. The program was conducted in four sessions using an educational and participatory approach, covering network and Wi-Fi security, fake apps, phishing, as well as password management and authentication. Post-activity evaluation was carried out through questionnaires, discussions, and participant feedback to examine participants' responses regarding the relevance, clarity, usefulness, and level of engagement in the program. The evaluation results showed that 144 participants gave positive assessments of the program, with average scores above 3.60 on a scale of 1–4. These findings suggest that the participants perceived the materials as relevant, understandable, useful, and appropriate to their needs. Participant feedback also showed greater attention to digital security issues that are closely related to their daily lives. Overall, the program was well received and may support efforts to strengthen students' digital literacy, particularly in recognizing information security risks in everyday digital activities.

Keywords: *digital literacy; information security; cybersecurity education; phishing; fake apps*

A. PENDAHULUAN

Perkembangan teknologi digital membuat aktivitas siswa semakin banyak berlangsung melalui perangkat dan layanan daring. Dalam konteks ini, siswa tidak hanya menggunakan teknologi untuk mengakses materi pembelajaran, tetapi juga untuk berkomunikasi, mencari informasi, menggunakan media sosial, dan memanfaatkan berbagai aplikasi digital dalam kehidupan sehari-hari (UNESCO, 2023). Kondisi ini menunjukkan bahwa pelajar merupakan

DOI : doi.org/10.21009/sarwahita.231.7

kelompok pengguna teknologi yang aktif. Namun, kebiasaan menggunakan teknologi belum selalu diikuti dengan pemahaman yang cukup mengenai keamanan informasi (Shahbazi et al., 2025). Akibatnya, siswa dapat lebih mudah menghadapi risiko seperti phishing, aplikasi palsu, kebocoran data pribadi, penyalahgunaan akun, dan penggunaan jaringan Wi-Fi publik yang tidak aman.

Kebutuhan terhadap edukasi keamanan informasi juga didukung oleh tingginya angka ancaman siber di Indonesia. Tercatat adanya peningkatan 25% serangan siber dari 232,4 juta kasus pada 2018 menjadi 290,3 juta kasus pada 2019 (Anjani, 2021). Pada periode Januari–April 2020, terdapat sekitar 88 juta insiden siber yang meliputi *phishing*, *malware*, dan *information gathering* (Puspitasari et al., 2024). Sementara itu, pada 2022 dilaporkan sebanyak 164.131 kasus email phishing (Adipa et al., 2023). Data tersebut menunjukkan bahwa ancaman siber terus hadir dalam berbagai bentuk dan memerlukan respons yang tidak hanya bersifat teknis, tetapi juga edukatif. Oleh karena itu, penguatan literasi keamanan informasi di kalangan pelajar menjadi relevan sebagai bagian dari upaya membangun kesadaran digital sejak dini.

SMA Negeri 8 Tangerang sebagai mitra kegiatan memiliki peserta didik yang aktif menggunakan teknologi digital, baik untuk kepentingan belajar maupun aktivitas sosial. Dalam konteks tersebut, edukasi keamanan informasi menjadi penting karena siswa tidak hanya perlu mampu menggunakan teknologi, tetapi juga perlu memahami cara melindungi akun, data pribadi, dan aktivitas digital mereka. Materi edukasi perlu disusun berdasarkan situasi yang dekat dengan pengalaman siswa, misalnya penggunaan jaringan internet, pemasangan aplikasi, penerimaan pesan atau tautan, serta pengelolaan akun digital. Dengan cara ini, materi yang disampaikan tidak berhenti sebagai pengetahuan umum, tetapi dapat dikaitkan langsung dengan praktik digital yang mereka lakukan sehari-hari.

Kegiatan Pengabdian kepada Masyarakat ini dirancang sebagai program edukasi keamanan informasi yang berfokus pada empat topik utama, yaitu keamanan jaringan dan Wi-Fi publik, aplikasi palsu, *phishing*, serta manajemen kata sandi dan autentikasi. Keempat topik tersebut dipilih karena berkaitan langsung dengan aktivitas digital siswa, seperti penggunaan jaringan internet di ruang publik (Fatimah et al., 2022), pemasangan aplikasi pada perangkat pribadi yang dapat mengarahkan siswa pada aplikasi palsu (Nyakapu et al., 2021), penerimaan pesan atau tautan mencurigakan (Novitasari, 2025), serta pengelolaan akun digital (Fatimah et al., 2022; Nyakapu et al., 2021; Ramadhan et al., 2024).

Sejumlah kegiatan pengabdian terdahulu telah membahas literasi digital dan keamanan siber dalam berbagai konteks masyarakat (Andry et al., 2023; Hakim et al., 2025; Surbakti, 2024; Syafiih et al., 2024). Namun, kegiatan edukasi keamanan informasi pada pelajar masih perlu dikembangkan dalam bentuk yang lebih terstruktur, kontekstual, dan sesuai dengan pengalaman digital siswa. Program ini tidak hanya berfokus pada penyampaian materi, tetapi juga melibatkan evaluasi pascakegiatan melalui kuesioner, diskusi, dan umpan balik peserta. Evaluasi tersebut digunakan untuk mengetahui respons peserta terhadap relevansi, kejelasan, manfaat, dan keterlibatan dalam kegiatan, sekaligus menjadi dasar dalam merumuskan kebutuhan pengembangan program lanjutan.

DOI : doi.org/10.21009/sarwahita.231.7

Berdasarkan uraian tersebut, kegiatan ini difokuskan pada dua hal. Pertama, bagaimana program edukasi keamanan informasi dapat dirancang berdasarkan risiko digital yang dekat dengan aktivitas siswa. Kedua, bagaimana respons peserta terhadap pelaksanaan edukasi keamanan informasi yang diberikan melalui empat sesi kegiatan. Dengan demikian, artikel ini bertujuan menguraikan pelaksanaan program edukasi keamanan informasi di SMA Negeri 8 Tangerang, menjelaskan relevansi materi dengan kebutuhan peserta, serta menganalisis respons peserta terhadap kegiatan sebagai dasar pengembangan program literasi digital yang lebih aplikatif dan berkelanjutan.

B. TINJAUAN LITERATUR

Keamanan informasi merupakan upaya untuk melindungi data, sistem, dan aktivitas digital dari berbagai ancaman yang dapat merugikan pengguna (Lestari, 2024; Lestari et al., 2024). Dalam konteks penggunaan teknologi sehari-hari, keamanan informasi tidak hanya bergantung pada perangkat atau sistem, tetapi juga pada perilaku pengguna dalam menjaga data pribadi, mengelola akun, serta mengenali tanda-tanda ancaman digital. Lestari et al. (2025) menjelaskan bahwa keamanan informasi dipengaruhi oleh aspek teknologi, jaringan, dan pengelolaan informasi, sedangkan Nonum et al. (2025) menegaskan bahwa faktor manusia masih menjadi salah satu titik lemah utama dalam keamanan informasi, terutama ketika pengguna belum memiliki kesadaran yang cukup terhadap risiko digital dan teknik *social engineering*. Oleh karena itu, keamanan informasi menjadi bagian penting dari literasi digital, terutama bagi pelajar yang aktif menggunakan internet, media sosial, aplikasi mobile, dan berbagai layanan digital.

Literasi digital tidak hanya mencakup kemampuan menggunakan perangkat teknologi, tetapi juga kemampuan memahami risiko, menilai informasi, menjaga privasi, serta menggunakan teknologi secara aman dan bertanggung jawab. Dalam konteks pelajar, literasi digital perlu diarahkan pada kemampuan praktis yang dekat dengan kehidupan mereka. Siswa perlu memahami bahwa aktivitas seperti mengakses Wi-Fi publik, mengunduh aplikasi, membuka tautan dari pesan, dan menggunakan akun digital memiliki risiko keamanan yang perlu dikelola dengan baik.

Salah satu risiko yang dekat dengan aktivitas siswa adalah penggunaan jaringan Wi-Fi publik. Jaringan yang tidak aman dapat membuka peluang terjadinya pencurian data, penyadapan aktivitas, atau penyalahgunaan informasi pribadi. Fatimah et al. (2022) menunjukkan bahwa jaringan Wi-Fi yang rentan dapat dimanfaatkan dalam serangan seperti *packet sniffing*, sedangkan Agustina et al. (2025) mengingatkan bahwa penggunaan Wi-Fi publik tanpa perlindungan yang memadai dapat membuka peluang terjadinya kebocoran data. Karena itu, siswa perlu memahami bahwa tidak semua jaringan internet aman digunakan, terutama untuk aktivitas yang melibatkan data sensitif seperti login akun, transaksi, atau pengiriman informasi pribadi. Edukasi mengenai keamanan Wi-Fi publik menjadi penting agar siswa dapat lebih berhati-hati dalam memilih jaringan dan memahami langkah perlindungan dasar saat terhubung ke internet.

DOI : doi.org/10.21009/sarwahita.231.7

Selain risiko dari jaringan, aplikasi palsu juga menjadi ancaman yang perlu diperhatikan. Aplikasi palsu dapat dibuat menyerupai aplikasi resmi untuk menarik pengguna agar mengunduh dan memberikan akses ke data pribadi atau perangkat (Nyakapu et al., 2021). Ancaman ini berbahaya karena sering tidak mudah dibedakan oleh pengguna yang belum terbiasa memeriksa keaslian aplikasi. Oleh karena itu, siswa perlu dibekali pemahaman tentang cara memeriksa sumber aplikasi, nama pengembang, ulasan, jumlah unduhan, izin akses, dan tanda-tanda mencurigakan lainnya sebelum memasang aplikasi pada perangkat pribadi.

Phishing merupakan bentuk ancaman digital lain yang banyak memanfaatkan kelengahan pengguna. Serangan ini biasanya dilakukan melalui pesan, tautan, situs web, atau formulir palsu yang dirancang untuk memperoleh informasi sensitif seperti *username*, *password*, kode OTP, atau data pribadi (Novitasari, 2025). Dalam perkembangannya, modus *phishing* juga menjadi semakin kompleks karena didukung penggunaan teknologi berbasis AI yang membuat pesan penipuan tampak lebih meyakinkan. Siswa perlu mengetahui bahwa pesan yang terlihat meyakinkan sekalipun tetap perlu diperiksa, terutama jika meminta data pribadi, mengarahkan ke tautan tidak dikenal, atau memberikan tekanan untuk segera bertindak.

Aspek lain yang tidak kalah penting adalah pengelolaan kata sandi dan autentikasi. Ramadhan et al. (2024) menunjukkan bahwa penggunaan kata sandi yang lemah atau berulang masih menjadi salah satu penyebab tingginya risiko pembobolan akun. Chanda (2016) juga menekankan bahwa panjang dan tingkat keacakan kata sandi memiliki peran penting dalam meningkatkan keamanan akun, sehingga pengguna perlu didorong untuk menerapkan kata sandi yang kuat dan tidak digunakan ulang. Pada sisi lain, Nonum and Imianvan-Anthony (2025) menunjukkan bahwa penggunaan autentikasi berlapis, seperti OTP, *two-factor authentication,* dan *multi-factor authentication*, dapat menurunkan risiko akses tidak sah pada berbagai layanan digital. Dengan memahami praktik tersebut, siswa diharapkan dapat menerapkan kebiasaan digital yang lebih aman dalam penggunaan akun pribadi.

Dalam kerangka pengabdian kepada masyarakat, edukasi keamanan digital dapat dipahami sebagai bentuk pemberdayaan, karena kegiatan ini membantu peserta memahami risiko, membangun kewaspadaan, dan mengenali langkah-langkah pencegahan yang relevan dengan kehidupan sehari-hari. Penguatan kapasitas seperti ini penting terutama bagi pelajar, karena mereka berada pada tahap pembentukan kebiasaan dalam menggunakan teknologi. Kajian sebelumnya menunjukkan bahwa kegiatan edukasi keamanan digital memang dibutuhkan oleh masyarakat. Johal and Abdulsahib (2023); Nopriadi (2024), misalnya, menunjukkan bahwa sosialisasi mengenai keamanan data pribadi dan bahaya Wi-Fi publik diperlukan karena peserta belum sepenuhnya menyadari risiko penggunaan internet yang tidak aman. Namun, sebagian besar kegiatan sebelumnya masih membahas isu keamanan digital secara parsial. Berbeda dari itu, artikel ini menempatkan program edukasi dalam satu rangkaian yang mengintegrasikan empat topik yang saling berkaitan, yaitu Wi-Fi publik, aplikasi palsu, *phishing*, serta manajemen kata sandi dan autentikasi, disertai evaluasi berbasis kuesioner dan umpan balik peserta. Dengan demikian, tinjauan literatur ini mendukung posisi artikel bahwa penguatan literasi keamanan informasi pada pelajar perlu dilakukan melalui pendekatan yang kontekstual, terstruktur, dan dekat dengan pengalaman digital mereka.

DOI : doi.org/10.21009/sarwahita.231.7

C. METODE PELAKSANAAN

Kegiatan pengabdian kepada masyarakat ini dilaksanakan dengan pendekatan edukatif-partisipatif. Pendekatan edukatif digunakan karena kegiatan berfokus pada penyampaian pengetahuan dan pemahaman mengenai keamanan informasi. Sementara itu, pendekatan partisipatif digunakan karena peserta tidak hanya menjadi penerima materi, tetapi juga dilibatkan dalam diskusi, tanya jawab, dan pemberian umpan balik terhadap topik keamanan digital yang mereka anggap relevan. Pendekatan ini dipilih agar kegiatan tidak hanya bersifat penyuluhan satu arah, tetapi juga menjadi ruang pembelajaran yang sesuai dengan pengalaman digital peserta.

Sasaran kegiatan adalah siswa SMA Negeri 8 Tangerang yang aktif menggunakan internet, media sosial, dan berbagai perangkat digital dalam proses belajar maupun kegiatan lainnya. Kegiatan dirancang untuk memberikan pemahaman dasar mengenai keamanan informasi melalui topik-topik yang dekat dengan aktivitas siswa. Pelaksanaan program dibagi ke dalam lima tahap, yaitu analisis kebutuhan mitra, perancangan materi edukasi, pelaksanaan edukasi, evaluasi pascakegiatan, serta refleksi dan tindak lanjut program.

Analisis Kebutuhan Mitra

Tahap awal kegiatan dilakukan dengan mengidentifikasi kebutuhan mitra terkait edukasi keamanan informasi bagi siswa. Identifikasi kebutuhan dilakukan melalui diskusi awal dengan pihak sekolah dan kajian terhadap isu-isu keamanan digital yang relevan dengan aktivitas pelajar. Hasil identifikasi menunjukkan bahwa siswa membutuhkan edukasi yang berkaitan dengan risiko penggunaan Wi-Fi publik, aplikasi palsu, phishing, serta pengelolaan kata sandi dan autentikasi. Keempat isu tersebut dipilih karena dekat dengan aktivitas digital siswa dan berpotensi menimbulkan risiko apabila tidak dipahami dengan baik.

Perancangan Materi Edukasi

Berdasarkan hasil analisis kebutuhan, tim menyusun materi edukasi keamanan informasi ke dalam empat sesi utama. Materi disusun dengan memperhatikan karakteristik peserta sebagai siswa sekolah menengah, sehingga bahasa, contoh, dan ilustrasi yang digunakan dibuat sederhana, kontekstual, dan mudah dipahami. Selain memberikan pemahaman mengenai berbagai ancaman keamanan informasi, setiap materi juga dirancang untuk membekali peserta dengan langkah-langkah mitigasi yang dapat diterapkan dalam aktivitas digital sehari-hari.

Pada materi keamanan jaringan dan Wi-Fi publik, peserta diberikan pemahaman mengenai risiko penggunaan jaringan publik serta langkah pencegahan, seperti menghindari login ke akun penting melalui Wi-Fi publik, memastikan penggunaan situs dengan protokol HTTPS, menonaktifkan fitur *auto-connect*, serta memanfaatkan *Virtual Private Network* (VPN) ketika diperlukan.

Pada materi aplikasi palsu (*fake apps)*, peserta diajarkan cara mengidentifikasi aplikasi resmi dengan memeriksa identitas pengembang (developer), jumlah unduhan, ulasan pengguna, izin akses aplikasi, serta hanya mengunduh aplikasi melalui toko aplikasi resmi.

Pada materi *phishing*, peserta diberikan contoh berbagai bentuk pesan, tautan, maupun situs palsu yang sering digunakan pelaku kejahatan siber. Peserta juga dilatih mengenali

DOI : doi.org/10.21009/sarwahita.231.7

karakteristik *phishing* melalui pemeriksaan alamat URL, identitas pengirim, permintaan data pribadi, serta teknik verifikasi sebelum membuka tautan atau memberikan informasi sensitif.

Pada materi manajemen kata sandi dan autentikasi, peserta dibimbing untuk menerapkan praktik keamanan akun melalui penggunaan kata sandi yang kuat dan unik pada setiap layanan digital, menghindari penggunaan kata sandi yang sama pada berbagai akun, serta mengaktifkan *multi-factor authentication* (MFA) sebagai lapisan keamanan tambahan.

Pelaksanaan Edukasi

Tahap pelaksanaan dilakukan secara tatap muka melalui empat sesi edukasi. Setiap sesi memiliki fokus materi yang berbeda agar pembelajaran berlangsung terstruktur dan bertahap. Metode yang digunakan meliputi pemaparan materi, diskusi, tanya jawab, pembahasan contoh kasus, serta demonstrasi sederhana mengenai berbagai ancaman keamanan informasi.

Pada setiap sesi, peserta tidak hanya menerima penjelasan teoritis, tetapi juga diajak menganalisis contoh kasus yang sering ditemui dalam kehidupan sehari-hari. Misalnya, peserta diminta membedakan situs web asli dan situs *phishing*, mengidentifikasi karakteristik aplikasi resmi dan aplikasi palsu berdasarkan informasi pada toko aplikasi, mengevaluasi keamanan penggunaan jaringan Wi-Fi publik, serta menyusun contoh kata sandi yang memenuhi prinsip keamanan informasi. Pendekatan tersebut diharapkan mampu meningkatkan kemampuan peserta dalam mengenali potensi ancaman sekaligus menerapkan langkah-langkah pencegahan yang sesuai ketika menggunakan layanan digital. Alur kegiatan edukasi keamanan informasi yang mencakup tahap analisis kebutuhan, perancangan materi, pelaksanaan edukasi, evaluasi, serta refleksi dan tindak lanjut program ditampilkan pada Gambar 1.

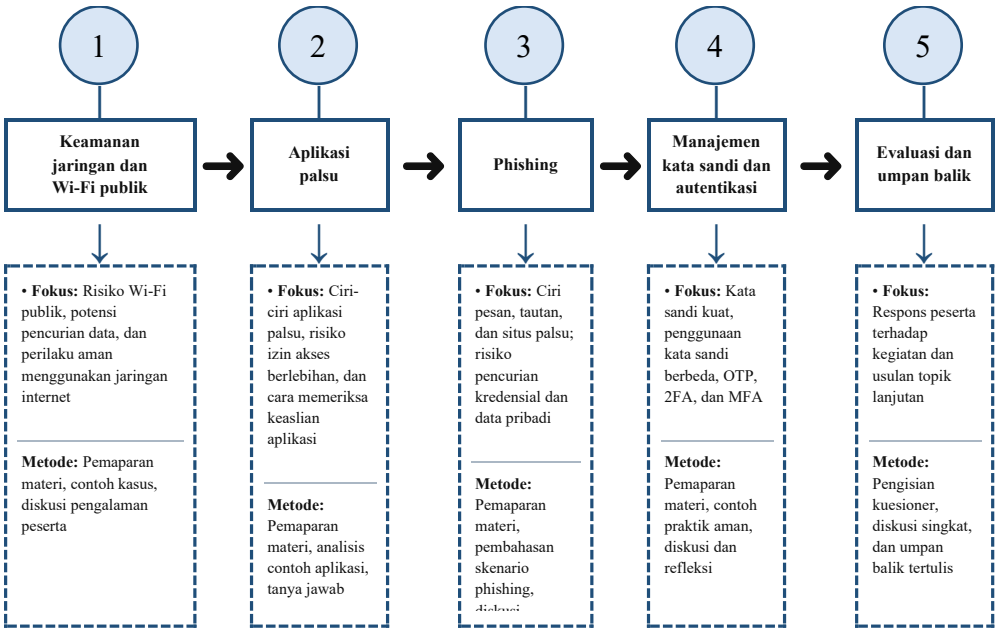
Evaluasi Pascakegiatan

Evaluasi dilakukan setelah seluruh rangkaian edukasi selesai dilaksanakan. Evaluasi bertujuan mengetahui respons peserta terhadap pelaksanaan kegiatan, terutama terkait relevansi materi, kejelasan penyampaian, manfaat kegiatan, dan keterlibatan peserta. Instrumen evaluasi berupa kuesioner dengan skala 1–4, diskusi singkat, dan umpan balik tertulis dari peserta. Aspek yang dinilai meliputi edukatif, objektif, akuntabel, dan transparan. Aspek edukatif digunakan untuk menilai manfaat kegiatan bagi peserta. Aspek objektif digunakan untuk menilai kesesuaian materi dengan kebutuhan peserta. Aspek akuntabel digunakan untuk menilai kejelasan penyampaian materi. Aspek transparan digunakan untuk menilai keterlibatan peserta dalam kegiatan.

Refleksi dan Tindak Lanjut Program

Tahap refleksi dan tindak lanjut dilakukan dengan menelaah hasil kuesioner, diskusi, dan umpan balik tertulis dari peserta. Hasil evaluasi digunakan untuk mengidentifikasi kekuatan kegiatan, aspek yang masih perlu diperbaiki, serta topik lanjutan yang dianggap relevan oleh peserta. Masukan peserta kemudian dikelompokkan ke dalam beberapa tema, seperti keamanan aplikasi dan situs web, *malware*, ancaman digital terkini, kecerdasan buatan, serta keamanan sistem dan perilaku pengguna. Hasil pengelompokan tersebut menjadi dasar dalam merumuskan rekomendasi kegiatan lanjutan yang lebih aplikatif, seperti simulasi identifikasi phishing, latihan mengevaluasi keamanan aplikasi, dan pembahasan contoh ancaman digital yang dekat dengan pengalaman siswa.

DOI : doi.org/10.21009/sarwahita.231.7



D. HASIL DAN PEMBAHASAN

Pelaksanaan Program Edukasi Keamanan Informasi

Kegiatan edukasi keamanan informasi di SMA Negeri 8 Tangerang dilaksanakan sebagai upaya mendukung penguatan literasi digital siswa, khususnya dalam memahami risiko keamanan informasi yang dekat dengan aktivitas digital sehari-hari. Program ini dirancang berdasarkan kebutuhan siswa sebagai pengguna aktif internet, media sosial, aplikasi digital, dan perangkat pribadi. Oleh karena itu, materi yang disampaikan tidak hanya berfokus pada konsep keamanan informasi secara umum, tetapi juga diarahkan pada contoh ancaman yang mudah ditemui oleh siswa.

Pelaksanaan kegiatan dibagi ke dalam empat sesi utama. Sesi pertama membahas keamanan jaringan dan Wi-Fi publik, dengan penekanan pada risiko penggunaan jaringan internet yang tidak aman. Sesi kedua membahas aplikasi palsu, termasuk ciri-ciri aplikasi tidak resmi dan risiko pemberian izin akses secara sembarangan. Sesi ketiga membahas *phishing*, terutama melalui pesan, tautan, dan situs palsu yang bertujuan memperoleh data pribadi atau kredensial pengguna. Sesi keempat membahas manajemen kata sandi dan autentikasi, termasuk pentingnya penggunaan kata sandi kuat dan autentikasi berlapis.

Dokumentasi pelaksanaan kegiatan ditampilkan pada Gambar 2 dan Gambar 3. Gambar 2 menunjukkan penyampaian materi melalui demonstrasi langsung mengenai praktik penggunaan layanan digital secara aman. Gambar 3 menampilkan suasana diskusi ketika peserta membahas hal-hal yang perlu diperhatikan saat mengakses halaman digital. Selama kegiatan berlangsung, peserta tidak hanya menerima materi, tetapi juga diberi kesempatan untuk bertanya, menyampaikan pengalaman, dan memberikan tanggapan terhadap isu

DOI : doi.org/10.21009/sarwahita.231.7

keamanan digital yang mereka temui dalam kehidupan sehari-hari. Bentuk keterlibatan ini penting karena keamanan informasi tidak hanya berkaitan dengan pengetahuan teknis, tetapi juga dengan kebiasaan dan pengambilan keputusan pengguna saat berinteraksi dengan teknologi. Dengan demikian, kegiatan ini diarahkan sebagai proses edukasi yang kontekstual dan sesuai dengan kebutuhan siswa.

(a) (b)

Gambar 2. (a) Penyampaian Materi Edukasi Keamanan Informasi kepada Peserta; (b) Sesi Diskusi dan Tanya Jawab Bersama Peserta Kegiatan

Evaluasi Respons Peserta terhadap Kegiatan

Evaluasi kegiatan dilakukan terhadap 144 peserta melalui kuesioner pascakegiatan. Penilaian difokuskan pada empat aspek, yaitu edukatif, objektif, akuntabel, dan transparan. Keempat aspek tersebut digunakan untuk melihat bagaimana peserta menilai manfaat kegiatan, kesesuaian materi dengan kebutuhan, kejelasan penyampaian, serta keterlibatan peserta dalam pelaksanaan program.

Berdasarkan Tabel 1, seluruh komponen memperoleh nilai rata-rata di atas 3,60 pada skala 1–4. Hasil ini menunjukkan bahwa kegiatan memperoleh respons positif dari peserta dan dinilai relevan sebagai upaya edukasi keamanan informasi di lingkungan sekolah. Nilai tertinggi terdapat pada aspek edukatif, yaitu 3,75. Temuan ini menunjukkan bahwa peserta menilai materi yang diberikan bermanfaat dan berkaitan dengan kebutuhan mereka sebagai pengguna teknologi digital. Topik seperti *phishing*, aplikasi palsu, Wi-Fi publik, dan pengelolaan kata sandi merupakan isu yang dekat dengan pengalaman siswa dalam menggunakan internet, media sosial, dan aplikasi digital (Shahbazi et al., 2025).

Aspek akuntabel memperoleh nilai rata-rata 3,71. Hasil ini menunjukkan bahwa peserta menilai materi telah disampaikan dengan cukup jelas dan mudah dipahami. Hal ini penting karena topik keamanan informasi sering kali memiliki istilah teknis yang tidak selalu mudah dipahami oleh siswa (Resch et al., 2024). Dengan penyampaian yang sederhana dan disertai contoh yang dekat dengan kehidupan sehari-hari, materi dapat lebih mudah diterima oleh peserta.

Aspek objektif memperoleh nilai rata-rata 3,67. Nilai ini menunjukkan bahwa materi dinilai sesuai dengan kondisi dan persoalan yang dihadapi peserta dalam aktivitas digital mereka. Kesesuaian materi dengan kebutuhan peserta menjadi salah satu faktor penting dalam

DOI : doi.org/10.21009/sarwahita.231.7

keberhasilan kegiatan edukasi, karena siswa akan lebih mudah memahami materi ketika contoh yang diberikan berkaitan langsung dengan pengalaman mereka.

Sementara itu, aspek transparan memperoleh nilai rata-rata 3,65. Meskipun masih berada pada kategori tinggi, aspek ini memiliki nilai paling rendah dibandingkan komponen lainnya. Temuan ini menunjukkan bahwa bentuk keterlibatan peserta masih dapat ditingkatkan pada kegiatan berikutnya. Program lanjutan dapat dikembangkan dengan metode yang lebih aplikatif, seperti simulasi identifikasi tautan *phishing*, latihan membedakan aplikasi resmi dan palsu, kuis interaktif, atau studi kasus keamanan digital yang lebih dekat dengan pengalaman siswa. Dengan demikian, peserta tidak hanya memahami materi, tetapi juga berlatih mengambil keputusan dalam situasi digital yang menyerupai kondisi nyata.

Tabel 1. Ringkasan Evaluasi Kuesioner Kegiatan

No	Komponen Penilaian	Rata-rata
1	Edukatif: kegiatan memberikan manfaat dan menjawab kebutuhan peserta	3,75
2	Objektif: materi sesuai dengan kondisi dan masalah yang dihadapi peserta	3,67
3	Akuntabel: materi disampaikan dengan jelas dan dapat dipahami oleh peserta	3,71
4	Transparan: peserta dilibatkan secara aktif dalam pelaksanaan kegiatan	3,65

Umpan Balik Peserta dan Kebutuhan Pengembangan Materi

Selain evaluasi kuantitatif, kegiatan ini juga menghasilkan umpan balik kualitatif dari peserta. Umpan balik tersebut memberikan gambaran mengenai topik keamanan digital lain yang dianggap penting oleh siswa untuk dibahas pada kegiatan berikutnya. Masukan peserta menunjukkan bahwa kebutuhan literasi keamanan informasi tidak hanya terbatas pada materi dasar, tetapi juga berkembang mengikuti perubahan ancaman digital yang mereka temui dalam kehidupan sehari-hari. Ringkasan tema masukan peserta disajikan pada Tabel 2.Tabel 2 menunjukkan bahwa peserta memiliki perhatian terhadap isu keamanan digital yang lebih luas. Topik seperti *malware*, *deepfake*, keamanan aplikasi, dan risiko penggunaan kecerdasan buatan menunjukkan bahwa siswa menyadari adanya ancaman digital yang terus berkembang. Hal ini menjadi temuan penting karena menunjukkan bahwa kegiatan edukasi tidak hanya memberikan informasi kepada peserta, tetapi juga memunculkan kesadaran awal terhadap kebutuhan belajar lanjutan.

Masukan peserta tersebut dapat menjadi dasar untuk merancang program pengabdian berikutnya. Kegiatan lanjutan sebaiknya tidak hanya berupa pemaparan materi, tetapi juga melibatkan simulasi dan praktik sederhana. Misalnya, peserta dapat diberikan contoh tautan atau pesan mencurigakan untuk dianalisis, contoh aplikasi untuk diperiksa keasliannya, atau skenario penggunaan Wi-Fi publik untuk didiskusikan bersama. Dengan pendekatan seperti itu, penguatan literasi digital dapat dilakukan secara lebih aplikatif dan berkelanjutan.

DOI : doi.org/10.21009/sarwahita.231.7

Tabel 2. Tema Masukan Peserta untuk Kegiatan Lanjutan

No	Tema	Rangkuman Usulan Topik dari Peserta
1	Keamanan aplikasi dan situs web	Bahaya situs yang tidak terenkripsi, keamanan aplikasi resmi dan palsu, serta risiko pada aplikasi gim dan streaming
2	Malware dan perlindungan perangkat	Pentingnya antivirus, cara membedakan file asli dan malware, serta risiko mod atau executor pada gim
3	Ancaman digital terkini	Deepfake, iklan berbahaya, pop-up, phishing, dan ancaman siber pada sistem operasi
4	Kecerdasan buatan	Manfaat dan risiko penggunaan AI serta deteksi AI yang tidak terpercaya
5	Keamanan sistem dan perilaku pengguna	Keamanan sistem Windows dan langkah perlindungan diri saat menggunakan teknologi sehari-hari

Refleksi dan Implikasi Kegiatan

Hasil kegiatan menunjukkan bahwa edukasi keamanan informasi bagi siswa sekolah menengah lebih mudah diterima ketika materi dikaitkan dengan situasi yang mereka temui dalam aktivitas digital sehari-hari. Topik seperti phishing, aplikasi palsu, Wi-Fi publik, dan pengelolaan kata sandi menjadi relevan karena siswa sering berhadapan dengan pesan digital, tautan, halaman login, aplikasi, dan akun pribadi (Pohan et al., 2025). Melalui contoh kasus, demonstrasi langsung, serta diskusi, peserta dapat melihat bahwa keamanan informasi bukan hanya persoalan teknis, tetapi juga berkaitan dengan kebiasaan dalam menggunakan layanan digital.

Selama pelaksanaan kegiatan, peserta tidak hanya menerima penjelasan mengenai jenis-jenis ancaman, tetapi juga diajak memperhatikan hal-hal sederhana yang sering diabaikan, seperti memastikan alamat situs, tidak membagikan informasi akun, berhati-hati terhadap tautan yang diterima, dan mempertimbangkan izin akses aplikasi sebelum digunakan. Hal ini menunjukkan bahwa edukasi keamanan informasi perlu diarahkan pada pembentukan kewaspadaan dan kebiasaan aman, bukan hanya pada pengenalan istilah atau konsep.

Dari hasil evaluasi, kegiatan memperoleh respons positif dari peserta. Namun, nilai aspek transparan yang lebih rendah dibandingkan aspek lainnya menunjukkan bahwa keterlibatan peserta masih dapat ditingkatkan. Pada kegiatan berikutnya, metode yang digunakan dapat dibuat lebih aktif melalui simulasi identifikasi phishing, latihan membedakan aplikasi resmi dan palsu, kuis berbasis kasus, atau diskusi kelompok mengenai contoh ancaman digital yang dekat dengan kehidupan siswa. Pendekatan tersebut dapat membantu peserta tidak hanya memahami materi, tetapi juga berlatih mengambil keputusan dalam situasi digital yang lebih nyata.

Secara umum, kegiatan ini dapat menjadi model awal edukasi keamanan informasi bagi siswa sekolah menengah. Model ini dimulai dari identifikasi kebutuhan peserta, pemilihan materi berdasarkan risiko digital yang dekat dengan siswa, pelaksanaan edukasi dalam sesi tematik, evaluasi respons peserta, dan perumusan topik lanjutan berdasarkan masukan yang

DOI : doi.org/10.21009/sarwahita.231.7

diberikan. Dengan alur tersebut, kegiatan pengabdian dapat dikembangkan menjadi program literasi digital yang lebih berkelanjutan dan tidak berhenti pada satu kali sosialisasi.

Keterbatasan Kegiatan

Kegiatan ini memiliki keterbatasan pada aspek pengukuran dampak. Evaluasi yang dilakukan masih berfokus pada respons dan persepsi peserta setelah kegiatan, sehingga belum dapat menunjukkan peningkatan literasi keamanan informasi secara kuantitatif. Kegiatan ini belum menggunakan instrumen *pre-test* dan *post-test* untuk membandingkan pemahaman peserta sebelum dan sesudah edukasi. Oleh karena itu, hasil kegiatan lebih tepat dimaknai sebagai gambaran keterterimaan program, persepsi manfaat, dan potensi dukungan terhadap penguatan literasi digital siswa.

Keterbatasan lainnya adalah bentuk kegiatan yang masih dominan berupa pemaparan materi, diskusi, dan tanya jawab. Meskipun metode tersebut mampu memberikan pemahaman awal kepada peserta, kegiatan lanjutan perlu dikembangkan dengan aktivitas yang lebih aplikatif, seperti simulasi kasus, latihan identifikasi tautan *phishing*, analisis aplikasi palsu, dan praktik pengelolaan akun yang aman. Dengan pengembangan tersebut, dampak kegiatan dapat diamati secara lebih konkret dan terukur.

E. KESIMPULAN

Kegiatan pengabdian kepada masyarakat yang dilaksanakan di SMA Negeri 8 Tangerang memperoleh respons positif dari 144 peserta berdasarkan hasil evaluasi pascakegiatan. Seluruh aspek penilaian memperoleh skor rata-rata di atas 3,60 pada skala 1–4, yaitu aspek edukatif (3,75), akuntabel (3,71), objektif (3,67), dan transparan (3,65). Hasil tersebut menunjukkan bahwa materi yang diberikan dinilai bermanfaat, relevan dengan kebutuhan peserta, mudah dipahami, serta mampu melibatkan peserta secara aktif selama pelaksanaan kegiatan.

Edukasi yang mencakup keamanan Wi-Fi publik, aplikasi palsu, *phishing*, serta manajemen kata sandi dan autentikasi menunjukkan bahwa pendekatan edukatif-partisipatif mampu meningkatkan keterterimaan materi keamanan informasi pada siswa. Penyampaian materi yang dikaitkan dengan aktivitas digital sehari-hari memudahkan peserta memahami berbagai bentuk ancaman serta langkah-langkah dasar untuk mengurangi risiko keamanan informasi.

Umpan balik peserta menunjukkan adanya kebutuhan terhadap materi lanjutan mengenai keamanan aplikasi dan situs web, malware, ancaman digital terkini seperti deepfake, pemanfaatan kecerdasan buatan, serta keamanan sistem dan perilaku pengguna. Temuan tersebut menunjukkan bahwa kebutuhan literasi keamanan informasi pada pelajar terus berkembang mengikuti dinamika ancaman siber sehingga program edukasi serupa perlu dilaksanakan secara berkelanjutan dengan pendekatan yang lebih aplikatif melalui simulasi, studi kasus, dan latihan identifikasi ancaman digital.

Program edukasi tidak hanya memberikan pemahaman konseptual, tetapi juga membekali peserta dengan langkah-langkah mitigasi sederhana, seperti mengenali indikasi phishing, memilih aplikasi dari sumber resmi, menggunakan kata sandi yang kuat, serta menerapkan autentikasi berlapis dalam penggunaan layanan digitalSecara makro, kemitraan global UNJ-

WMSU ini memberikan kontribusi spesifik dalam memperkuat ketahanan sistem pendidikan Islam dan menjembatani hambatan kultural konvensional, sehingga menjadikannya model strategis yang layak direplikasi pada wilayah dengan tantangan sosial-budaya serupa. Temuan program ini menegaskan bahwa kendala struktural dan kultural — seperti keterbatasan sarana prasarana serta dominasi metode konvensional — dapat dijembatani melalui peningkatan kapasitas sumber daya manusia yang terstruktur dan berkelanjutan.

F. DAFTAR PUSTAKA

Adipa, M., Zy, A. T., Effendi, M., & Korespondensi, P. (2023). Klasifikasi Email Phishing Menggunakan Algoritma K-Nearest Neighbor. *Jurnal RESTIKOM: Riset Teknik Informatika dan Komputer.* https://doi.org/10.52005/restikom.v5i2.152

Agustina, D., Aulia, M. R., & Afriandi, N. (2025). Pengenalan Ancaman dan Pencegahan Serangan Siber Melalui Edukasi Keamanan Jaringan Wi-Fi dan Internet. *Menulis: Jurnal Penelitian Nusantara*, *1*(12), 643-649. https://doi.org/10.59435/menulis.v1i12.835

Andry, J. F., Wijaya, A., Bernanda, D. Y., Geasela, Y. M., Yusup, C. R., Chandra, J. C., & Alexandre, J. (2023). Kebijakan Keamanan Teknologi Informasi pada Perangkat Keras di Perusahaan Distributor Sepatu. *Jurnal Pengabdian Dan Kewirausahaan*, *7*(2).

Anjani, N. H. (2021). Cybersecurity Protection in Indonesia. *In Center for Indonesian Policy Studies: Center for Indonesian Policy Studies.* https://doi.org/10.35497/341779

Chanda, K. (2016). Password Security: An Analysis of Password Strengths and Vulnerabilities. *International Journal of Computer Network and Information Security*, *8*, 23-30. https://doi.org/10.5815/ijcnis.2016.07.04

Fatimah, F., Mary, T., & Pernanda, A. Y. (2022). Analisis Keamanan Jaringan Wi-Fi Terhadap Serangan Packet Sniffing di Universitas PGRI Sumatera Barat. *JURTEII: Jurnal Teknologi Informasi*, *1*(2), 7-11. https://doi.org/10.22202/jurteii.2022.5707

Hakim, B., Lestari, M., Geasela, Y. M., Chandra, M. M. D., & Wendy, A. (2025). Mengenal UI/UX: Kolaborasi Kreativitas dan Teknologi dalam Desain Mobile Interface. *Jurnal Pengabdian dan Kewirausahaan*, *9*(2).

Johal, A. B., & Abdulsahib, A. (2023). Anatomy of Network Security Execution through Utilizing SPSS to Evaluate Public Wi-Fi. *Asia-Pacific Journal of Information Technology and Multimedia*. https://doi.org/10.17576/apjitm-2023-1201-06

Lestari, D. P. (2024). Factors Affecting Security Information Systems : Information Security, Threats and Cyber Attack, Physical Security, and Information Technology. *IJIIS: International Journal of Informatics and Information Systems*. https://doi.org/10.47738/ijiis.v7i1.193

Lestari, M., Puspita, M. E., Geasela, Y., Wijaya, A. F., Hiskiawan, P., & Vicky, V. (2025). Assessing Information Security Readiness in Indonesian Fintech Companies Using KAMI Index 5.0 Framework. *CogITo Smart Journal*, *11*(2), 271-280.

Lestari, M., Puspita, M. E., & Wijaya, A. F. (2024). Model Tata Kelola TI Terintegrasi untuk Keamanan Informasi di Sektor Fintech. *Jurnal Teknologi Dan Manajemen Industri Terapan*, *3*(3), 766-776.

Nonum, E., Avwokuruaye, O., & Umar, A. M. (2025). Social Engineering: Understanding Human Factors in Cyber Security. *International Journal of Convergent and Informatics Science Research*. https://doi.org/10.70382/hijcisr.v07i9.032

Nonum, E., & Imianvan-Anthony, P. (2025). A Comparative Analysis of Multi-Factor Authentication Methods for Enhanced Online Security. *International Journal of Science Research and Technology*. https://doi.org/10.70382/tijsrat.v07i9.046

Nopriadi. (2024). Menjaga Privasi Digital: Studi Tentang Kesadaran Mahasiswa dalam Perlindungan Data Pribadi di Media Sosial. *Polygon: Jurnal Ilmu Komputer dan Ilmu Pengetahuan Alam*. https://doi.org/10.62383/polygon.v2i6.297

Novitasari, U. (2025). Phishing Berbasis AI sebagai Serangan Social Engineering: Ancaman Baru di Dunia Keamanan Siber. *Jurnal Ilmu Hukum*, *14*, 154-171. https://doi.org/10.30652/h9g1cd34

Nyakapu, R., Sandela, N., Ram, V., Nuthikattu, P., & Madala, P. (2021). Analysis of Fake Apps in Android Environment. *International Journal of Creative Research Thoughts (IJCRT)*, *9*(5).

Pohan, S., Mardivta, H., & Damanik, R. S. (2025). Program Sosialisasi Keamanan Email Akademik Mahasiswa Terhadap Ancaman Phishing Berbasis Social Engineering. *Sevaka : Hasil Kegiatan Layanan Masyarakat,* 1(4). https://doi.org/10.62027/sevaka.v1i4.528

Puspitasari, D., Manajemen, S. T., & Mercusuar, I. K. (2024). Digital Risks in Emerging Economies: Cyber Threat Escalation in Indonesia (2020–2023). *Data : Journal of Information Systems and Management*. https://doi.org/10.61978/data.v2i3.697

Ramadhan, M. A., Arpinda, A., Saputra, D., & Mulyana, D. I. (2024). Pencegahan Serangan Berbasis Kata Sandi: Studi Komprehensif Tentang Implementasi Hash Pada Aplikasi Web. *INTECOMS J. Inf. Technol. Comput. Sci*, *7*(3), 920-925. https://doi.org/10.31539/intecoms.v7i3

Resch, C., Gardner-McCune, C., & Wintjen, K. (2024, 2024-02-06). Cross-Sectional Survey of CS Students' Knowledge of and Attitudes Toward Cybersecurity.

Surbakti, F. (2024). Edukasi Keamanan Siber Berdigital dengan Aman. *Prima Abdika: Jurnal Pengabdian Masyarakat*. https://doi.org/10.37478/abdika.v4i4.4967

Syafiih, M., Nadiyah, Khairi, M., Furqan, M., & Yusman, B. (2024). Pendampingan Literasi Digital untuk Mengurangi Risiko Kejahatan Siber Membentuk Masyarakat yang Lebih Aman. *JILPI : Jurnal Ilmiah Pengabdian dan Inovasi*. https://doi.org/10.57248/jilpi.v2i4.456

UNESCO. (2023). Global education monitoring report, 2023: technology in education: a tool on whose terms? In: UNESCO.

Shahbazi, Z., Jalali, R., & Molaeevand, M. (2025). AI-Based Phishing Detection and Student Cybersecurity Awareness in the Digital Age. *Big Data Cogn. Comput.*, *9*, 210. https://doi.org/10.3390/bdcc9080210