

Sosialisasi Cyber Security Awareness: Mitigasi Phishing dan Pengamanan Akun Digital bagi Siswa SMA/SMK

Hendy Prasetyo¹, Kameliani², Wildan^{*3}, Andi Rasya⁴, Argiyo Prasetyo Tutu⁵

^{1,5}Program Studi Teknik Komputer, Fakultas Teknik, Universitas Negeri Gorontalo

²Program Studi Pendidikan Matematika, Fakultas MIPA, Universitas Negeri Gorontalo

^{3,4}Program Studi Teknik Elektro, Fakultas Teknik, Universitas Negeri Gorontalo

e-mail: hendy@ung.ac.id¹, kamelianimath@ung.ac.id², *wildanteknik@ung.ac.id³

Article history

Received: 06-04-2026

Accepted: 30-05-2026

Published: 30-05-2026

Abstrak

Meluasnya akses internet di Indonesia menempatkan siswa SMA/SMK sebagai pengguna digital paling aktif sekaligus paling rentan terhadap ancaman *phishing* dan pembajakan akun digital. Kesenjangan antara kecakapan teknis dan kesadaran keamanan digital di kalangan remaja menjadi persoalan yang mendesak untuk ditangani secara terstruktur. Kegiatan pengabdian ini bertujuan meningkatkan *cyber security awareness* siswa SMAN 1 Limboto, Kabupaten Gorontalo, melalui sosialisasi yang berfokus pada tiga aspek utama: pengenalan dan mitigasi serangan *phishing*, pengamanan akun digital melalui autentikasi dua faktor (2FA), serta penerapan prinsip privasi data dalam aktivitas daring sehari-hari. Kegiatan dilaksanakan menggunakan metode ceramah interaktif berbasis studi kasus nyata yang relevan dengan kehidupan digital remaja, dilengkapi sesi demonstrasi langsung dan diskusi tanya jawab. Evaluasi dilakukan melalui kuis interaktif yang mengukur tingkat pemahaman siswa sebelum dan sesudah sosialisasi. Hasil menunjukkan peningkatan rata-rata sebesar 58 poin persentase di seluruh indikator pemahaman, dari rata-rata 33% sebelum sosialisasi menjadi 91% setelah sosialisasi, dengan peningkatan tertinggi pada indikator pengetahuan 2FA sebesar 63 poin persentase. Kegiatan ini membuktikan bahwa pendekatan sosialisasi berbasis konteks kehidupan digital remaja lebih efektif dalam membangun kesadaran keamanan siber dibandingkan pendekatan teknis yang bersifat generik, sekaligus berkontribusi dalam membentuk generasi muda yang tidak sekadar cakap secara teknologi, tetapi juga aman secara digital.

Kata kunci: autentikasi dua faktor; *cyber security awareness*; literasi digital; pengamanan akun digital; *phishing*

Abstract

The widespread internet access in Indonesia has positioned senior high school and vocational students as the most active digital users while simultaneously making them the most vulnerable group to phishing attacks and digital account hijacking. The gap between technical proficiency and digital security awareness among adolescents has become an urgent issue requiring structured intervention. This community service activity aimed to enhance the cyber security awareness of students at SMAN 1 Limboto, Gorontalo Regency, through socialization focusing on three main aspects: phishing identification and mitigation, digital account security through Two-Factor Authentication (2FA), and data privacy principles in daily online activities. The activity employed an interactive lecture method based on real-life case studies relevant to adolescents' digital lives, complemented by live demonstrations and question-and-answer sessions. Evaluation through an interactive quiz revealed an average increase of 58 percentage points across all comprehension indicators, from 33% before to 91% after the socialization, with the highest increase recorded on the 2FA knowledge indicator at 63 percentage points. This activity demonstrates that a context-based socialization approach grounded in adolescents' real digital experiences is more effective in building cyber security awareness than generic technical approaches, while contributing to shaping a generation that is not only digitally proficient but also digitally safe.

Keywords: *cyber security awareness; digital account security; digital literacy; phishing; two-factor authentication*

1. PENDAHULUAN

Meluasnya akses internet di Indonesia telah menjadikan kelompok siswa SMA/SMK sebagai salah satu segmen pengguna digital paling aktif dengan intensitas penggunaan media sosial, aplikasi perpesanan, dan permainan daring yang tinggi (Kemp, 2023). Kementerian Komunikasi dan Informatika Republik Indonesia (2024) mencatat bahwa meskipun kecakapan digital (digital skills) remaja Indonesia tergolong tinggi, skor pada dimensi keamanan digital (digital safety) masih jauh tertinggal. Kondisi inilah yang menciptakan paradoks tech-savvy namun digitally naïve, fasih mengoperasikan perangkat digital, tetapi rentan terhadap ancaman siber yang terus berkembang. Andria et al. (2025) menegaskan bahwa cyber security awareness bagi siswa sekolah menengah bukan lagi sekadar nilai tambah, melainkan kebutuhan yang mendesak dan fundamental di era digital ini.

Ancaman yang paling marak menyasar siswa SMA/SMK adalah serangan phishing dan pembajakan akun digital. Sari et al. (2025) menemukan bahwa penyebaran link palsu merupakan modus penipuan yang paling banyak dihadapi siswa SMK, sementara Ardy et al. (2024) mengungkapkan bahwa phishing di era media sosial telah berevolusi; pelaku tidak hanya membidik data keuangan, tetapi juga kredensial akun media sosial dan akun permainan daring yang bernilai ekonomis. Dalam keseharian siswa, modus ini hadir dalam berbagai bentuk: tautan "dana kaget" palsu di grup WhatsApp, tipuan permintaan kode OTP berdalih verifikasi akun Instagram, hingga link login palsu berkedok item game gratis di Mobile Legends dan Free Fire. Bada et al. (2019) dan Sofana & Primartha (2019) menegaskan bahwa keberhasilan serangan-serangan tersebut hampir selalu bertumpu pada manipulasi psikologi korban, sehingga edukasi dan peningkatan kewaspadaan pengguna merupakan lini pertahanan yang paling krusial, jauh lebih efektif daripada mengandalkan perangkat lunak keamanan semata.

Urgensi pengamanan akun digital bagi remaja juga diperkuat oleh kerangka regulasi nasional. UU ITE Nomor 19 Tahun 2016 mengatur sanksi pidana atas akses ilegal terhadap akun dan sistem informasi milik orang lain, sementara UU Pelindungan Data Pribadi Nomor 27 Tahun 2022 menegaskan hak setiap individu atas perlindungan data pribadinya. Kedua regulasi ini memiliki implikasi langsung pada perilaku digital sehari-hari remaja yang setiap harinya meninggalkan jejak data di berbagai platform, sehingga pemahaman terhadap kerangka hukum tersebut menjadi bagian tidak terpisahkan dari literasi keamanan digital yang komprehensif.

Berbagai perguruan tinggi telah melaksanakan kegiatan pengabdian serupa, di antaranya Yuliansah et al. (2025) di SMK Insan Cendekia Yogyakarta, dan Din et al. (2024) dengan pendekatan teknologi pembelajaran di SMK, serta Nisa et al. (2025) di MAN 2 Cilacap. Namun, Puslitbang ARTIKA (2024) dan Nisa et al. (2025) mencatat bahwa sebagian besar program tersebut masih bertumpu pada materi teknis-korporat yang kurang relevan dengan kehidupan digital remaja, sehingga sulit memicu perubahan perilaku yang nyata. Fidya et al. (2025) menegaskan bahwa kontekstualisasi materi pada pengalaman digital nyata peserta terbukti secara signifikan meningkatkan efektivitas transfer pengetahuan dan keterlibatan peserta.

Berangkat dari kesenjangan tersebut, kegiatan pengabdian ini dirancang dengan pendekatan sosialisasi berbasis kasus nyata kehidupan digital siswa SMA/SMK, bukan skenario keamanan siber korporat yang asing bagi remaja. Kegiatan bertujuan untuk meningkatkan kemampuan siswa SMAN 1 Limboto dalam mengenali dan menghindari serangan phishing serta modus penipuan daring; membekali siswa dengan keterampilan praktis mengamankan akun digital secara mandiri melalui autentikasi dua faktor (2FA); dan menanamkan prinsip dasar privasi data dalam perilaku digital sehari-hari siswa selaras dengan semangat UU PDP 2022.

2. METODE

Kegiatan pengabdian kepada masyarakat ini dilaksanakan di SMAN 1 Limboto, Kabupaten Gorontalo, Provinsi Gorontalo, pada 5 Maret 2026. Sasaran kegiatan adalah siswa kelas XII sebanyak lebih dari 150 siswa yang ditetapkan melalui koordinasi dengan pihak manajemen sekolah. Pelaksanaan kegiatan dilakukan dalam tiga tahap berurutan: persiapan, pelaksanaan, dan evaluasi.

Tahap persiapan diawali dengan pengiriman surat permohonan izin kepada Kepala SMAN 1 Limboto, dilanjutkan dengan pertemuan koordinasi bersama pihak sekolah untuk menetapkan jadwal, durasi, dan peserta kegiatan. Tim pelaksana kemudian menyusun materi sosialisasi yang relevan dengan kehidupan digital siswa, mencakup contoh-contoh kasus phishing yang sedang marak di kalangan remaja, panduan pengaktifan 2FA, serta prinsip dasar pengelolaan privasi akun media sosial. Materi dirancang menggunakan bahasa yang sederhana dan mudah dipahami oleh audiens non-teknis agar pesan yang disampaikan dapat diterima secara efektif (Din et al., 2024).

Tahap pelaksanaan berlangsung di aula SMAN 1 Limboto dengan metode ceramah interaktif. Sebagaimana tampak pada Gambar 1, penyampaian materi dilakukan secara langsung oleh tim pelaksana di hadapan seluruh peserta tanpa bantuan perangkat proyektor, dengan mengandalkan komunikasi verbal yang ekspresif dan contoh-contoh kasus yang disampaikan secara lisan. Pendekatan ini justru mendorong interaksi yang lebih personal dan responsif antara pemateri dan peserta, sebagaimana dikemukakan oleh Yustisia et al. (2023) bahwa pendekatan edukasi yang interaktif dan sesuai konteks peserta mendukung pemahaman siswa.. Materi disampaikan secara berurutan mencakup tiga topik utama: (1) pengenalan modus phishing dan cara mengidentifikasi tautan palsu; (2) pengamanan akun digital melalui autentikasi dua faktor (2FA); serta (3) pengelolaan privasi data dan jejak digital di media sosial. Kondisi pelaksanaan yang kondusif dan partisipatif tercermin dari suasana peserta selama mengikuti seluruh rangkaian sesi, sebagaimana terdokumentasi pada Gambar 2. Sesi kemudian dilanjutkan dengan diskusi dan tanya jawab yang memberikan ruang bagi siswa untuk mengajukan pertanyaan dan berbagi pengalaman digital mereka secara langsung.



Gambar 1. *Penyampaian Materi Cyber Security Awareness oleh Tim Pelaksana di Aula SMAN 1 Limboto*



Gambar 2. Suasana Peserta Mengikuti Sesi Sosialisasi Cyber Security Awareness di Aula SMAN 1 Limboto

Tahap evaluasi dilakukan melalui kuis interaktif singkat yang diberikan segera setelah sesi pemaparan selesai. Kuis mencakup lima indikator pemahaman utama: kemampuan mengenali ciri-ciri phishing link; pengetahuan tentang 2FA; pemahaman modus penipuan daring; kesadaran privasi data; serta kemampuan membedakan tautan aman dan berbahaya. Data pemahaman awal (baseline) diperoleh melalui pertanyaan reflektif lisan di awal sesi sebelum materi disampaikan, kemudian dibandingkan dengan hasil kuis pasca-sosialisasi sebagai indikator keberhasilan kegiatan. Observasi langsung terhadap partisipasi siswa selama sesi tanya jawab juga dijadikan data evaluasi kualitatif yang melengkapi temuan kuantitatif (Nisa et al., 2025).

3. HASIL DAN PEMBAHASAN

Kegiatan sosialisasi Cyber Security Awareness di SMAN 1 Limboto terlaksana dengan lancar dan kondusif. Seluruh siswa yang dijadwalkan sebagai peserta hadir mengikuti kegiatan dari awal hingga akhir sesi tanpa kendala berarti yang mengganggu jalannya pelaksanaan. Kondisi ini merupakan hasil dari koordinasi yang matang pada tahap persiapan antara tim pelaksana dan pihak sekolah. Antusiasme peserta terlihat sejak awal sesi ketika pemateri membuka kegiatan dengan pertanyaan-pertanyaan ringan seputar pengalaman digital siswa. Sebagian besar siswa mengaku pernah menerima pesan mencurigakan berisi tautan hadiah atau saldo gratis melalui WhatsApp dan Instagram, namun tidak mengetahui bahwa pesan-pesan tersebut merupakan bagian dari modus phishing yang terorganisasi. Pengakuan ini sekaligus mengonfirmasi relevansi dan urgensi materi yang disampaikan dalam kegiatan ini.

Sesi pemaparan materi berlangsung secara interaktif dan dinamis. Pada topik pengenalan phishing, siswa diajak menganalisis secara langsung contoh-contoh pesan dan tautan palsu yang umum beredar di kalangan remaja. Antusiasme peserta meningkat tajam ketika pemateri membedah modus "dana kaget" palsu serta notifikasi pemblokiran akun game — banyak siswa yang spontan mengakui pernah menerima pesan serupa dan hampir atau bahkan sempat mengklik tautan yang tercantum. Momen ini menjadi titik pembelajaran yang sangat berharga (teachable moment) karena siswa merasakan secara langsung betapa dekatnya mereka dengan ancaman yang selama ini dianggap remeh. Ardy et al. (2024) menegaskan bahwa kesadaran berbasis pengalaman pribadi seperti ini jauh lebih efektif dalam membentuk kewaspadaan jangka panjang dibandingkan pemaparan konseptual semata. Pada topik pengamanan akun

melalui 2FA, siswa didorong untuk langsung mencoba mengaktifkan fitur tersebut pada akun Instagram dan Google mereka menggunakan ponsel pintar yang mereka bawa. Sejumlah besar siswa berhasil mengaktifkan 2FA secara mandiri sebelum sesi berakhir, yang merupakan bukti konkret perubahan perilaku, bukan sekadar perubahan pengetahuan (Andria et al., 2025). Pada topik privasi data, siswa mendiskusikan secara aktif kebiasaan digital mereka dan mengevaluasi sendiri potensi risiko yang selama ini tidak mereka sadari, termasuk kebiasaan berbagi informasi pribadi secara berlebihan dan mengizinkan akses aplikasi pihak ketiga tanpa seleksi.

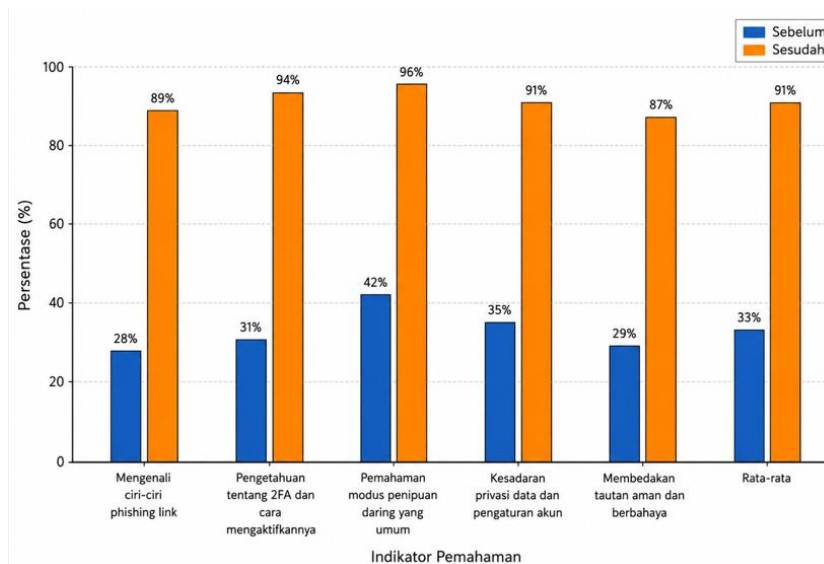
Sesi diskusi dan tanya jawab berlangsung sangat aktif dan melebihi batas waktu yang dialokasikan. Lebih dari [masukkan jumlah] pertanyaan diajukan oleh siswa dengan topik yang bervariasi, mulai dari pertanyaan teknis seperti "Apakah aplikasi autentikator lebih aman daripada OTP via SMS?", hingga pertanyaan skenario seperti "Kalau teman meminta kode OTP kita, apakah boleh diberikan?". Kualitas dan keberagaman pertanyaan yang diajukan mengindikasikan bahwa siswa tidak sekadar menyimak secara pasif, melainkan secara aktif memproses dan mengontekstualisasikan informasi ke dalam situasi kehidupan nyata mereka. Puslitbang ARTIKA (2024) menyebutkan bahwa tingginya frekuensi pertanyaan dalam sesi diskusi merupakan indikator kualitatif yang kuat terhadap keberhasilan sebuah program edukasi siber dalam membangun kesadaran kritis peserta.

Hasil evaluasi melalui kuis interaktif pasca-sosialisasi menunjukkan peningkatan yang signifikan pada seluruh indikator pemahaman yang diukur, sebagaimana disajikan pada Tabel 1 berikut.

Tabel 1. Perbandingan Tingkat Pemahaman Siswa Sebelum dan Sesudah Sosialisasi

Indikator Pemahaman	Sebelum (%)	Sesudah (%)	Peningkatan
Kemampuan mengenali ciri-ciri phishing link	28%	89%	61%
Pengetahuan tentang 2FA dan cara mengaktifkannya	31%	94%	63%
Pemahaman modus penipuan daring yang umum	42%	96%	54%
Kesadaran privasi data dan pengaturan akun	35%	91%	56%
Kemampuan membedakan tautan aman dan berbahaya	29%	87%	58%
Rata-rata	33%	91%	58%

Berdasarkan Tabel 1, rata-rata tingkat pemahaman siswa meningkat dari 33% sebelum sosialisasi menjadi 91% setelah sosialisasi, dengan peningkatan rata-rata sebesar 58 poin persentase. Gambaran peningkatan tersebut dapat dilihat secara lebih jelas melalui visualisasi pada Gambar 3, yang memperlihatkan perbandingan persentase pemahaman siswa pada setiap indikator secara berdampingan.



Gambar 3. Perbandingan Tingkat Pemahaman Siswa Sebelum dan Sesudah Sosialisasi Cyber Security Awareness

Peningkatan tertinggi terjadi pada indikator pengetahuan tentang 2FA sebesar 63 poin persentase, dari 31% menjadi 94%. Angka baseline yang rendah ini mencerminkan bahwa fitur 2FA, meskipun tersedia secara luas dan gratis di hampir semua platform digital, hampir tidak dikenal oleh sebagian besar siswa sebelum mendapatkan edukasi yang spesifik, sejalan dengan temuan Yuliansah et al. (2025) dalam kegiatan serupa di SMK Insan Cendekia Yogyakarta. Peningkatan signifikan juga tercatat pada kemampuan mengenali phishing link sebesar 61 poin persentase, dari 28% menjadi 89%, yang menunjukkan bahwa pendekatan pembelajaran berbasis contoh kasus nyata efektif dalam membangun pola pengenalan (pattern recognition) terhadap karakteristik umum tautan berbahaya (Ardy et al., 2024).

Sementara itu, indikator pemahaman modus penipuan daring mencatat angka baseline tertinggi di antara seluruh indikator (42%), namun sekaligus mencapai skor tertinggi pasca-sosialisasi (96%). Kondisi ini mengindikasikan bahwa siswa sebenarnya telah memiliki paparan terhadap informasi tentang penipuan daring melalui media sosial, namun pemahaman tersebut masih bersifat parsial dan tidak terstruktur. Sosialisasi ini berhasil mengkonsolidasi pengetahuan yang tersebar tersebut menjadi pemahaman yang lebih sistematis dan aplikatif, sebagaimana juga ditemukan oleh Sari et al. (2025) dalam konteks yang serupa di mana siswa SMK umumnya telah mendengar tentang penipuan daring namun belum mampu mengidentifikasi modus spesifiknya secara akurat sebelum mendapatkan edukasi yang terstruktur.

Secara keseluruhan, hasil kegiatan ini mengonfirmasi bahwa pendekatan sosialisasi berbasis kasus nyata yang kontekstual dengan kehidupan digital remaja terbukti efektif dalam meningkatkan cyber security awareness secara terukur. Nisa et al. (2025) menegaskan bahwa efektivitas program edukasi siber bagi pelajar tidak hanya ditentukan oleh kelengkapan materi, tetapi terutama oleh relevansi konteks penyampaian dengan realitas digital yang dihadapi peserta sehari-hari — dan temuan dalam kegiatan ini secara empiris menguatkan kesimpulan tersebut. Pengabdian kepada masyarakat adalah usaha untuk menyebarluaskan ilmu pengetahuan, teknologi, dan seni kepada masyarakat. Kegiatan tersebut harus mampu memberikan suatu nilai tambah bagi masyarakat, baik dalam kegiatan ekonomi, kebijakan, dan perubahan perilaku (sosial). Uraikan bahwa kegiatan pengabdian telah mampu memberi perubahan bagi individu/masyarakat maupun institusi baik jangka pendek maupun jangka panjang.

Pada bagian ini uraikanlah bagaimana kegiatan dilakukan untuk mencapai tujuan. Jelaskan indikator tercapainya tujuan dan tolak ukur yang digunakan untuk menyatakan keberhasilan dari kegiatan pengabdian yang telah dilakukan. Ungkapkan keunggulan dan kelemahan luaran atau fokus utama kegiatan apabila dilihat kesesuaiannya dengan kondisi masyarakat di lokasi kegiatan. Jelaskan juga tingkat kesulitan pelaksanaan kegiatan maupun produksi barang dan peluang pengembangannya kedepan. Artikel dapat diperkuat dengan dokumentasi yang relevan terkait jasa atau barang sebagai luaran, atau fokus utama kegiatan. Dokumentasi dapat berupa gambar proses penerapan atau pelaksanaan, gambar prototype produk, tabel, grafik, dan sebagainya.

4. KESIMPULAN

Kegiatan pengabdian kepada masyarakat berupa sosialisasi *Cyber Security Awareness* yang dilaksanakan di SMAN 1 Limboto, Kabupaten Gorontalo, telah terlaksana dengan baik dan mencapai seluruh target yang ditetapkan. Pendekatan sosialisasi berbasis kasus nyata kehidupan digital remaja terbukti efektif dalam meningkatkan kesadaran dan pemahaman siswa terhadap ancaman *phishing*, pentingnya pengamanan akun digital, serta prinsip dasar privasi data. Hasil evaluasi menunjukkan peningkatan rata-rata sebesar 58 poin persentase di seluruh indikator pemahaman, dari rata-rata 33% sebelum sosialisasi menjadi 91% setelah sosialisasi. Peningkatan paling signifikan terjadi pada pengetahuan tentang autentikasi dua faktor (2FA) sebesar 63 poin persentase, yang sekaligus mencerminkan betapa rendahnya pemahaman awal siswa terhadap mekanisme pengamanan akun yang sesungguhnya telah tersedia secara luas di platform yang mereka gunakan sehari-hari. Lebih dari sekadar perubahan pengetahuan, kegiatan ini juga berhasil mendorong perubahan perilaku nyata, yang tercermin dari keberhasilan sejumlah besar siswa mengaktifkan 2FA secara mandiri pada akun mereka sebelum sesi berakhir. Kegiatan ini juga mengonfirmasi bahwa kesenjangan antara kecakapan digital dan kesadaran keamanan di kalangan remaja merupakan persoalan yang nyata dan mendesak untuk ditangani secara terstruktur. Paradoks *tech-savvy* namun *digitally naive* yang melekat pada generasi muda tidak dapat diatasi hanya dengan menyediakan akses terhadap teknologi, melainkan membutuhkan intervensi edukatif yang relevan, kontekstual, dan berkelanjutan. Perguruan tinggi, melalui skema pengabdian kepada masyarakat, memiliki peran strategis dalam mengisi kesenjangan tersebut, khususnya dengan menghadirkan pendekatan sosialisasi yang menjembatani antara konsep teknis keamanan siber dan realitas kehidupan digital sehari-hari remaja. Berdasarkan hasil dan pengalaman pelaksanaan kegiatan ini, beberapa saran dirumuskan untuk memastikan keberlanjutan program literasi keamanan digital di lingkungan sekolah. Bagi pihak SMAN 1 Limboto, disarankan untuk mengintegrasikan materi dasar keamanan siber ke dalam mata pelajaran Informatika atau program ekstrakurikuler yang relevan, sehingga kesadaran yang telah dibangun melalui kegiatan ini dapat diperkuat dan dipertahankan secara berkelanjutan. Pihak sekolah juga dapat mempertimbangkan pembentukan kelompok siswa sebagai duta keamanan digital yang bertugas menyebarkan pemahaman kepada rekan-rekan mereka secara peer-to-peer, mengingat komunikasi antarsiswa seringkali lebih efektif dalam mengubah perilaku dibandingkan komunikasi dari otoritas formal (Andria et al., 2025). Bagi tim pelaksana dan perguruan tinggi, hasil kegiatan ini dapat menjadi dasar untuk mengembangkan program sosialisasi lanjutan yang lebih mendalam dan menjangkau lebih banyak sekolah mitra di Kabupaten Gorontalo, sehingga dampaknya dapat dirasakan secara lebih luas oleh generasi muda di wilayah tersebut. Kesimpulan harus mengindikasikan secara jelas hasil-hasil yang diperoleh, kelebihan dan kekurangannya, serta kemungkinan pengembangan selanjutnya. Kesimpulan sebaiknya dapat berupa paragraf, tidak berbentuk point-point.

DAFTAR PUSTAKA

- _____. (2016). *Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251.
- _____. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196.
- Andria, A., Laksono, R. D., Sussolaikah, K., Mat Din, M. B., Mansor, S., & Muhamat Dawam, S. R. (2025). Assessment of cyber security awareness using developed game from H5P on users aged at elementary and first secondary school in Madiun City. *Journal of Applied Engineering and Technological Science*, 7(1), 539–549.
- Ardy, L. A. F., Istiqomah, I., Ezer, A. E., & Neyman, S. N. (2024). Phishing di era media sosial: Identifikasi dan pencegahan ancaman di platform sosial. *Journal of Internet and Software Engineering*, 1(4), 1–11. <https://doi.org/10.47134/pjise.v1i4.2753>
- Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv*. <https://arxiv.org/abs/1901.02672>
- Din, M. B. M., Mansor, S., Dawam, S. R. M., Andria, A., Laksono, R. D., & Sussolaikah, K. (2023). The implementation of H5P in interactive games for cyber security awareness learning

- facilities for elementary and junior high school students. *Jurnal Ilmiah Teknik Elektro, Komputer, dan Informatika*, 9(3), 596–605. <https://doi.org/10.26555/jiteki.v9i3.26547>
- Fidya, S. N., Ummah, D. U. K., & Fatah, Z. (2025). Seminar edukasi penggunaan email dan keamanan siber bagi siswa SMPN 1 Nonggunong. *Jurnal Padamu Negeri*, 2(3), 131–136. <https://doi.org/10.69714/nkm55x70>
- Kementerian Komunikasi dan Informatika Republik Indonesia. (2024). *Tingkatkan literasi digital, Koinfo latih lebih dari 24 juta orang*. Kementerian Komunikasi dan Informatika Republik Indonesia.
- Kemp, S. (2023). *Digital 2023: Indonesia*. DataReportal.
- Nisa, K., Purwono, Handayani, O. P., & Setiawan. (2025). Peningkatan literasi digital: Edukasi kejahatan siber dan pinjaman online ilegal MAN 2 Cilacap. *Jurnal Pengabdian Masyarakat - PIMAS*, 4(2), 61–68. <https://doi.org/10.35960/pimas.v4i2.1831>
- Pusat Penelitian dan Pengembangan Akademi Relawan TIK Indonesia (ARTIKA). (2024). *Prosiding Konferensi Nasional Literasi Digital dan Kerelawanan (KNLDK II) 2024*. Puslitbang Akademi Relawan TIK Indonesia.
- Sari, S. D., Amalia, C. E., Nurhalisa, Risna, Meliani, M., Selviana, A., Ridwan, S. S. A., & Sunariyo. (2025). Edukasi keamanan siber pada penipuan online penyebaran link palsu. *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, 3(6), 10405–10409. <https://doi.org/10.61104/alz.v3i6.2731>
- Sofana, I., & Primartha, R. (2019). *Network security dan cyber security: Teori dan praktik Cisco CCNA, Linux, Windows, Amazon AWS, Android*. Informatika Bandung.
- Yuliansah, Y., Kustitik, K., Siregar, I. R. P. S. N., Dwihartanti, M., & Sutirman, S. (2025). Peningkatan kesadaran keamanan siber siswa SMK Insan Cendekia Yogyakarta. *Abdimas Altruis: Jurnal Pengabdian Kepada Masyarakat*, 8(1), 30–37. <https://doi.org/10.24071/aa.v8i1.9590>
- Yustisia, K. K., Winarsih, A. D., Lailiyah, M., Yudhawardhana, A. N., Binatoro, A. S., & Arifah, Q. F. (2023). Edukasi literasi digital siswa sekolah dasar tentang strategi keamanan dan manajemen siber. *GERVASI: Jurnal Pengabdian Kepada Masyarakat*, 7(1), 135–147. <https://doi.org/10.31571/gervasi.v7i1.4472>