



Edukasi Keamanan Digital bagi Siswa SMK Taruna Padang: Upaya Meningkatkan Literasi dan Pencegahan Kejahatan Siber

Diego^{1*}, Syaza Yasmin², Annisa Anindya³, Novi Elia⁴

^{1, 2, 3, 4} Departemen Ilmu Komunikasi, Universitas Andalas, Padang, Indonesia

*Corresponding author: diegoenmis@gmail.com

Received 26-05-2026

Revised 09-06-2026

Published 26-06-2026

ABSTRAK

Kegiatan pengabdian kepada masyarakat ini bertujuan meningkatkan literasi keamanan digital di kalangan siswa SMK Taruna Kota Padang yang rentan terhadap ancaman kejahatan siber. Rendahnya kesadaran digital di kalangan pelajar mendorong tingginya kasus scamming, phishing, dan pencurian identitas. Kegiatan dilaksanakan pada 9 Desember 2025 dan diikuti 38 siswa. Metode pelaksanaan meliputi pemaparan materi, simulasi interaktif, diskusi, serta evaluasi post-test dan kuis. Hasil menunjukkan peningkatan signifikan pemahaman siswa terhadap modus kejahatan siber dan langkah pencegahannya. Kegiatan ini menegaskan pentingnya peran perguruan tinggi dalam memperkuat literasi digital generasi muda agar mampu menggunakan internet secara aman, kritis, dan bertanggung jawab.

Kata kunci: Keamanan digital; Literasi digital; Kejahatan siber; *Phishing*; *Scamming*

ABSTRACT

This community service activity aims to improve digital security literacy among students of SMK Taruna Padang City who are vulnerable to cybercrime threats. Low digital awareness among students contributes to increasing cases of scamming, phishing, and identity theft. The activity was conducted on December 9, 2025, involving 38 students. Methods included material presentations, interactive simulations, discussions, and evaluations through post-tests and quizzes. Results showed a significant improvement in students' understanding of cybercrime modes and preventive measures. This activity affirms the important role of higher education institutions in strengthening digital literacy among younger generations to enable safe, critical, and responsible internet use.

Keywords: Digital Security; Digital Literacy; Cybercrime; *Phishing*; *Scamming*

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi yang pesat membawa berbagai kemudahan sekaligus ancaman nyata bagi masyarakat, khususnya generasi muda. Berdasarkan data We Are Social (2023), pengguna internet di Indonesia per Januari 2023 telah mencapai 212,9 juta jiwa atau sekitar 77% dari total populasi, dan angka ini terus meningkat setiap tahunnya. Tingginya jumlah pengguna internet tersebut berbanding lurus dengan meningkatnya risiko kejahatan siber, di mana literasi digital dalam keamanan siber memiliki peran strategis dalam menghadapi berbagai ancaman di ruang digital, termasuk dalam bentuk *social engineering*. Penggunaan media sosial dan internet di kalangan remaja yang sangat tinggi menjadikan mereka kelompok yang paling rentan terhadap berbagai bentuk penipuan



digital. Kasus-kasus pencurian akun, penipuan online, dan kebocoran data pribadi semakin marak terjadi, yang sebagian besar bermula dari rendahnya kesadaran pengguna terhadap pentingnya menjaga keamanan informasi digital (Kominfo, 2023).

Literasi digital bukan sekadar kemampuan mengoperasikan perangkat dan aplikasi, melainkan juga mencakup kemampuan berpikir kritis dalam menghadapi informasi dan ancaman di ruang digital. Survei yang dilakukan Kominfo dan KIC menunjukkan bahwa Indeks Literasi Digital Indonesia berada pada skor 3,49 dari skala 1–5, dengan skor untuk dimensi keamanan digital yang paling rendah, yakni hanya 3,10. Kondisi ini mengindikasikan bahwa aspek keamanan digital masih menjadi titik lemah dalam ekosistem literasi digital nasional. Bagi kalangan pelajar, kelemahan ini menjadi faktor utama yang membuat mereka mudah terjerumus dalam berbagai modus penipuan daring. Remaja, yang sering menjadi pengguna aktif internet, merupakan salah satu kelompok yang paling rentan terhadap serangan *phishing*, dan korban dapat mengalami kerugian finansial, pencurian identitas, hingga dampak psikologis yang serius. Ancaman ini semakin mengkhawatirkan mengingat tingginya frekuensi penggunaan platform digital dalam kehidupan sehari-hari siswa (Sulistyo & Wibowo, 2021; Syafuddin, K., 2023)

Berbagai penelitian terdahulu telah mengkaji upaya penanggulangan kejahatan siber di kalangan pelajar. Sunardi dkk. (2024) dalam penelitiannya tentang perilaku remaja dalam menggunakan internet di SMA Muhammadiyah Pacitan menemukan bahwa pemahaman siswa terhadap modus *phishing* masih sangat terbatas, sehingga diperlukan edukasi yang sistematis untuk meningkatkan kemampuan pengenalan dan penghindaran ancaman siber. Sejalan dengan itu, Sari dan Pratama (2023) menegaskan bahwa edukasi *cyber security* bagi pelajar merupakan upaya strategis dalam pencegahan kejahatan digital, mengingat tingginya angka serangan *phishing* yang menargetkan pengguna muda di Indonesia. Sementara itu, Sunardi, S., Murinto dkk. (2024) menunjukkan bahwa kegiatan edukasi *digital safety* yang terstruktur terbukti mampu meningkatkan kecakapan bermedia digital siswa secara signifikan.

Edukasi mengenai keamanan media sosial di sekolah-sekolah, terutama yang berada di luar pusat kota, masih sangat terbatas. Penelitian Yudiana (2023) mengungkapkan adanya kesenjangan yang cukup besar dalam kemampuan literasi siswa antara daerah perkotaan dibandingkan dengan daerah pinggiran kota dan pedesaan, dan kesenjangan serupa dapat dipastikan berlaku pula dalam konteks literasi keamanan digital. Nasrullah (2022) menunjukkan bahwa di Indonesia, kesenjangan digital ini terutama terlihat antara daerah perkotaan dan pedesaan, dan upaya mengatasinya memerlukan dukungan dari berbagai pihak, termasuk perguruan tinggi dan institusi pendidikan. SMK Taruna Kota Padang dipilih sebagai lokasi kegiatan karena edukasi mengenai literasi dan keamanan media sosial masih jarang menjangkau sekolah-sekolah di luar pusat kota, sementara penggunaan media sosial di kalangan siswanya sudah sangat tinggi dan kasus-kasus penipuan digital terus meningkat.

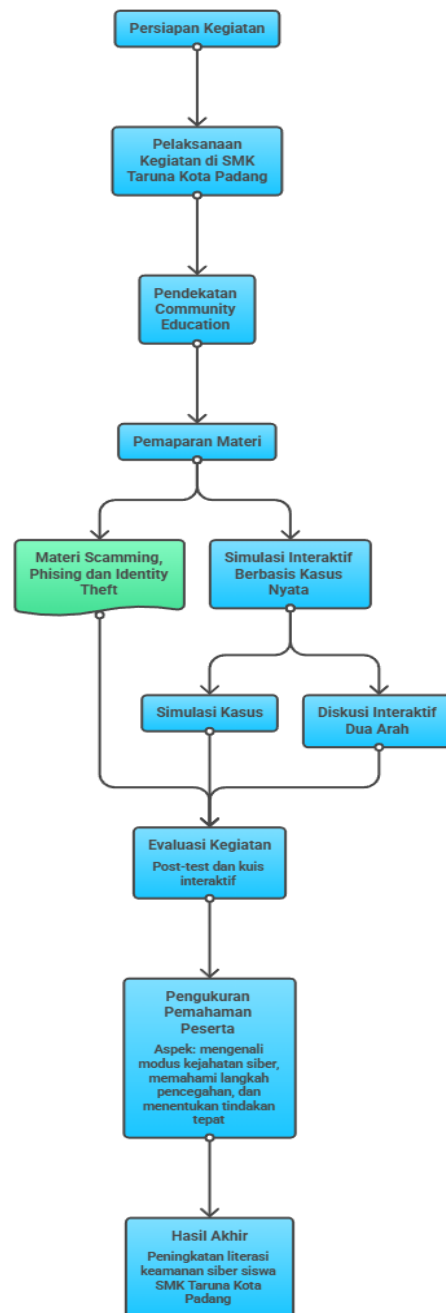
Berangkat dari permasalahan tersebut, Departemen Ilmu Komunikasi Universitas Andalas (Unand) melaksanakan kegiatan pengabdian kepada masyarakat bertema "Menjaga Informasi Pribadi di Internet: Menghindari *Scamming*, *Phishing*, dan *Identity Theft*". Kegiatan ini bertujuan: (1) meningkatkan literasi keamanan digital siswa; (2) memberikan pemahaman praktis mengenai modus kejahatan siber; serta (3) membekali siswa dengan keterampilan untuk melindungi diri di ruang digital.

METODE PELAKSANAAN

Kegiatan pengabdian masyarakat ini dilaksanakan pada Selasa, 9 Desember 2025 di SMK Taruna Kota Padang dan diikuti oleh 38 siswa dari berbagai jurusan. Pendekatan yang digunakan adalah *community education* (pendidikan masyarakat) yang dikombinasikan dengan pelatihan berbasis simulasi dan diskusi partisipatif. Pemilihan pendekatan ini didasarkan pada efektivitasnya dalam meningkatkan kesadaran dan keterampilan praktis peserta secara langsung. Kegiatan sosialisasi keamanan siber yang menggunakan metode interaktif dan partisipatif terbukti mampu meningkatkan pemahaman peserta terhadap ancaman digital serta cara-cara pencegahan yang efektif, termasuk kewaspadaan terhadap *phishing* dan penipuan *online*.

Kegiatan dilaksanakan oleh tim dosen dan mahasiswa Departemen Ilmu Komunikasi Universitas Andalas (Unand) yang bertindak sebagai fasilitator dan pemateri. Adapun tahapan metode pelaksanaan yang digunakan adalah sebagai berikut. Berikut diagram alir dari metode pengabdian ini:

Alur Pengabdian Edukasi Keamanan Digital bagi Siswa SMK Taruna Padang



Made with Napkin

Gambar 1. Diagram Alir Pengabdian

Pemaparan Materi

Tahap pertama adalah pemaparan materi yang disampaikan secara terstruktur oleh tim pemateri dari Departemen Ilmu Komunikasi Unand. Materi dirancang dengan mempertimbangkan relevansi terhadap kehidupan sehari-hari siswa SMK agar mudah dipahami dan diaplikasikan. Topik-topik yang disampaikan meliputi: (1) *scamming* dengan kedok verifikasi akun media sosial dan perbankan; (2) *phishing* melalui tautan

paket ekspedisi palsu dan lowongan kerja palsu; serta (3) pencurian identitas (*identity theft*) yang memanfaatkan data pribadi yang dibagikan sembarangan di media sosial, seperti nama lengkap, tanggal lahir, foto berseragam, dan nomor telepon. Penyampaian materi menggunakan media presentasi visual yang interaktif, disertai contoh tangkapan layar kasus nyata agar siswa dapat langsung mengidentifikasi ciri-ciri konten berbahaya. Kondisi di mana sekolah belum memiliki program khusus yang secara sistematis melatih siswa terkait keamanan digital menjadikan pemaparan materi yang terstruktur sebagai fondasi penting dalam membangun kesadaran awal siswa sebelum memasuki tahapan pelatihan praktis.

Simulasi Interaktif

Tahap kedua adalah simulasi interaktif yang dirancang untuk mempertemukan peserta langsung dengan skenario ancaman siber dalam kondisi terkontrol dan aman. Peserta diajak mengikuti simulasi cara kerja *phishing* dan menganalisis sejumlah kasus yang sempat viral di masyarakat, seperti tagihan ShopeePay Later palsu, tautan ekspedisi palsu, dan aksi penipuan yang mengatasnamakan guru sekolah. Pendekatan simulasi *phishing* dengan menyajikan contoh nyata dari situs web atau pesan palsu terbukti memungkinkan siswa untuk secara langsung berlatih mengenali pola serangan yang sering digunakan, sehingga meningkatkan kewaspadaan mereka secara praktis. Melalui simulasi ini, siswa tidak hanya menerima informasi secara pasif, tetapi juga dilatih untuk mengambil keputusan cepat dan tepat ketika menghadapi situasi penipuan digital yang sesungguhnya. Pendekatan berbasis skenario nyata ini dipilih karena relevansinya terhadap pengalaman keseharian siswa, sehingga proses pembelajaran menjadi lebih kontekstual dan bermakna (Zwilling et al., 2022).

Diskusi Interaktif

Tahap ketiga adalah diskusi interaktif dua arah antara pemateri dan peserta. Sesi ini dirancang untuk mendorong partisipasi aktif siswa melalui berbagi pengalaman pribadi, pertanyaan kritis, dan simulasi pengambilan keputusan dalam menghadapi ancaman siber. Siswa dilatih untuk mengenali pola-pola umum kejahatan digital, memverifikasi informasi sebelum bertindak, serta memahami langkah-langkah cepat yang harus dilakukan ketika berhadapan dengan potensi penipuan — mulai dari tidak mengklik tautan mencurigakan, tidak membagikan kode OTP kepada siapapun, hingga melaporkan akun atau konten mencurigakan kepada pihak berwenang. Program sosialisasi yang dirancang dengan pendekatan partisipatif, di mana siswa tidak hanya menjadi pendengar pasif tetapi aktif terlibat dalam diskusi dan simulasi, terbukti lebih efektif dalam meningkatkan pemahaman dan tanggung jawab digital pelajar. Diskusi juga menjadi ruang bagi pemateri untuk mengoreksi miskonsepsi yang berkembang di kalangan siswa seputar keamanan digital.

Evaluasi (*Post-Test* dan Kuis)

Tahap akhir kegiatan adalah evaluasi yang dilakukan melalui *post-test* dan kuis seputar keamanan digital. Instrumen evaluasi dirancang untuk menilai peningkatan

kompetensi peserta pada tiga aspek: (1) kemampuan mengidentifikasi modus kejahatan siber; (2) pemahaman terhadap langkah-langkah pencegahan; dan (3) kemampuan mengambil tindakan tepat saat menghadapi ancaman digital. Evaluasi melalui *pre-test* dan *post-test* merupakan metode yang lazim digunakan dalam program edukasi keamanan digital, di mana peserta juga diminta memberikan umpan balik melalui kuesioner singkat untuk mengukur efektivitas penyampaian materi secara menyeluruh. Selain mengukur peningkatan pemahaman kognitif, kuis yang dikemas dalam format interaktif juga berfungsi memperkuat materi yang telah disampaikan sekaligus menjaga antusiasme peserta hingga akhir sesi. Studi-studi pengabdian serupa menunjukkan bahwa metode penyuluhan dengan pendekatan ceramah interaktif, diskusi, dan simulasi kasus yang dievaluasi menggunakan instrumen *pre-test* dan *post-test* efektif meningkatkan literasi keamanan siber peserta secara signifikan dan terukur.

HASIL KEGIATAN

Kegiatan pengabdian masyarakat ini berjalan dengan lancar dan mendapat respons positif dari para peserta. Seluruh 38 siswa SMK Taruna Padang mengikuti rangkaian kegiatan dari awal hingga akhir dengan antusias, yang tercermin dari tingginya partisipasi aktif selama setiap sesi berlangsung. Keberhasilan pelaksanaan kegiatan ini sejalan dengan temuan sejumlah penelitian terdahulu yang menunjukkan bahwa pendekatan edukatif berbasis simulasi dan diskusi interaktif efektif dalam meningkatkan literasi keamanan digital di kalangan pelajar. Berikut diuraikan hasil kegiatan berdasarkan setiap tahapan yang dilaksanakan.



Gambar 2. Pemaparan Materi Oleh Tim Pemateri Departemen Ilmu Komunikasi UNAND

Peningkatan Pengetahuan tentang Modus Kejahatan Siber

Setelah mengikuti sesi pemaparan materi, siswa menunjukkan pemahaman yang jauh lebih baik terhadap berbagai modus kejahatan siber. Mereka mampu mengidentifikasi ciri-ciri *scamming* dengan kedok verifikasi akun, mengenali tautan *phishing* yang mencurigakan, serta memahami cara kerja pencurian identitas yang sering memanfaatkan data pribadi yang dibagikan secara tidak hati-hati di media sosial. Sebelum kegiatan dimulai, banyak siswa yang belum menyadari bahwa foto berseragam, tanggal lahir, dan nomor telepon yang mereka bagikan di media sosial dapat dimanfaatkan untuk keperluan penipuan.

Setelah pemaparan, pemahaman tersebut berubah secara signifikan dan siswa mulai menyadari pentingnya membatasi informasi pribadi di ruang digital. Pendekatan pemaparan yang dilengkapi dengan diskusi interaktif dan contoh kasus yang dekat dengan kehidupan siswa terbukti membantu peserta lebih mudah memahami dan menerapkan materi dalam keseharian mereka, sekaligus menumbuhkan kesadaran bahwa menjaga keamanan digital merupakan tanggung jawab pribadi setiap pengguna internet. Hal ini terlihat pula dari antusiasme siswa dalam sesi tanya jawab, di mana mereka aktif mengajukan pertanyaan berdasarkan pengalaman nyata yang pernah mereka alami atau saksikan (Hadlington, 2017).

Kemampuan Analisis Kasus Nyata

Melalui simulasi interaktif, peserta berhasil menganalisis kasus-kasus penipuan digital yang sempat viral di masyarakat. Siswa dilatih untuk memverifikasi informasi sebelum bertindak, mempertanyakan keaslian pesan atau tautan yang diterima, serta tidak sembarangan membagikan data pribadi kepada pihak yang tidak dikenal. Dalam simulasi tagihan ShopeePay Later palsu misalnya, siswa berhasil mengidentifikasi setidaknya empat indikator penipuan: ketidaksesuaian domain pengirim, penggunaan bahasa yang memancing kepanikan, permintaan data sensitif secara langsung, dan tautan yang mengarah ke situs tidak resmi. Kemampuan analisis kritis semacam ini merupakan kompetensi inti dalam literasi digital yang sangat dibutuhkan generasi muda saat ini (Mitnick & Simon, 2002).

Hasil evaluasi pada kegiatan-kegiatan serupa menunjukkan bahwa siswa yang telah mengikuti edukasi keamanan digital mampu mengidentifikasi ciri-ciri *phishing*, memahami bahaya aplikasi modifikasi, dan menerapkan praktik keamanan dasar, sehingga berhasil membentuk kesadaran keamanan digital di lingkungan sekolah dan mendorong perilaku berinternet yang lebih aman dan bertanggung jawab.



Gambar 3. Diskusi Interaktif Antara Pemateri Dan Siswa

Dampak terhadap Kesadaran dan Perilaku Digital

Di luar capaian kognitif yang terukur melalui evaluasi, kegiatan ini juga menghasilkan dampak kualitatif yang tidak kalah penting, yaitu terbentuknya kesadaran kritis dan perubahan sikap siswa dalam menggunakan media sosial dan internet. Edukasi *cyber security awareness* terbukti memberikan dampak positif terhadap peningkatan kesadaran keamanan digital siswa, di mana mereka menjadi lebih memahami bahwa menjaga keamanan digital bukan hanya tanggung jawab sekolah atau penyedia layanan teknologi, melainkan juga tanggung jawab pribadi sebagai pengguna internet. Perubahan sikap ini tampak dari antusiasme siswa dalam mendiskusikan pengalaman mereka menghadapi situasi mencurigakan di media sosial, serta komitmen yang mereka nyatakan untuk lebih berhati-hati dalam membagikan informasi pribadi. Kegiatan edukasi semacam ini menggarisbawahi pentingnya sosialisasi tentang keamanan data dan privasi di era digital, karena dengan pemahaman yang lebih baik dan praktik keamanan yang tepat, masyarakat termasuk kalangan pelajar dapat menggunakan teknologi secara lebih bijaksana dan melindungi data pribadi mereka dengan lebih efektif Manurung, J., Sihombing, A. P. E., & Pandiangan, B. (2023).

Hasil Evaluasi *Post-Test*

Berdasarkan data karakteristik responden dalam *post-test* yang telah dilaksanakan setelah proses pemberian edukasi keamanan digital, mayoritas peserta menggunakan *smartphone* dan aktif menggunakan media sosial dalam kehidupan sehari-hari. Diketahui pula *platform* yang kerap digunakan adalah Instagram (73,7%), TikTok (65,8%), WhatsApp (34,2%), dan Facebook (10,5%). Berikutnya durasi penggunaan media sosial per hari yang juga tergolong tinggi, yakni sebagian siswa

menggunakan media sosial lebih dari 3 jam per hari. Temuan ini menunjukkan bahwa siswa merupakan kelompok yang dekat dengan ruang digital sehingga memiliki kerentanan terhadap ancaman kejahatan siber seperti yang telah disebutkan sebelumnya, mulai dari penipuan online, pencurian identitas, penyalahgunaan data pribadi dan lainnya (UNESCO, 2023).

Hasil kegiatan menunjukkan bahwa edukasi keamanan digital memberikan dampak positif pada literasi digital siswa SMK Taruna Padang. Hasil *post-test* menunjukkan tingginya penggunaan media sosial yang juga memperlihatkan bahwa generasi muda hidup dalam lingkungan digital yang sangat aktif dan dibutuhkannya kemampuan literasi digital dan kesadaran atas keamanan digital yang memunculkan agar dapat menggunakan internet secara aman dan bertanggung jawab (UNESCO, 2023).

Berdasarkan *post-test* juga diketahui bahwa mayoritas siswa memperlihatkan tingkat pemahaman yang cukup baik terkait perlindungan data pribadi di ruang digital. Hal ini terlihat dari beberapa indikator pertanyaan yang diberikan dalam *post-test* setelah dilakukannya pemberian edukasi literasi digital. Indikator pertama, yakni kemampuan mencari informasi mengenai perlindungan data pribadi di internet, sebanyak 44,7% siswa menyatakan sangat setuju dan 23,7% setuju bahwa mereka mengetahui cara mencari informasi mengenai perlindungan data pribadi. Ini menunjukkan bahwa kegiatan edukasi literasi digital turut membantu siswa mengenali sumber informasi yang dapat digunakan untuk meningkatkan keamanan digital (Nasrullah et al., 2021). Indikator lainnya yakni kemampuan teknis keamanan digital, sebanyak 52,6% siswa menyatakan sangat setuju dan 34,2% setuju bahwa mereka mampu menemukan pengaturan keamanan pada aplikasi media sosial yang digunakan. Data ini juga menunjukkan bahwa kemampuan praktis siswa cukup baik dalam mengelola keamanan akun digital.

Selanjutnya terkait dengan data pribadi di internet, berdasarkan *post-test*, dapat diketahui bahwa siswa sudah mulai memahami pentingnya menjaga data pribadi dan mempertimbangkan konsekuensi dari aktivitas digital yang dilakukan. Para siswa juga setuju bahwa harus dilakukannya pemeriksaan terlebih dahulu pada individu atau akun pengirim pesan sebelum memberikan respons, terlebih pada pesan-pesan yang terlihat mencurigakan seperti pemberian hadiah atau voucher dan lainnya. Ini juga mengindikasikan kemampuan siswa dalam mengenali modus penipuan digital dan *phishing*.

Kegiatan pengabdian ini juga menunjukkan bahwa para siswa sudah mulai mempertimbangkan audiens media sosial sebelum mengunggah konten dan menghindari membagi nomor telepon di ruang publik digital. Berdasarkan hasil *post-test* juga diketahui bahwa edukasi keamanan digital ini memiliki peran penting dalam meningkatkan literasi digital bagi generasi muda untuk lebih sadar, kritis dan aman dalam menggunakan teknologi digital.



Gambar 4. Dokumentasi Photo Bersama Seluruh Siswa SMK Taruna Padang

KESIMPULAN DAN SARAN

Kegiatan pengabdian kepada masyarakat berupa edukasi keamanan digital yang dilaksanakan oleh Departemen Ilmu Komunikasi Universitas Andalas di SMK Taruna Padang telah berhasil meningkatkan literasi dan kesadaran keamanan digital siswa. Melalui kombinasi pemaparan materi, simulasi interaktif, diskusi, dan evaluasi, peserta memperoleh pemahaman yang lebih komprehensif mengenai ancaman kejahatan siber beserta cara pencegahannya. Hasil evaluasi *post-test* menunjukkan peningkatan signifikan pada aspek pengetahuan modus kejahatan siber, kemampuan identifikasi phishing, kesadaran perlindungan data pribadi, dan kemampuan analisis kasus nyata.

Kegiatan ini menegaskan pentingnya peran perguruan tinggi dalam menjangkau komunitas sekolah yang masih minim akses terhadap edukasi keamanan digital. Disarankan agar program edukasi keamanan digital dilaksanakan secara berkala dan diperluas ke sekolah-sekolah lain, khususnya di kawasan pinggiran kota, serta melibatkan orang tua dan guru sebagai agen literasi digital di lingkungan keluarga dan sekolah.

UCAPAN TERIMA KASIH

Tim pengabdian masyarakat mengucapkan terima kasih kepada pihak SMK Taruna Kota Padang atas dukungan, fasilitas, dan kerja samanya. Penghargaan juga disampaikan kepada seluruh siswa yang telah berpartisipasi aktif serta kepada Departemen Ilmu Komunikasi Universitas Andalas yang telah memfasilitasi dan mendukung terlaksananya program pengabdian masyarakat ini.

DAFTAR PUSTAKA

Badan Siber dan Sandi Negara. (2023). Laporan ancaman siber Indonesia 2022. BSSN.

- Cho, H., Rivera-Sanchez, M., & Lim, S. S. (2009). A multinational study on online privacy: Global concerns and local responses. *New Media & Society*, 11(3), 395–416. <https://doi.org/10.1177/1461444808101614>
- Hadlington, L. (2017). Human factors in cybersecurity: Examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, 3(7), e00346. <https://doi.org/10.1016/j.heliyon.2017.e00346>
- Kemdikbud. (2021). *Panduan literasi digital untuk pendidikan menengah*. Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi.
- Kominfo. (2023). *Laporan Tahunan Keamanan Siber Indonesia*. Kementerian Komunikasi Dan Informatika Republik Indonesia.
- Manurung, J., Sihombing, A. P. E., & Pandiangan, B. (2023). Sosialisasi Dan Edukasi Tentang Keamanan Data Dan Privasi Di Era Digital Untuk Meningkatkan Kesadaran Dan Perlindungan Masyarakat. *Jurnal Pengabdian Masyarakat Nauli*, 2(1), 1-7.
- Mitnick, K. D., & Simon, W. L. (2002). *The Art Of Deception: Controlling The Human Element Of Security*. John Wiley & Sons.
- MJNews.id. (2025, Desember 22). Departemen Ilmu Komunikasi Unand gelar edukasi keamanan digital di SMK Taruna Padang. Diakses dari <https://www.mjnews.id/sumatera-barat/kota-padang/m-146649/departemen-ilmu-komunikasi-unand-gelar-edukasi-keamanan-digital-di-smk-taruna-padang/>
- Nasrullah, R. (2019). *Media Sosial: Perspektif Komunikasi, Budaya, Dan Sosioteknologi (Edisi Ke-4)*. Simbiosis Rekatama Media.
- Nasrullah, R., Aditya, W., Satya, T. I., Nento, M. N., Hanifah, N., Miftahussururi, & Akbari, Q. S. (2021). *Literasi digital: Cakap, aman, dan berbudaya di ruang digital*. Kementerian Komunikasi dan Informatika Republik Indonesia.
- Pratama, I. P. A. E. (2020). *Keamanan informasi di era digital: Ancaman, tantangan, dan solusi*. Informatika.
- Rahayu, S., & Pratiwi, D. (2022). Pengaruh Literasi Digital Terhadap Kemampuan Identifikasi Hoaks Pada Remaja. *Jurnal Ilmu Komunikasi*, 19(1), 87–102.
- Sulistyo, E. T., & Wibowo, A. (2021). Literasi Digital Dan Keamanan Siber Pada Remaja: Studi Kasus Di Sekolah Menengah. *Jurnal Komunikasi Indonesia*, 10(2), 115–130.
- Sunardi, S., Murinto, M., Astianingrum, K., Yuliasih, B. N., & Putri, S. A. (2024). Perilaku Remaja dalam Menggunakan Internet untuk Mengenali dan Mengindari Phishing pada SMA Muhammadiyah Pacitan. *Ahsana: Jurnal Penelitian dan Pengabdian kepada Masyarakat*, 2(3), 70-78.

- Syafuddin, K. (2023). Peningkatan literasi keamanan digital dan perlindungan data pribadi bagi siswa di SMPN 154 Jakarta. *Eastasouth Journal of Impactive Community Services*, 1(03), 122-133.
- UNESCO. (2023). *Global framework of reference on digital literacy skills for indicator 4.4.2*. UNESCO Publishing.
- Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. (2022). Sekretariat Negara.
- Widodo, A., & Handayani, T. (2021). Pelatihan Keamanan Media Sosial Untuk Generasi Z Di Lingkungan Sekolah. *Jurnal Pengabdian Kepada Masyarakat*, 7(2), 210–220.
- Yusup, F., & Subekti, P. (2020). Edukasi Keamanan Siber Bagi Pelajar SMA Sebagai Upaya Penanggulangan Kejahatan Digital. *Jurnal Pengabdian Masyarakat*, 3(1), 45–54.
- Zwilling, M., Klien, G., Lesjak, D., Wiechetek, L., Cetin, F., & Basim, H. N. (2022). Cyber Security Awareness, Knowledge And Behavior: A Comparative Study. *Journal of Computer Information Systems*, 62(1), 82–97.
<https://doi.org/10.1080/08874417.2020.1712269>