Abdi Akommedia : Jurnal Pengabdian Masyarakat
ISSN: 3025-8103
Vol. 1, No. 2, Juni 2023

Peningkatan Literasi Digital Lanjutan dan Keamanan Siber

Didik Setiadi[1], Ribut Julianto[2], Ranto Siswanto[3]
[123]*Program Studi Informatika, Universitas Indonesia Mandiri*
e-mail: didiksetiadi@uimandiri.ac.id

ABSTRAK

Kegiatan pengabdian kepada masyarakat ini bertujuan untuk meningkatkan literasi digital lanjutan dan keamanan siber pada masyarakat agar lebih mampu menghadapi berbagai risiko di ruang digital. Permasalahan yang dihadapi mitra meliputi rendahnya pemahaman mengenai perlindungan data pribadi, keamanan akun, verifikasi informasi digital, serta ancaman siber seperti phishing, penipuan online, dan penyalahgunaan informasi. Kegiatan dilaksanakan dengan pendekatan edukatif, partisipatif, dan aplikatif melalui tahapan persiapan, analisis kebutuhan, penyusunan materi, pelatihan, praktik dan simulasi, pendampingan, serta evaluasi. Hasil kegiatan menunjukkan adanya peningkatan pemahaman peserta mengenai literasi digital lanjutan, meningkatnya kesadaran terhadap pentingnya keamanan siber, serta bertambahnya kemampuan peserta dalam menerapkan langkah-langkah perlindungan akun dan data pribadi. Peserta juga menunjukkan peningkatan kemampuan dalam mengenali ancaman digital dan memverifikasi informasi sebelum menyebarkannya. Kegiatan ini memberikan dampak positif terhadap pembentukan perilaku digital yang lebih aman, kritis, dan bertanggung jawab. Dengan demikian, program peningkatan literasi digital lanjutan dan keamanan siber dapat menjadi bentuk pengabdian yang relevan dalam mendukung terwujudnya masyarakat yang cakap digital dan memiliki ketahanan yang lebih baik terhadap risiko siber.

Kata Kunci: literasi digital lanjutan, keamanan siber, pengabdian kepada masyarakat, perlindungan data, verifikasi informasi

ABSTRACT

This community service program aimed to improve advanced digital literacy and cybersecurity awareness in the community so that participants would be better prepared to face various risks in the digital environment. The problems faced by the partners included limited understanding of personal data protection, account security, digital information verification, and cyber threats such as phishing, online fraud, and information misuse. The program was carried out using an educational, participatory, and practical approach through the stages of preparation, needs analysis, material development, training, practice and simulation, mentoring, and evaluation. The results showed an improvement in participants' understanding of advanced digital literacy, greater awareness of the importance of cybersecurity, and better ability to apply account protection and personal data security measures. Participants also demonstrated improved skills in identifying digital threats and verifying information before sharing it. This program had a positive impact on the development of safer, more critical, and more responsible digital behavior. Therefore, the program on advanced digital literacy and cybersecurity can serve as a relevant form of community service in supporting the creation of a digitally competent society with stronger resilience against cyber risks.

Keywords: *advanced digital literacy, cybersecurity, community service, data protection, information verification*

1. PENDAHULUAN

Literasi digital telah berkembang menjadi kompetensi yang tidak lagi terbatas pada kemampuan mengoperasikan perangkat, melainkan mencakup kemampuan mengakses, memahami, mengevaluasi, memproduksi, dan menggunakan informasi digital secara bertanggung jawab. Perluasan makna ini menunjukkan bahwa masyarakat memerlukan kecakapan yang lebih tinggi agar dapat berpartisipasi secara aman dan efektif dalam lingkungan digital yang terus berubah (UNESCO, 2024).

Transformasi digital telah memperluas penggunaan teknologi dalam pendidikan, komunikasi, ekonomi, dan layanan publik, tetapi perkembangan tersebut juga memperbesar risiko terhadap kesejahteraan, privasi,

dan keamanan pengguna. OECD menegaskan bahwa teknologi digital membawa manfaat luas, namun juga menimbulkan risiko yang harus dikelola secara bertanggung jawab agar kepercayaan publik terhadap ekosistem digital tetap terjaga (OECD, 2024a).

Kecakapan digital lanjutan menjadi penting karena masyarakat saat ini tidak cukup hanya memahami fungsi aplikasi, melainkan juga perlu memahami konsekuensi penggunaan teknologi. Pengguna digital dituntut mampu mengelola privasi, memahami jejak digital, mengenali risiko platform, dan mengambil keputusan yang tepat saat berinteraksi di ruang siber. Kajian pengembangan program literasi digital juga menunjukkan bahwa dimensi privasi dan keselamatan digital merupakan komponen inti dalam desain literasi digital kontemporer (Buchan et al., 2024; UNESCO, 2024).

Keamanan siber menjadi bagian yang tidak terpisahkan dari literasi digital lanjutan karena hampir seluruh aktivitas digital melibatkan data, identitas, dan akses akun yang rentan disalahgunakan. Perlindungan terhadap perangkat, jaringan, akun, dan informasi pribadi tidak lagi dapat dipahami sebagai isu teknis yang hanya relevan bagi ahli teknologi, tetapi sudah menjadi kebutuhan dasar setiap pengguna digital (World Economic Forum, 2024).

Ancaman siber yang dihadapi masyarakat semakin beragam, mulai dari phishing, malware, rekayasa sosial, pencurian identitas, hingga pembajakan akun. Kompleksitas ancaman tersebut meningkat seiring dengan meluasnya konektivitas digital dan ketergantungan masyarakat pada platform daring. World Economic Forum menilai bahwa lanskap keamanan siber global semakin kompleks dan menuntut peningkatan kesiapan di tingkat individu maupun organisasi (World Economic Forum, 2024).

Kerentanan pengguna digital sering kali dipicu oleh kebiasaan yang tampak sederhana, seperti menggunakan kata sandi yang lemah, mengabaikan autentikasi dua faktor, membuka tautan tanpa verifikasi, atau membagikan data pribadi tanpa mempertimbangkan risiko. Penelitian menunjukkan bahwa literasi digital memiliki pengaruh penting terhadap perilaku keamanan daring, sehingga peningkatan kecakapan digital berpotensi langsung memperkuat praktik keamanan pengguna (Nguyen et al., 2024).

Kesadaran keamanan siber juga tidak tumbuh otomatis hanya karena seseorang sering menggunakan internet. Penelitian pada mahasiswa menunjukkan bahwa pengetahuan, sikap, dan kemampuan menilai risiko siber masih memerlukan penguatan melalui intervensi pendidikan yang lebih terarah. Temuan ini memperlihatkan bahwa kelompok yang aktif menggunakan teknologi pun tetap dapat memiliki tingkat kesadaran keamanan yang belum memadai (Adeshola & Oluwajana, 2025).

Literasi digital lanjutan juga berkaitan erat dengan kemampuan menghadapi misinformasi, disinformasi, dan berita palsu yang beredar di ruang digital. Arus informasi yang cepat di media sosial membuat pengguna tidak hanya berperan sebagai penerima informasi, tetapi juga sebagai penyebar. Tinjauan ilmiah terbaru menunjukkan bahwa deteksi berita palsu masih menjadi tantangan besar karena konten yang salah sering dirancang menyerupai kebenaran dan sulit diverifikasi hanya dari tampilan permukaan (Aïmeur et al., 2023).

Kemampuan mengevaluasi kebenaran informasi perlu menjadi bagian inti dari program literasi digital karena kerentanan terhadap informasi palsu dapat menimbulkan kerugian sosial dan individual. Berbagai upaya pendidikan mengenai online information literacy berkembang pesat dalam beberapa tahun terakhir untuk membantu pengguna menilai sumber, konteks, dan kredibilitas konten digital secara lebih kritis (McGrew & Kohnen, 2024).

Pendekatan lateral reading dan pelatihan berbasis evaluasi sumber terbukti menjadi salah satu strategi yang menjanjikan dalam melawan misinformasi. Studi eksperimental menunjukkan bahwa pelatihan lateral reading dapat membantu peserta lebih baik dalam menilai kredibilitas berita online. Hal ini menguatkan pandangan bahwa literasi digital lanjutan perlu diarahkan pada pembentukan kebiasaan verifikasi, bukan

hanya peningkatan akses teknologi (Fendt et al., 2023).

Aspek privasi perlu mendapat perhatian khusus karena penggunaan teknologi digital hampir selalu melibatkan pengumpulan, pemrosesan, dan pertukaran data pribadi. Kajian terbaru mengenai privasi di era digital menekankan bahwa privasi dan keamanan siber saling berkaitan, terutama karena perlindungan pengguna bergantung pada kemampuan memahami serangan, kontrol akses, dan mitigasi risiko dasar dalam penggunaan sistem digital (Farnell et al., 2024).

Konteks Indonesia memperlihatkan bahwa penguatan literasi digital perlu didukung oleh kolaborasi, inovasi, dan keberlanjutan pendidikan digital. Penelitian terbaru di Indonesia menegaskan pentingnya ekosistem pembelajaran yang mendorong kerja sama lintas pihak dalam memperkuat kemampuan digital masyarakat. Hal ini relevan bagi kegiatan pengabdian karena peningkatan literasi digital akan lebih efektif apabila disesuaikan dengan kebutuhan lokal dan dilaksanakan secara partisipatif (Sari et al., 2024).

Pelatihan keamanan siber yang efektif tidak cukup hanya memberikan informasi mengenai ancaman, tetapi juga harus membentuk perilaku perlindungan yang nyata. Tinjauan kritis mengenai framework dan model pelatihan keamanan siber menunjukkan bahwa program awareness yang jelas dan terstruktur dapat menurunkan insiden keamanan sekaligus memperkuat ketahanan siber. Temuan ini mendukung pentingnya pendekatan pengabdian yang menggabungkan edukasi, simulasi, dan praktik langsung (Taherdoost, 2024).

Perkembangan generative artificial intelligence semakin menambah urgensi penguatan literasi digital lanjutan karena teknologi ini dapat menghasilkan teks, gambar, audio, dan video yang tampak meyakinkan. Tinjauan cakupan terbaru menunjukkan bahwa AI generatif memiliki peran ganda: dapat memperkuat penyebaran misinformasi, tetapi juga dapat dimanfaatkan untuk mendeteksi dan memitigasi konten palsu. Kondisi ini menuntut masyarakat memiliki kemampuan berpikir kritis yang lebih tinggi dalam menilai keandalan informasi digital (Park & Nan, 2026).

Kegiatan pengabdian kepada masyarakat dengan fokus pada peningkatan literasi digital lanjutan dan keamanan siber menjadi relevan karena menjawab kebutuhan nyata pengguna teknologi dalam menghadapi risiko digital sehari-hari. Edukasi yang menekankan perlindungan data pribadi, keamanan akun, verifikasi informasi, dan kewaspadaan terhadap ancaman siber diharapkan mampu membentuk masyarakat yang lebih aman, kritis, dan bertanggung jawab dalam memanfaatkan teknologi. Oleh karena itu, tema ini layak dikembangkan sebagai dasar program pengabdian yang mendukung terbentuknya masyarakat cakap digital dan memiliki ketahanan siber yang lebih baik (OECD, 2024a; UNESCO, 2024; World Economic Forum, 2024).

2. TINJAUAN PUSTAKA

Literasi digital merupakan kemampuan individu dalam mengakses, memahami, mengevaluasi, menciptakan, dan memanfaatkan informasi melalui teknologi digital secara efektif, kritis, dan bertanggung jawab. Dalam perkembangannya, literasi digital tidak lagi dipahami hanya sebagai keterampilan teknis menggunakan perangkat, tetapi juga mencakup kemampuan berpikir kritis, etika digital, keamanan, privasi, dan partisipasi sosial di ruang digital. Perspektif ini menunjukkan bahwa literasi digital memiliki cakupan yang luas karena berkaitan dengan bagaimana seseorang berinteraksi secara sadar dan aman dalam ekosistem digital modern (UNESCO, 2024; OECD, 2024a).

Literasi digital lanjutan merujuk pada tingkat kemampuan yang lebih tinggi, yaitu kemampuan untuk mengelola risiko digital, memahami konsekuensi penggunaan teknologi, serta mengambil keputusan yang tepat dalam aktivitas daring. Pada tahap ini, individu tidak hanya mampu menggunakan aplikasi dan platform digital, tetapi juga memahami keamanan akun, pengaturan privasi, perlindungan data pribadi,

serta cara mengenali ancaman digital yang dapat merugikan. Dengan demikian, literasi digital lanjutan menempatkan pengguna sebagai aktor yang aktif, kritis, dan sadar risiko dalam menggunakan teknologi (Buchan et al., 2024).

Konsep literasi digital lanjutan sangat berkaitan dengan kemampuan evaluatif terhadap informasi. Pengguna digital saat ini dihadapkan pada arus informasi yang sangat besar, sehingga diperlukan kemampuan untuk membedakan informasi yang valid, menyesatkan, atau palsu. Dalam konteks ini, literasi digital mencakup kemampuan memverifikasi sumber, memahami konteks informasi, dan menilai kredibilitas konten sebelum menerima atau menyebarkannya. Kemampuan tersebut menjadi penting karena lingkungan digital memungkinkan informasi menyebar dengan cepat tanpa proses verifikasi yang memadai (McGrew & Kohnen, 2024; Aïmeur et al., 2023).

Misinformasi, disinformasi, dan berita palsu merupakan salah satu tantangan utama dalam ekosistem digital saat ini. Konten palsu sering kali dirancang menyerupai informasi yang benar sehingga sulit dibedakan hanya dari tampilan luarnya. Dalam banyak kasus, pengguna yang tidak memiliki keterampilan verifikasi informasi yang baik cenderung lebih mudah mempercayai atau bahkan menyebarkan informasi yang tidak akurat. Oleh karena itu, literasi digital lanjutan harus mencakup kemampuan literasi informasi yang kuat agar masyarakat dapat membangun sikap yang lebih kritis dalam menerima konten digital (Aïmeur et al., 2023).

Pendekatan lateral reading menjadi salah satu strategi penting dalam meningkatkan kemampuan verifikasi informasi digital. Strategi ini mendorong pengguna untuk tidak hanya membaca isi suatu informasi secara langsung, tetapi juga memeriksa sumber lain, menelusuri asal informasi, dan membandingkannya dengan referensi yang lebih kredibel. Penelitian menunjukkan bahwa pelatihan berbasis lateral reading dapat membantu meningkatkan kemampuan peserta dalam mengevaluasi kebenaran informasi online. Hal ini menegaskan bahwa penguatan literasi digital perlu dibangun melalui pembelajaran yang terstruktur dan praktis (Fendt et al., 2023).

Selain aspek informasi, literasi digital lanjutan juga memiliki hubungan erat dengan keamanan siber. Keamanan siber merupakan upaya untuk melindungi sistem, jaringan, data, dan aktivitas digital dari berbagai ancaman yang dapat mengganggu kerahasiaan, integritas, dan ketersediaan informasi. Dalam konteks pengguna umum, keamanan siber berkaitan dengan kebiasaan menggunakan kata sandi yang kuat, mengaktifkan autentikasi dua faktor, mengenali tautan berbahaya, mengelola privasi akun, dan melindungi data pribadi dari penyalahgunaan (World Economic Forum, 2024).

Ancaman siber yang umum dihadapi masyarakat meliputi phishing, malware, social engineering, pencurian identitas, penipuan digital, dan pembajakan akun. Ancaman tersebut tidak hanya menyasar lembaga besar, tetapi juga individu dan komunitas biasa yang aktif menggunakan layanan digital. Meningkatnya ketergantungan masyarakat terhadap internet membuat potensi kerugian akibat serangan siber semakin besar. Oleh sebab itu, keamanan siber perlu dipahami sebagai bagian dari kecakapan dasar yang harus dimiliki setiap pengguna teknologi digital (World Economic Forum, 2024; Taherdoost, 2024).

Berbagai penelitian menunjukkan bahwa perilaku keamanan digital dipengaruhi oleh tingkat literasi digital pengguna. Semakin baik kemampuan seseorang dalam memahami teknologi dan risiko digital, semakin besar kemungkinannya untuk menerapkan perilaku keamanan yang tepat. Perilaku tersebut mencakup kehati-hatian dalam berbagi data, kewaspadaan terhadap pesan mencurigakan, serta penggunaan fitur perlindungan akun dan perangkat. Hubungan ini menunjukkan bahwa penguatan literasi digital dapat menjadi fondasi penting dalam membangun budaya keamanan siber di masyarakat (Nguyen et al., 2024).

Privasi digital juga merupakan komponen utama dalam literasi digital lanjutan. Privasi berkaitan dengan kemampuan individu untuk memahami bagaimana data pribadi dikumpulkan, digunakan, disimpan, dan

dibagikan dalam sistem digital. Banyak pengguna yang belum sepenuhnya menyadari bahwa aktivitas sederhana seperti mengunduh aplikasi, mengisi formulir online, atau menggunakan media sosial dapat membuka akses luas terhadap data pribadi mereka. Dalam konteks ini, literasi digital lanjutan membantu individu memahami risiko privasi serta menerapkan langkah-langkah perlindungan yang tepat (Farnell et al., 2024).

Penguatan keamanan siber melalui edukasi menjadi sangat penting karena banyak insiden keamanan sebenarnya disebabkan oleh faktor manusia. Kelalaian, kurangnya pengetahuan, dan rendahnya kesadaran risiko sering menjadi pintu masuk bagi ancaman digital. Tinjauan kritis terhadap model pelatihan keamanan siber menunjukkan bahwa program awareness yang dirancang dengan baik dapat meningkatkan kemampuan pengguna dalam mengenali dan mencegah ancaman. Dengan demikian, pendidikan keamanan siber tidak hanya berfungsi menambah pengetahuan, tetapi juga membentuk kebiasaan digital yang lebih aman (Taherdoost, 2024).

Konteks pendidikan masyarakat menempatkan pengabdian kepada masyarakat sebagai sarana strategis untuk meningkatkan literasi digital lanjutan dan keamanan siber. Melalui pengabdian, perguruan tinggi dapat mentransformasikan hasil kajian akademik menjadi bentuk edukasi yang lebih praktis, sederhana, dan sesuai dengan kebutuhan masyarakat. Program pelatihan, sosialisasi, simulasi, dan pendampingan dapat membantu masyarakat memahami risiko digital yang mereka hadapi sekaligus membangun kemampuan untuk melindungi diri secara mandiri.

Pendekatan partisipatif dalam pengabdian menjadi penting karena masyarakat memiliki tingkat pengalaman dan kebutuhan digital yang berbeda-beda. Materi literasi digital dan keamanan siber akan lebih efektif jika disusun berdasarkan konteks pengguna, seperti penggunaan media sosial, transaksi digital, aktivitas pembelajaran daring, atau pengelolaan data komunitas. Pendekatan kontekstual semacam ini memungkinkan peserta tidak hanya memahami materi secara teoritis, tetapi juga mampu mengaitkannya dengan situasi yang mereka alami dalam kehidupan sehari-hari (Sari et al., 2024).

Perkembangan teknologi baru, termasuk artificial intelligence generatif, juga memperluas tantangan literasi digital dan keamanan siber. Teknologi ini mampu menghasilkan konten yang tampak sangat meyakinkan, sehingga meningkatkan risiko penyebaran misinformasi dan manipulasi digital. Pada saat yang sama, AI juga dapat digunakan untuk membantu deteksi ancaman dan identifikasi konten palsu. Kondisi ini menunjukkan bahwa masyarakat memerlukan tingkat literasi digital yang lebih tinggi agar mampu memahami perubahan lanskap informasi digital yang semakin kompleks (Park & Nan, 2026).

Kerangka teoritis dalam kegiatan pengabdian ini berangkat dari pemahaman bahwa literasi digital lanjutan dan keamanan siber merupakan dua aspek yang saling terkait. Literasi digital tanpa kesadaran keamanan akan membuat pengguna rentan terhadap ancaman, sedangkan pemahaman keamanan tanpa kemampuan evaluasi informasi juga belum cukup untuk menghadapi dinamika ruang digital. Oleh karena itu, keduanya perlu dikembangkan secara terpadu agar masyarakat tidak hanya mahir menggunakan teknologi, tetapi juga aman, kritis, dan bertanggung jawab dalam memanfaatkannya (UNESCO, 2024; OECD, 2024a).

Berdasarkan uraian tersebut, tinjauan pustaka ini menegaskan bahwa peningkatan literasi digital lanjutan dan keamanan siber memiliki landasan konseptual yang kuat dalam studi literasi digital, literasi informasi, privasi digital, dan cybersecurity awareness. Penguatan kemampuan masyarakat pada aspek-aspek tersebut sangat relevan untuk dilakukan melalui kegiatan pengabdian kepada masyarakat, karena dapat membantu membentuk perilaku digital yang lebih aman, kritis, dan adaptif terhadap perubahan teknologi. Dengan demikian, program pengabdian bertema peningkatan literasi digital lanjutan dan keamanan siber menjadi penting sebagai upaya membangun masyarakat yang lebih siap menghadapi tantangan era digital.

3. METODE PELAKSANAAN

Kegiatan pengabdian kepada masyarakat ini dilaksanakan dengan pendekatan edukatif, partisipatif, dan aplikatif untuk meningkatkan literasi digital lanjutan serta kesadaran keamanan siber pada masyarakat sasaran. Pendekatan edukatif digunakan untuk memberikan pemahaman konseptual mengenai literasi digital, perlindungan data pribadi, verifikasi informasi, dan keamanan aktivitas daring. Pendekatan partisipatif diterapkan dengan melibatkan peserta secara aktif dalam diskusi, praktik, dan evaluasi, sedangkan pendekatan aplikatif digunakan agar materi yang diberikan dapat langsung diterapkan dalam kehidupan sehari-hari.

Sasaran kegiatan adalah kelompok masyarakat yang telah memanfaatkan teknologi digital dalam aktivitas belajar, bekerja, berkomunikasi, maupun bertransaksi, tetapi masih memiliki keterbatasan dalam memahami risiko digital dan cara melindungi diri di ruang siber. Peserta dapat berasal dari kalangan pelajar, mahasiswa, guru, aparatur desa, pelaku UMKM, maupun masyarakat umum yang aktif menggunakan media sosial, aplikasi komunikasi, layanan keuangan digital, dan berbagai platform daring lainnya. Penentuan sasaran dilakukan berdasarkan kebutuhan mitra dan kondisi lapangan.

Metode pelaksanaan kegiatan disusun dalam beberapa tahapan, yaitu persiapan, identifikasi masalah dan analisis kebutuhan, penyusunan materi, pelaksanaan sosialisasi dan pelatihan, praktik dan simulasi, pendampingan, serta evaluasi. Rangkaian tahapan ini dirancang secara sistematis agar kegiatan tidak hanya menambah pengetahuan peserta, tetapi juga membangun keterampilan praktis dan kebiasaan digital yang lebih aman. Setiap tahap saling berkaitan dan mendukung pencapaian tujuan program pengabdian.

Tahap persiapan diawali dengan koordinasi antara tim pelaksana dan pihak mitra untuk menyepakati tujuan kegiatan, waktu pelaksanaan, jumlah peserta, lokasi, serta sarana pendukung yang dibutuhkan. Pada tahap ini juga dilakukan observasi awal untuk melihat tingkat pemanfaatan teknologi digital oleh peserta, jenis aplikasi yang paling sering digunakan, dan persoalan umum yang sering dihadapi saat beraktivitas di ruang digital. Hasil observasi awal ini menjadi dasar untuk merancang bentuk kegiatan yang sesuai dengan kebutuhan peserta.

Tahap identifikasi masalah dan analisis kebutuhan dilakukan melalui wawancara, diskusi kelompok, dan penyebaran angket awal. Wawancara dan diskusi digunakan untuk menggali pengalaman peserta terkait penggunaan media sosial, keamanan akun, penyebaran informasi, perlindungan data pribadi, serta ancaman digital seperti penipuan online dan phishing. Angket awal digunakan untuk mengetahui tingkat pemahaman awal peserta mengenai literasi digital lanjutan dan keamanan siber. Dari tahap ini diperoleh gambaran mengenai kebutuhan utama peserta yang kemudian dijadikan acuan dalam penyusunan materi.

Materi kegiatan disusun berdasarkan hasil analisis kebutuhan dan difokuskan pada beberapa topik utama, yaitu konsep literasi digital lanjutan, etika dan tanggung jawab digital, keamanan akun, pengelolaan kata sandi yang kuat, autentikasi dua langkah, perlindungan data pribadi, keamanan media sosial, keamanan transaksi digital, pengenalan phishing dan social engineering, serta cara memverifikasi kebenaran informasi di internet. Materi dirancang dalam bahasa yang sederhana, komunikatif, dan kontekstual agar mudah dipahami oleh peserta dari berbagai latar belakang.

Pelaksanaan kegiatan dilakukan dalam bentuk sosialisasi dan pelatihan. Pada sesi sosialisasi, peserta diberikan pemahaman mengenai pentingnya literasi digital lanjutan dan keamanan siber dalam kehidupan sehari-hari. Pada sesi pelatihan, materi disampaikan melalui ceramah interaktif, diskusi, tanya jawab, dan demonstrasi. Metode ini dipilih agar peserta tidak hanya menerima penjelasan secara satu arah, tetapi juga memiliki kesempatan untuk mengajukan pertanyaan, berbagi pengalaman, dan memahami contoh nyata dari ancaman digital yang sering terjadi.

Tahap praktik dan simulasi menjadi bagian penting dalam metode pelaksanaan. Peserta diajak untuk

langsung mempraktikkan beberapa langkah pengamanan digital, seperti membuat kata sandi yang kuat, mengaktifkan autentikasi dua faktor, memeriksa pengaturan privasi akun, mengenali ciri-ciri pesan phishing, dan mengevaluasi keaslian informasi yang beredar di media digital. Simulasi ini bertujuan agar peserta memperoleh pengalaman langsung dalam mengidentifikasi risiko digital dan menerapkan langkah pencegahan yang tepat.

Setelah pelatihan dan simulasi, kegiatan dilanjutkan dengan tahap pendampingan. Pendampingan dilakukan untuk membantu peserta yang masih mengalami kesulitan dalam menerapkan materi, baik saat mengatur keamanan akun, memahami pengelolaan data pribadi, maupun saat menilai kredibilitas informasi digital. Pendampingan dilakukan secara langsung selama kegiatan dan dapat dilanjutkan secara terbatas melalui komunikasi dengan pihak mitra. Tahap ini bertujuan agar peserta tidak hanya memahami teori, tetapi benar-benar mampu menerapkannya dalam aktivitas digital sehari-hari.

Evaluasi kegiatan dilakukan untuk mengukur keberhasilan program dalam meningkatkan pemahaman dan keterampilan peserta. Evaluasi dilaksanakan melalui angket sebelum dan sesudah pelatihan, observasi selama kegiatan, serta diskusi reflektif pada akhir program. Angket digunakan untuk mengetahui perubahan tingkat pemahaman peserta, observasi dilakukan untuk melihat partisipasi dan kemampuan peserta saat praktik, sedangkan diskusi reflektif digunakan untuk memperoleh masukan mengenai manfaat kegiatan dan kebutuhan tindak lanjut.

Indikator keberhasilan kegiatan ini meliputi meningkatnya pemahaman peserta tentang literasi digital lanjutan, meningkatnya kesadaran terhadap pentingnya keamanan siber, bertambahnya kemampuan peserta dalam melindungi akun dan data pribadi, serta meningkatnya kemampuan peserta dalam mengenali ancaman digital dan memverifikasi informasi sebelum menyebarkannya. Selain itu, keberhasilan juga ditunjukkan oleh tumbuhnya sikap lebih hati-hati, kritis, dan bertanggung jawab dalam penggunaan teknologi digital.

Melalui metode pelaksanaan yang sistematis, kontekstual, dan berbasis praktik, kegiatan pengabdian ini diharapkan mampu memberikan dampak nyata bagi masyarakat dalam membangun perilaku digital yang lebih aman dan cerdas. Peningkatan literasi digital lanjutan dan keamanan siber tidak hanya penting untuk melindungi individu dari risiko digital, tetapi juga untuk membentuk masyarakat yang lebih siap menghadapi dinamika transformasi teknologi secara berkelanjutan.

4. HASIL DAN PEMBAHASAN

Kegiatan Kegiatan pengabdian kepada masyarakat dengan tema peningkatan literasi digital lanjutan dan keamanan siber memberikan hasil yang menunjukkan adanya peningkatan pemahaman, kesadaran, dan keterampilan peserta dalam menghadapi risiko digital. Sebelum kegiatan dilaksanakan, sebagian besar peserta masih memandang penggunaan teknologi digital hanya sebagai sarana komunikasi, hiburan, pembelajaran, dan akses informasi tanpa disertai pemahaman yang memadai mengenai ancaman keamanan siber. Kondisi awal ini terlihat dari kebiasaan peserta yang masih menggunakan kata sandi sederhana, belum mengaktifkan autentikasi dua langkah, kurang memahami pentingnya perlindungan data pribadi, dan belum terbiasa memverifikasi informasi sebelum membagikannya kepada orang lain.

Hasil identifikasi awal menunjukkan bahwa masalah utama yang dihadapi peserta tidak hanya terletak pada keterbatasan pengetahuan teknis, tetapi juga pada rendahnya kesadaran terhadap risiko digital dalam aktivitas sehari-hari. Sebagian peserta belum memahami bahwa tindakan sederhana seperti mengklik tautan yang tidak jelas, menggunakan jaringan publik tanpa kewaspadaan, atau membagikan data pribadi di media sosial dapat menimbulkan ancaman serius terhadap keamanan akun dan informasi pribadi. Temuan ini menunjukkan bahwa kebutuhan peserta bukan sekadar pengenalan teknologi, melainkan peningkatan

literasi digital pada tingkat yang lebih lanjut dan aplikatif.

Pelaksanaan sosialisasi dan pelatihan memberikan dampak positif terhadap pemahaman peserta mengenai konsep literasi digital lanjutan. Peserta mulai memahami bahwa literasi digital tidak hanya berarti mampu menggunakan perangkat atau aplikasi, tetapi juga mencakup kemampuan berpikir kritis, menjaga keamanan akun, mengelola jejak digital, melindungi data pribadi, serta menilai keandalan informasi digital. Perubahan pemahaman ini menjadi hasil penting karena menunjukkan adanya pergeseran cara pandang peserta dari pengguna teknologi pasif menjadi pengguna yang lebih sadar risiko dan bertanggung jawab.

Pada aspek keamanan siber, hasil kegiatan menunjukkan adanya peningkatan kesadaran peserta terhadap pentingnya pengamanan akun digital. Setelah mengikuti pelatihan, peserta lebih memahami fungsi kata sandi yang kuat, risiko penggunaan kata sandi yang sama pada banyak akun, pentingnya autentikasi dua faktor, dan perlunya memperbarui pengaturan keamanan secara berkala. Dalam sesi praktik, sebagian besar peserta mampu mengikuti langkah-langkah pengamanan akun dengan baik, seperti mengganti kata sandi menjadi lebih kuat, meninjau perangkat yang terhubung, dan mengaktifkan fitur keamanan tambahan pada akun media sosial maupun layanan digital lainnya.

Peningkatan pemahaman juga terlihat pada kemampuan peserta dalam mengenali bentuk-bentuk ancaman digital. Sebelum kegiatan, banyak peserta belum dapat membedakan pesan atau tautan yang aman dan yang berpotensi berbahaya. Setelah dilakukan pelatihan dan simulasi, peserta mulai mampu mengidentifikasi ciri-ciri phishing, pesan penipuan, permintaan data mencurigakan, dan pola rekayasa sosial yang sering digunakan untuk memperoleh akses terhadap akun atau informasi pribadi. Hasil ini menunjukkan bahwa metode simulasi dan contoh kasus nyata cukup efektif dalam membantu peserta memahami bentuk ancaman yang sering mereka jumpai di ruang digital.

Dalam aspek perlindungan data pribadi, kegiatan ini juga menghasilkan perubahan positif. Peserta mulai memahami bahwa data pribadi seperti nomor telepon, alamat email, nomor identitas, lokasi, serta informasi akun memiliki nilai penting dan tidak boleh dibagikan secara sembarangan. Sebelumnya, sebagian peserta belum menyadari bahwa kebiasaan membagikan informasi tertentu di media sosial atau platform digital dapat membuka peluang penyalahgunaan data. Setelah pelatihan, peserta menjadi lebih berhati-hati dalam mengunggah informasi, mengatur privasi akun, dan membatasi akses aplikasi terhadap data pribadi mereka.

Hasil lain yang cukup menonjol adalah meningkatnya kemampuan peserta dalam memverifikasi informasi digital. Pada kondisi awal, beberapa peserta masih cenderung mempercayai dan menyebarkan informasi berdasarkan tampilan judul, sumber yang tampak populer, atau isi pesan yang sesuai dengan keyakinan pribadi. Setelah kegiatan berlangsung, peserta mulai memahami pentingnya memeriksa sumber informasi, membandingkan dengan referensi lain, memperhatikan konteks, dan tidak langsung membagikan konten yang belum terverifikasi. Perubahan ini sangat penting karena menunjukkan bahwa literasi digital lanjutan tidak hanya berkaitan dengan keamanan teknis, tetapi juga dengan kualitas perilaku informasi masyarakat.

Pelaksanaan praktik dan simulasi memberikan kontribusi besar terhadap keberhasilan kegiatan. Peserta tidak hanya menerima materi secara teoritis, tetapi juga diberi kesempatan untuk langsung menerapkan langkah-langkah pengamanan digital. Dalam praktik tersebut, peserta tampak lebih mudah memahami materi karena dapat langsung melihat hubungan antara penjelasan konsep dengan penerapannya pada akun dan perangkat yang mereka gunakan sehari-hari. Pendekatan ini membantu mengurangi kesan bahwa keamanan siber adalah hal yang rumit dan hanya dapat dilakukan oleh orang yang memiliki kemampuan teknis tinggi.

Pembahasan hasil kegiatan menunjukkan bahwa pendekatan edukatif yang dipadukan dengan simulasi praktis sangat efektif untuk meningkatkan kesiapan digital peserta. Hal ini disebabkan karena ancaman siber sering kali bersifat konkret dan dekat dengan aktivitas harian, sehingga materi menjadi lebih mudah

dipahami ketika dikaitkan langsung dengan pengalaman pengguna. Peserta lebih mudah menyadari pentingnya keamanan akun ketika mereka memahami contoh kasus pembajakan media sosial, penipuan melalui tautan palsu, atau kebocoran data yang dapat terjadi akibat kelalaian kecil. Dengan demikian, kegiatan pengabdian ini berhasil menghubungkan pengetahuan teoretis dengan realitas digital yang dihadapi peserta.

Kegiatan ini juga menunjukkan bahwa peningkatan literasi digital lanjutan memerlukan pendekatan yang kontekstual. Peserta dengan latar belakang yang berbeda memiliki kebutuhan yang berbeda pula dalam penggunaan teknologi. Peserta yang aktif menggunakan media sosial lebih tertarik pada isu privasi akun dan penyebaran informasi, sedangkan peserta yang sering bertransaksi digital lebih tertarik pada keamanan data dan kewaspadaan terhadap penipuan. Kondisi ini menunjukkan bahwa efektivitas kegiatan pengabdian meningkat ketika materi disesuaikan dengan kebiasaan digital dan kebutuhan riil peserta.

Dari sisi partisipasi, kegiatan menunjukkan respons yang baik dari peserta. Peserta aktif dalam diskusi, mengajukan pertanyaan, dan berbagi pengalaman mengenai masalah digital yang pernah mereka alami. Tingginya partisipasi ini menunjukkan bahwa isu literasi digital lanjutan dan keamanan siber memang dirasakan relevan dan dekat dengan kehidupan peserta. Keterlibatan aktif peserta juga memperkuat proses pembelajaran karena pengalaman nyata yang dibagikan selama diskusi membantu peserta lain memahami bahwa ancaman digital merupakan persoalan yang dapat terjadi pada siapa saja.

Walaupun memberikan hasil yang positif, kegiatan ini juga menemukan beberapa kendala. Sebagian peserta masih mengalami kesulitan dalam memahami istilah-istilah teknis tertentu yang berkaitan dengan keamanan siber. Selain itu, tidak semua peserta memiliki tingkat kesiapan yang sama dalam mengikuti praktik digital, terutama peserta yang memiliki keterbatasan pengalaman menggunakan pengaturan akun atau fitur keamanan perangkat. Kendala lain adalah masih adanya anggapan bahwa langkah pengamanan digital memerlukan proses yang rumit dan menyita waktu. Hal ini menunjukkan bahwa pendampingan lanjutan masih diperlukan agar perubahan perilaku dapat berlangsung secara berkelanjutan.

Untuk mengatasi kendala tersebut, pendekatan penyampaian materi secara sederhana dan berbasis contoh sehari-hari terbukti menjadi strategi yang efektif. Penjelasan yang mengaitkan keamanan siber dengan aktivitas biasa, seperti menerima pesan di aplikasi perpesanan, membuka email, menggunakan Wi-Fi publik, atau berbelanja online, membuat peserta lebih mudah memahami bahwa keamanan digital adalah bagian dari kebiasaan hidup sehari-hari. Selain itu, penggunaan simulasi sederhana membantu peserta melihat bahwa perlindungan digital dapat dimulai dari langkah kecil, seperti memperkuat kata sandi atau meninjau pengaturan privasi akun.

Secara keseluruhan, hasil kegiatan menunjukkan bahwa program pengabdian ini berhasil meningkatkan pemahaman peserta tentang literasi digital lanjutan dan keamanan siber. Peningkatan tersebut terlihat pada aspek kesadaran risiko, pemahaman perlindungan data pribadi, kemampuan mengenali ancaman digital, keterampilan mengamankan akun, dan kebiasaan memverifikasi informasi. Perubahan ini menunjukkan bahwa intervensi edukatif yang dirancang secara partisipatif dan aplikatif dapat memberikan dampak nyata dalam membentuk perilaku digital yang lebih aman, kritis, dan bertanggung jawab.

Pembahasan dari hasil kegiatan ini menegaskan bahwa penguatan literasi digital lanjutan dan keamanan siber merupakan kebutuhan penting dalam masyarakat digital saat ini. Penggunaan teknologi yang semakin luas harus diimbangi dengan kesiapan pengguna untuk melindungi diri, data, dan aktivitas digital mereka. Melalui kegiatan pengabdian seperti ini, masyarakat tidak hanya memperoleh pengetahuan baru, tetapi juga dibekali keterampilan praktis yang dapat langsung diterapkan. Dengan demikian, program ini berkontribusi dalam membangun masyarakat yang lebih cakap digital, lebih tangguh menghadapi ancaman siber, dan lebih bijak dalam memanfaatkan teknologi.

5. KESIMPULAN

Kegiatan pengabdian kepada masyarakat dengan tema Peningkatan Literasi Digital Lanjutan dan Keamanan Siber telah memberikan hasil yang positif dalam meningkatkan pemahaman, kesadaran, dan keterampilan peserta dalam menghadapi berbagai risiko di ruang digital. Sebelum kegiatan dilaksanakan, peserta pada umumnya telah terbiasa menggunakan teknologi digital dalam aktivitas sehari-hari, tetapi belum sepenuhnya memahami pentingnya perlindungan data pribadi, keamanan akun, verifikasi informasi, dan kewaspadaan terhadap ancaman siber. Setelah mengikuti rangkaian kegiatan, peserta menunjukkan peningkatan pemahaman mengenai literasi digital lanjutan sebagai kemampuan yang tidak hanya berkaitan dengan penggunaan teknologi, tetapi juga dengan kemampuan berpikir kritis, menjaga keamanan, dan bertindak secara bertanggung jawab di ruang digital.

DAFTAR PUSTAKA

Adeshola, I., & Oluwajana, D. I. (2025). Assessing cybersecurity awareness among university students: Implications for educational interventions. *Journal of Computers in Education, 12*, 1283–1305.

Aïmeur, E., Amri, S., & Brassard, G. (2023). Fake news, disinformation and misinformation in social media: A review. *Social Network Analysis and Mining, 13*(1), Article 30. https://doi.org/10.1007/s13278-023-01028-5

Buchan, M. C., Bhawra, J., & Katapally, T. R. (2024). Navigating the digital world: Development of an evidence-based digital literacy program and assessment tool for youth. *Smart Learning Environments, 11*, Article 17. https://doi.org/10.1186/s40561-024-00293-x

Farnell, C., Huff, P., & Cox, W. (2024). Privacy in the digital age: Navigating the risks and benefits of cybersecurity measures. In *Human Privacy in Virtual and Physical Worlds*. Springer.

Fendt, M., Nistor, N., Scheibenzuber, C., & Artmann, B. (2023). Sourcing against misinformation: Effects of a scalable lateral reading training based on cognitive apprenticeship. *Computers in Human Behavior, 146*, 107820. https://doi.org/10.1016/j.chb.2023.107820

McGrew, S., & Kohnen, A. M. (2024). Tackling misinformation through online information literacy: Structural and contextual considerations. *Journal of Research on Technology in Education, 56*(1), 1–6. https://doi.org/10.1080/15391523.2023.2280385

Nguyen, T. T., Tran, T. N. H., Do, T. H. M., Dinh, T. K. L., Nguyen, T. U. N., & Dang, T. M. K. (2024). Digital literacy, online security behaviors and e-payment intention. *Journal of Open Innovation: Technology, Market, and Complexity, 10*, 100292. https://doi.org/10.1016/j.joitmc.2024.100292

OECD. (2024a). *OECD digital economy outlook 2024 (Volume 1): Embracing the technology frontier*. OECD Publishing.

OECD. (2024b). *OECD digital economy outlook 2024 (Volume 2)*. OECD Publishing.

Park, S., & Nan, X. (2026). Generative AI and misinformation: A scoping review of the role of generative AI in the generation, detection, mitigation, and impact of misinformation. *AI & Society, 41*, 1501–1515.

Sari, G. I., Winasis, S., Pratiwi, I., Nuryanto, U. W., & Basrowi. (2024). Strengthening digital literacy in Indonesia: Collaboration, innovation, and sustainability education. *Social Sciences & Humanities Open, 10*, 101100. https://doi.org/10.1016/j.ssaho.2024.101100

Taherdoost, H. (2024). A critical review on cybersecurity awareness frameworks and training models. *Procedia Computer Science, 235*, 1649–1663. https://doi.org/10.1016/j.procs.2024.03.180

UNESCO. (2024). *Digital literacy assessment*. UNESCO.

World Economic Forum. (2024). *Global cybersecurity outlook 2024*. World Economic Forum.