Abdimas Mandalika
http://journal.ummat.ac.id/index.php/mandalika
ISSN 2807-5943
Vol. 4, No. 4, Agustus 2025, Hal. 295-304

Keamanan Digital untuk Generasi Muda: Meningkatkan Kesadaran dan Keterampilan Anak Asuh Panti Al Hasanat

[1]Neneng Rachmalia Feta, [2]Fitria, [3]Agus Trihandoyo, [4]Elin Panca Saputra, [5]Priyono, [6]Talitha Khansa Fahira, [7]Syaikhah Aditya Ramadhani, [8]Adnan Syukur
[1]Program Studi Sistem dan Teknologi Informasi, Universitas Siber Indonesia, Indonesia
Corresponding Author. Email : nrachmaliafeta@cyber-univ.ac.id

ARTICLE INFO

Article History:

Received : 23-06-2025
Revised : 05-08-2025
Accepted : 06-08-2025
Online : 10-08-2025

Keywords:
Keamanan Digital;
Malware; Phising;

ABSTRACT

Abstract: *The rapid development of digital technology is accompanied by cybersecurity risks, particularly for teenagers who lack digital literacy. This community service activity aims to increase the digital security awareness and skills of the foster children at the Al Hasanat Yatim Piatu Orphanage. The method used was a participatory approach consisting of three stages: presentation, live demonstration, and practice. The training covered material on digital threats such as phishing and malware, the importance of strong passwords, and social media ethics. The results of the activity showed positive response from the participants. They became more aware of the importance of maintaining privacy and personal data security, and expressed a desire to apply the knowledge gained in their daily digital activities.*

Abstrak: Perkembangan teknologi digital yang pesat diiringi dengan risiko keamanan siber, terutama bagi remaja yang kurang memiliki literasi digital. Kegiatan Pengabdian kepada Masyarakat ini bertujuan untuk meningkatkan kesadaran dan keterampilan keamanan digital anak asuh di Panti Asuhan Yatim Piatu Al Hasanat. Metode yang digunakan adalah pendekatan partisipatif yang terdiri dari tiga tahap: presentasi, demonstrasi langsung, dan latihan. Pelatihan ini mencakup materi mengenai ancaman digital seperti phishing dan malware, pentingnya kata sandi yang kuat, serta etika bermedia sosial. Hasil kegiatan menunjukkan respons yang positif dari para peserta. Mereka menjadi lebih sadar akan pentingnya menjaga privasi dan keamanan data pribadi, serta berkeinginan untuk menerapkan pengetahuan yang didapat dalam aktivitas digital sehari-hari

https://doi.org/10.31764/justek.vXiY.ZZZ

A. LATAR BELAKANG

Perkembangan teknologi digital telah memberikan dampak yang sangat besar dalam berbagai aspek kehidupan, termasuk dalam bidang pendidikan, komunikasi, dan hiburan. Namun, di balik berbagai manfaat yang ditawarkan, dunia digital juga menyimpan risiko yang serius, terutama bagi para pengguna yang belum memiliki literasi digital serta pemahaman yang memadai mengenai keamanan siber (Purba et al., 2023). Kelompok anak-anak dan remaja menjadi salah satu kelompok yang paling rentan terhadap risiko ini (Niyu et al., 2021). Khususnya mereka yang tinggal di lingkungan panti asuhan karena sering kali

memiliki keterbatasan akses terhadap edukasi formal mengenai perlindungan data pribadi, etika digital, dan cara menghadapi ancaman di dunia maya.

Mitra dalam kegiatan pengabdian ini, Panti Asuhan Yatim Piatu Al Hasanat, menaungi anak-anak asuh berusia 12 hingga 18 tahun yang sedang menempuh pendidikan di tingkat SMP dan SMK. Berdasarkan hasil observasi awal dan wawancara, diketahui bahwa meskipun anak-anak asuh sudah akrab dengan teknologi seperti *smartphone* dan komputer, penggunaan perangkat tersebut lebih banyak ditujukan untuk hiburan dan media sosial tanpa disertai pemahaman yang mendalam tentang keamanan digital. Permasalahan yang teridentifikasi secara spesifik adalah banyak di antara mereka belum memahami pentingnya penggunaan kata sandi yang kuat, tidak terbiasa dengan pengaturan privasi pada akun media sosial, serta tidak menyadari bahaya dari membagikan informasi pribadi secara sembarangan.

Pemahaman tentang keamanan digital penting untuk dimiliki agar masyarakat dapat menggunakan internet dan media sosial dengan aman (Sidyawati et al., 2021). Hal tersebut karena kejahatan saat ini sudah menyasar pada semua pengguna teknologi, termasuk pada pencurian data pribadi dengan teknik phising. Phising merupakan teknik rekayasa sosial untuk mendapatkan data seseorang dengan seolah-olah menjadi orang terpercaya yang sedang memvalidasi data (Vadila & Pratama, 2021).

Menjawab permasalahan tersebut, Program Studi Sistem dan Teknologi Informasi Universitas Siber Indonesia menyelenggarakan kegiatan Pengabdian kepada Masyarakat (PkM) sebagai wujud kepedulian terhadap pentingnya edukasi keamanan digital bagi generasi muda, khususnya anak-anak asuh di panti. Pendekatan yang dipilih adalah pelatihan berbasis praktik, di mana anak-anak asuh tidak hanya mendengar, tetapi juga diajak untuk belajar secara aktif dan mencoba langsung cara mengamankan akun serta data pribadi mereka.

Beberapa kegiatan PkM terkait keamanan digital yang telah dilakukan diantaranya kegiatan PkM yang diselenggarakan oleh dosen dari Fakultas Ilmu Komputer, Universitas Pamulang, di Pondok Pesantren Nafidatunnajah. Kegiatan ini merupakan sebuah sosialisasi mengenai kesadaran keamanan siber (*Cyber Security Awareness*). Hasil dari kegiatan tersebut diharapkan terciptanya pemahaman mengenai kesadaran keamanan siber sehingga mereka dapat menerapkan tindakan pencegahan untuk terhindar dari kejahatan di dunia maya (Hidayat & Napila, 2024). Kegiatan PkM yang terkait keamanan digital selanjutnya yaitu sosialisasi mengenai keamanan siber pada remaja menghadapi social engineering yang dilaksanakan oleh Program Studi Teknik Informatika, Universitas Raharja. Hasil dari kegiatan tersebut diperoleh bahwa remaja sebagai user terbesar dari media internet belum banyak yang memiliki literasi digital tentang keamanan siber. Selain itu, literasi digital yang dimiliki juga belum memadai untuk menghadapi serangan kejahatan siber (Effendy & Oktiani, 2024).

Berdasarkan hasil permasalahan yang diperoleh pada mitra Panti Asuhan Yatim Piatu Al Hasanat terkait keamanan digital, kegiatan PkM yang dilakukan mencakup penyampaian materi mengenai jenis-jenis ancaman digital seperti phishing dan malware, pentingnya kata sandi yang kuat, dan etika digital di media sosial. Selain itu, kegiatan ini memfasilitasi sesi praktik langsung yang memungkinkan peserta untuk berlatih membuat kata sandi yang aman, mengatur privasi akun, dan melakukan simulasi untuk mengenali upaya penipuan. Dengan pendekatan ini, pengetahuan teoritis dapat langsung diaplikasikan menjadi kebiasaan digital yang lebih aman.

Kegiatan ini secara keseluruhan bertujuan untuk membentuk peserta agar menjadi individu yang lebih bijak dan bertanggung jawab dalam menggunakan teknologi digital. Tujuan utamanya adalah tidak hanya sekadar memahami teori keamanan, tetapi juga mampu membentuk kebiasaan digital yang sehat, menjaga privasi saat beraktivitas online, serta mampu menghindari konten maupun interaksi yang berisiko. Kegiatan PkM ini diharapkan dapat menjadi sarana untuk membangun kesadaran di lingkungan panti asuhan mengenai pentingnya menjadikan keamanan digital sebagai bagian tak terpisahkan dari kehidupan sehari-hari di era modern.

B. METODE PELAKSANAAN

1. Metode Pelaksanaan

Metode pelaksanaan PkM ini menerapkan pendekatan partisipatif melalui tiga tahapan yaitu presentasi, demonstrasi langsung, dan latihan. Tahap presentasi bertujuan untuk memberikan pemahaman teori mengenai pentingnya dan ragam ancaman keamanan digital. Selanjutnya, demonstrasi langsung difokuskan pada visualisasi langkah-langkah pengamanan digital. Kemudian tahapan akhir berupa latihan yang memfasilitasi peserta untuk mengaplikasikan pengetahuan secara langsung. Kombinasi metode yang mengintegrasikan aspek teori, visual, dan aplikatif ini terbukti efektif dalam meningkatkan kompetensi serta partisipasi aktif peserta (Satar et al., 2025).

2. Deskripsi Singkat Profil Mitra

Yayasan Al Hasanat Jaya merupakan lembaga sosial yang berdiri sejak tahun 1993 dan berlokasi di Jalan Pancoran Barat VII B No.70, Pancoran, Jakarta Selatan. Yayasan ini menaungi sekitar 30 anak panti dan 30 anak non-panti, dengan misi membentuk generasi yang bertakwa, berakhlak mulia, cerdas, terampil, mandiri, disiplin, dan bertanggung jawab. Selain mengelola panti asuhan, Yayasan Al Hasanat Jaya juga menaungi dua lembaga pendidikan formal, yaitu SMP Bakti 17 dan SMK Bakti 17, yang berlokasi di Jalan Persahabatan No. 23, Cipedak, Jagakarsa, Jakarta Selatan. Berdasarkan Data Pokok Pendidikan (DAPODIK) SMP Bakti 17 adalah sekolah swasta berakreditasi A yang telah berdiri pada 17 Juli 1985, sementara SMK Bakti 17 adalah sekolah menengah

kejuruan swasta yang berdiri sejak 21 Juli 2009 dan memiliki akreditasi B. Objek binaan dalam kegiatan PkM ini adalah anak-anak asuh yang berada di bawah naungan Yayasan Al Hasanat Jaya sebanyak 20 peserta yang terdiri atas 8 siswa tingkat SMP dan 12 siswa tingkat SMK.

3. Langkah-Langkah Pelaksanaan

Langkah-langkah pelaksanaan kegiatan PkM ini dibagi menjadi tiga tahapan, yaitu tahap persiapan, pelaksanaan, dan evaluasi. Tahapan persiapan diawali dengan melakukan survei awal dan koordinasi langsung dengan pengurus Panti Asuhan Yatim Piatu Al Hasanat. Tujuan dari survei ini adalah untuk melakukan analisis kebutuhan yang mencakup identifikasi profil peserta, pemetaan kondisi akses dan penggunaan teknologi digital, serta penentuan topik-topik keamanan siber yang paling relevan bagi mereka.

Tahapan pelaksanaan kegiatan diselenggarakan di Aula Universitas Siber Indonesia. Metode yang digunakan adalah pelatihan berbasis praktik yang menggabungkan beberapa pendekatan, yaitu presentasi, demonstrasi langsung oleh pemateri, serta sesi latihan pengamanan akun secara mandiri oleh peserta menggunakan PC laboratorium kampus. Materi yang disampaikan mencakup pengenalan ancaman digital, etika dan keamanan media sosial, serta praktik perlindungan data pribadi seperti pembuatan kata sandi yang kuat dan simulasi mengenali phishing.

Tahapan terakhir dalam kegiatan PkM ini adalah evaluasi. Evaluasi dilakukan setelah sesi pelatihan berakhir untuk mengukur efektivitas dan dampak kegiatan terhadap pemahaman peserta. Alat ukur untuk evaluasi yang digunakan adalah kuesioner yang diisi oleh seluruh peserta untuk mendapatkan masukan mengenai kualitas acara, relevansi materi, dan interaktivitas penyampaian. Hasil dari evaluasi ini kemudian dianalisis dan menjadi dasar penyusunan laporan akhir serta menjadi acuan untuk merumuskan rencana tindak lanjut pada kegiatan selanjutnya.

C. HASIL DAN PEMBAHASAN

1. Persiapan

Tahapan kegiatan yang pertama adalah survei awal dan koordinasi langsung bersama pengurus Panti Asuhan Yatim Piatu Al Hasanat. Langkah ini bertujuan untuk mendapatkan kebutuhan mitra, yang mencakup identifikasi profil peserta yaitu anak-anak asuh berusia 12 hingga 18 tahun dan pemetaan kondisi akses digital mereka.

Hasil observasi dan wawancara awal menunjukkan bahwa meskipun para peserta telah familiar dengan teknologi, pemahaman mereka terkait keamanan digital masih rendah dan penggunaan teknologi lebih difokuskan pada hiburan tanpa adanya kesadaran akan risiko keamanan. Hasil tersebut menjadi landasan untuk merancang kegiatan PkM yang relevan dan dapat menjawab

permasalahan yang dihadapi oleh mitra. Tim pelaksana kemudian menyusun proposal kegiatan, mengembangkan modul pelatihan, merancang materi simulasi dan praktik langsung, serta mempersiapkan seluruh kebutuhan logistik seperti sertifikat dan perlengkapan presentasi.

Gambar 1. Survei Awal dan Koordinasi Langsung dengan Pengurus Panti Asuhan Yatim Piatu Al Hasanat

2. Pelaksanaan

Pelaksanaan kegiatan PkM dibagi menjadi tiga (3) sesi, yaitu sesi Presentasi Materi, Sesi Demontrasi Langsung, dan diakhiri dengan Sesi Latihan.

1. Presentasi Materi

Sesi presentasi materi diisi dengan kegiatan dari tim pelaksana yang memaparkan materi mengenai keamanan digital untuk generasi muda yang meliputi jenis-jenis ancaman digital seperti phising dan malware, pentingnya penggunaan kata sandi yang kuat, dan etika digital di media sosial.

Keamanan digital adalah serangkaian praktik, teknologi, dan proses yang dirancang untuk melindungi sistem komputer, jaringan, perangkat, program, dan data dari serangan, kerusakan, atau akses tidak sah (Pratama et al., 2024). Sederhananya, keamanan digital seperti sistem keamanan untuk rumah di dunia maya. Sama seperti mengunci pintu, memasang alarm, dan berhati-hati pada orang asing untuk melindungi rumah, keamanan digital adalah semua tindakan yang dilakukan untuk melindungi aset digital seperti akun media sosial, email, data perbankan, dan file pribadi.

Jenis-jenis ancaman digital yang paling umum adalah malware dan phising. Malware adalah istilah umum untuk perangkat lunak sengaja dibuat untuk menyebabkan kerusakan pada komputer (Rahman et al., 2024). Ada berbagai jenis malware, masing-masing dengan cara kerja yang berbeda. Contohnya adalah virus yang merupakan program jahat yang menempel pada file atau program lain. Ketika file tersebut dibuka, virus akan menyebar dan menginfeksi sistem lain. Kemudian ransomware merupakan program yang sengaja dibuat untuk mengenkripsi (mengunci) file-file di komputer dan meminta uang tebusan untuk membukanya kembali (Rahman et al., 2024).

Sedangkan ancaman selanjutnya adalah phishing yang merupakan upaya penipuan untuk mendapatkan informasi sensitif seperti nama pengguna, kata sandi, dan detail kartu kredit dengan menyamar sebagai orang tepercaya

melalui komunikasi elektronik (Dharani et al., 2024). Biasanya, pelaku mengirim email atau pesan teks yang terlihat seperti dari bank, perusahaan, atau layanan digital, lalu mengarahkan korban ke situs web palsu untuk memasukkan data korban.

Pencegahan terhadap malware dan phishing memerlukan literasi terhadap keamanan digital dan disertai dengan kesadaran individu. Malware dapat dideteksi dini dengan menggunakan aplikasi antivirus. Sedangkan untuk menghindari phising kunci utamanya adalah dengan tidak mengklik tautan atau membuka lampiran dari sumber yang tidak dikenal atau mencurigakan, baik itu melalui email maupun pesan lainnya. Agar data pribadi terlindungi, pemilihan kata sandi yang digunakan untuk membuka media sosial juga perlu diperhatikan (Yildirim & Mackie, 2019).

Gambar 2. Sesi Presentasi Materi

Etika digital adalah tata krama atau sopan santun saat kita berinteraksi di dunia maya (Fahrimal, 2018). Sama seperti di dunia nyata, ada aturan tidak tertulis tentang bagaimana berperilaku yang baik, hormat, dan bertanggung jawab. Di media sosial, di mana interaksi terjadi dengan sangat cepat dan luas, etika ini menjadi penting. Tujuan utamanya adalah menciptakan ruang digital yang aman, positif, dan nyaman untuk semua orang. Contoh etika digital adalah dengan tidak membagikan informasi pribadi secara berlebihan. Hal tersebut mengurangi potensi data pribadu disalahgunakan oleh pihak tidak bertanggung jawab untuk melancarkan serangan *phishing*. Sikap waspada terhadap informasi yang diterima dan dibagikan, serta menghormati privasi diri sendiri dan orang lain di dunia maya, merupakan cerminan etika digital yang sekaligus berfungsi sebagai langkah pencegahan terhadap kejahatan digital (Syahda et al., 2024).

2. Demonstrasi

Setelah penyampaian materi mengenai keamanan digital, kegiatan dilanjutkan dengan sesi demonstrasi yang bertujuan untuk menjembatani konsep dengan praktik. Tim pelaksana mendemokan secara langsung teknik-teknik keamanan digital. Demonstrasi pertama adalah pembuatan kata sandi yang kuat dan unik. Dalam sesi ini, Tim Pelaksana menunjukkan metode penggunaan kata sandi yang memenuhi kriteria kompleksitas dan panjang

sesuai rekomendasi lembaga standar internasional seperti National Institute of Standards and Technology, yang menyarankan penggunaan kata sandi yang panjang dibandingkan menggunakan kombinasi karakter acak yang sulit diingat (Grassi et al., 2020). Beberapa teknik pembuatan kata sandi yang direkomendasikan adalah minimal panjang kata sandi adalah 8 karakter, memiliki satu atau lebih huruf kapital, memiliki satu atau lebih angka, dan memiliki satu atau lebih simbol (Kävrestad, 2020).

Gambar 3. Sesi Demonstrasi dari Tim Pelaksana

Kegiatan dilanjutkan dengan cara-cara untuk melindungi data pribadi pada media sosial Instagram. Pada media sosial tersebut terdapat beberapa pilihan pada menu setting yang dapat digunakan untuk membatasi interaksi dengan pengguna lainnya. Seperti membuat akun menjadi private, membatasi siapa saja yang dapat mengomentari konten yang diupload, membatasi siapa saja yang dapat mengirimkan pesan, serta membatasi siapa saja yang dapat melakukan tagging pada akun Instagram peserta. Juga dilakukan pembahasan konten-konten apa saja yang seharusnya tidak diupload pada media sosial.

Selanjutnya, dilakukan demonstrasi untuk mengidentifikasi phishing melalui analisis sederhana pada aplikasi Whatsapp. Peserta ditunjukkan cara memeriksa tautan (URL) yang mencurigakan, mengenali jenis file yang dikirim, mengenali bahasa yang bersifat mendesak dan manipulatif, serta memeriksa keaslian pengirim.

3. Latihan

Peserta pada sesi terakhir ini mengaplikasikan materi yang telah disampaikan oleh Tim Pelaksana. Setiap peserta dipandu untuk membuat contoh kata sandi baru menggunakan prinsip yang telah didemonstrasikan dan memeriksanya menggunakan perangkat lunak pemeriksa kekuatan kata sandi. Kemudian para peserta membuka media sosial masing-masing dan dilakukan setting privasi pada aplikasi Instagram. Beberapa pilihan terkait privasi pengguna dicoba dan dilakukan pengetesan hasilnya terhadap opsi-opsi yang tersedia. Dilakukan tanya jawab interaktif selama sesi latihan ini untuk meningkatkan pemahaman para peserta. Kemudian peserta diberikan beberapa studi kasus berupa tangkapan layar pesan Whatsapp dan notifikasi media sosial yang dirancang menyerupai upaya phishing. Peserta diminta untuk menganalisis dan memutuskan apakah pesan tersebut aman atau berbahaya, serta menjelaskan alasannya. Metode latihan berbasis pengalaman

ini diharapkan efektif dalam meningkatkan kewaspadaan dan kemampuan analisis kritis peserta.

3. Evaluasi

Proses evaluasi kegiatan telah dilakukan oleh tim pelaksana dengan cara memberikan survei menggunakan Google Form terhadap peserta pelatihan. Survei ini bertujuan untuk memperoleh masukan mengenai kualitas pelaksanaan kegiatan, relevansi materi, efektivitas penyampaian, serta ngukur efektivitas dan dampak kegiatan terhadap pemahaman peserta.

Berdasarkan data dari total 20 responden yang merupakan anak asuh Panti Asuhan Al Hasanat (tingkat SMP dan SMK), diperoleh hasil sebagai berikut:

1. Relevansi Tema dan Materi

Mayoritas peserta menyatakan bahwa tema pelatihan "Keamanan Digital untuk Generasi Muda" sangat sesuai dengan kebutuhan mereka. Ancaman seperti pencurian akun, penipuan daring, serta etika penggunaan media sosial dianggap sangat dekat dengan kehidupan mereka sehari-hari.

2. Kualitas Penyampaian dan Interaktivitas

Sebagian besar peserta memberikan nilai "Puas" dan "Sangat Puas" terhadap cara penyampaian materi. Narasumber dinilai komunikatif dan mudah dipahami, terutama karena banyak menggunakan contoh nyata dan simulasi langsung.

3. Pemahaman dan Dampak Pribadi

Peserta menyatakan bahwa kegiatan ini memberikan pemahaman baru tentang pentingnya melindungi data pribadi dan menggunakan internet secara aman. Banyak dari mereka menyadari bahwa selama ini telah menggunakan media digital tanpa memperhatikan risiko keamanan.

4. Minat untuk Kegiatan Serupa

Sebagian peserta menyatakan "Berminat" untuk mengikuti kegiatan serupa di masa depan, ada juga yang menyatakan "Sangat Berminat". Hal ini menunjukkan adanya ruang untuk memperdalam materi pada pertemuan berikutnya dengan pendekatan yang lebih aplikatif dan menyenangkan

5. Saran dan Tanggapan Umum

Mayoritas peserta memberikan tanggapan positif, seperti "Sangat baik dan mudah dipahami", "Semoga lebih baik lagi", dan "Kegiatan berjalan dengan lancar". Beberapa peserta juga mengharapkan adanya sesi lanjutan dengan praktik yang lebih banyak. Secara keseluruhan, hasil survei menunjukkan bahwa kegiatan ini berhasil memenuhi ekspektasi peserta dan memberikan dampak positif terhadap peningkatan literasi keamanan digital di kalangan anak-anak asuh. Mayoritas peserta memberikan respon puas terhadap pelaksanaan kegiatan. Rekomendasi dari peserta akan menjadi dasar untuk merancang kegiatan selanjutnya yang berkelanjutan.

Dalam pelaksanaan kegiatan pengabdian ini, tim pelaksana juga menemui beberapa kendala yang menjadi pelajaran penting untuk pengembangan program selanjutnya. Kendala utama adalah keterbatasan waktu yang tersedia untuk sesi praktik, sehingga belum semua peserta dapat mencoba seluruh fitur pengaturan privasi secara menyeluruh pada perangkat masing-masing. Selain itu, beberapa peserta mengalami kesulitan teknis dalam memahami istilah-istilah baru terkait keamanan digital, seperti phishing dan malware, sehingga membutuhkan pendampingan lebih intensif. Kendala lainnya adalah keterbatasan perangkat yang dimiliki peserta, karena tidak semua anak asuh memiliki perangkat digital pribadi atau akun media sosial aktif yang bisa langsung digunakan saat praktik. Hal ini menyebabkan beberapa peserta harus berbagi perangkat, yang berdampak pada efektivitas pelatihan individual. Meskipun demikian, seluruh kegiatan tetap dapat berjalan dengan baik dan peserta tetap menunjukkan antusiasme yang tinggi.

D. SIMPULAN DAN SARAN

Hasil evaluasi menunjukkan bahwa peserta merespons kegiatan dengan positif. Peserta kegiatan merasa lebih sadar akan pentingnya menjaga privasi dan keamanan digital, dan menunjukkan keinginan untuk menerapkan pengetahuan yang diperoleh dalam kehidupan sehari-hari. Kegiatan ini juga mempererat hubungan antara Universitas Siber Indonesia dengan mitra sosial binaan Yayasan Al Hasanat Jaya dalam upaya bersama membangun literasi digital di kalangan generasi muda. Kegiatan ini bukan hanya menjadi bentuk implementasi Tri Dharma Perguruan Tinggi, tetapi juga berkontribusi langsung dalam menciptakan masyarakat yang lebih cakap digital, bertanggung jawab, dan siap menghadapi tantangan dunia maya yang semakin kompleks.

Berdasarkan pelaksanaan dan hasil evaluasi kegiatan, berikut beberapa saran yang dapat menjadi pertimbangan untuk pelaksanaan kegiatan serupa di masa mendatang yaitu: diperlukan pengembangan materi lanjutan yang lebih teknis dan spesifik, seperti pengelolaan jejak digital, cara mendeteksi konten hoaks, atau pelatihan pembuatan konten digital positif; disarankan agar kegiatan pengabdian seperti ini dilaksanakan secara rutin dengan kurikulum berjenjang, sehingga peserta dapat memperoleh pendampingan yang berkesinambungan dan mendalam; dan penggunaan aplikasi interaktif, kuis daring, dan platform pembelajaran digital akan memperkaya pengalaman belajar peserta dan membuat pelatihan lebih menarik dan adaptif bagi generasi muda.

UCAPAN TERIMA KASIH

Tim penulis mengucapkan terima kasih kepada Program Studi Sistem dan Teknologi Informasi Universitas Siber Indonesia meliputi Kaprodi, Dosen, dan Mahasiswa yang telah berkontribusi dalam perencanaan dan pelaksanaan kegiatan. Ucapan terima kasih yang tulus juga kami sampaikan kepada mitra

kami, Panti Asuhan Yatim Piatu Al Hasanat, atas kerja sama dan sambutan hangat yang diberikan selama kegiatan berlangsung. Apresiasi kami berikan kepada seluruh peserta, yaitu anak-anak asuh dari tingkat SMP dan SMK, yang telah mengikuti seluruh rangkaian acara dengan antusiasme dan partisipasi aktif. Dukungan dari semua pihak menjadi faktor utama keberhasilan program ini, semoga memberikan manfaat berkelanjutan bagi masyarakat.

REFERENSI

Dharani, L. I. C., Idayanti, S., & Rahayu, K. (2024). *Perlindungan Hukum terhadap Tindakan Phishing di Media Sosial*. Penerbit NEM.

Effendy, M. Y., & Oktiani, H. (2024). Literasi Digital Keamanan Siber pada Remaja Menghadapi Social Engineering. *Jurnal Wacana Publik*, *18*(01), 35–42.

Fahrimal, Y. (2018). *Netiquette: Etika jejaring sosial generasi milenial dalam media sosial*.

Grassi, P. A., Garcia, M. E., & Fenton, J. L. (2020). Digital identity guidelines.(National Institute of Standards and Technology, Gaithersburg, MD). *NIST Special Publicaiton 800-63-3*, *58*(2), 130–137. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

Hidayat, A., & Napila, A. (2024). Sosialisasi Cyber Security Awareness Dalam Upaya Melindungi Data Pribadi Sejak Dini Di Pondok Pesantren Nafidatunnajah. *Abdi Jurnal Publikasi*, *2*(3), 170–173. https://jurnal.portalpublikasi.id/index.php/AJP/index

Kävrestad, J. (2020). *Fundamentals of digital forensics*. Springer.

Niyu, N., Pengabdian, H. P.-P. K. N., & 2021, undefined. (2021). E-Safety: Keamanan Di Dunia Maya Bagi Pendidik Dan Anak Didik. *Prosiding-Pkmcsr.OrgN Niyu, H PurbaProsiding Konferensi Nasional Pengabdian Kepada Masyarakat Dan, 2021 • prosiding-Pkmcsr.Org*, *4*, 2655–3570. http://www.prosiding-pkmcsr.org/index.php/pkmcsr/article/view/1184

Pratama, A. M., Syaiful, M., & Rahman, M. F. (2024). *Keamanan Data dan Informasi*. Kaizen Media Publishing.

Purba, Y., Riset, A. M.-J. J. C. L., & 2023, undefined. (2023). Kejahatan Siber dan Kebijakan Identitas Kependudukan Digital: Sebuah Studi Tentang Potensi Pencurian Data Online. *Journal.Cicofficial.Com*, *5*(2), 55–66. https://doi.org/10.51486/jbo.v5i2.113

Rahman, R., Ariantini, M. S., Hadi, A., Hayati, N., Gunawan, P. W., Mandowen, S. A., Widiyasono, N., Saskara, G. A. J., Kurniasari, I., Salim, B. S., & others. (2024). *Buku Ajar Keamanan Jaringan Komputer*. PT. Sonpedia Publishing Indonesia.

Satar, S., Judijanto, L., Haryono, P., Septikasari, D., Zamsir, Z., Pirmani, P., Wijaya, S. A., Djollong, A. F., & Gaspersz, V. (2025). *Metode dan Model Pembelajar Inovatif: Teori dan Praktik*. PT. Green Pustaka Indonesia.

Sidyawati, L., Aviccienna, N. A., & Mahayasa, W. (2021). Literasi Keamanan Digital Untuk Meningkatkan Etika Berinternet Yang Aman Bagi Warga Desa Donowarih. *Community Development Journal: Jurnal Pengabdian Masyarakat*, *2*(3), 696–701.

Syahda, F. L., Nur'aisyah, Y., & Rachman, I. F. (2024). Pentingnya pendidikan etika digital dalam konteks SDGs 2030. *Perspektif: Jurnal Pendidikan Dan Ilmu Bahasa*, *2*(2), 66–80.

Vadila, N., & Pratama, A. R. (2021). Analisis Kesadaran Keamanan Terhadap Ancaman Phishing. *Automata*, *2*(2).

Yildirim, M., & Mackie, I. (2019). Encouraging users to improve password security and memorability. *International Journal of Information Security*, *18*, 741–759.