



Penguatan Literasi Digital Keluarga dalam Menghadapi Link Scam dan Risiko Penyalahgunaan AI di RW 03 Kalipancur

Strengthening Family's Digital Literacy of Link Scams and AI Misuse Risks in RW 03 Kalipancur

Indra Abdam Muwakhid^{1*}, Dewi Nurdiah²

¹Program Studi Informatika Medis, Universitas Widya Husada Semarang, Indonesia

²Program Studi Teknik Informatika, Universitas Semarang, Indonesia

Email: abdam.stiess@gmail.com ^{1*}, nurdiah@usm.ac.id ²

*Penulis Korespondensi: abdam.stiess@gmail.com

Article History:

Naskah Masuk: 19 September 2025;

Revisi: 20 Oktober 2025;

Diterima: 28 November 2025;

Terbit: 30 November 2025

Keywords: Artificial Intelligence;

Community Empowerment;

Cybersecurity Awareness; Digital

Literacy; Online Scam

Abstract: Digital transformation has reshaped community life by increasing internet dependency in daily communication, financial transactions, and public services. However, this rapid development has also intensified cybersecurity risks, particularly link-based scams and the misuse of Artificial Intelligence (AI). Limited digital literacy at the family level makes communities vulnerable to phishing attacks, personal data breaches, and AI-generated fraud. This community service program aimed to strengthen digital literacy among residents of RW 03 Kalipancur, Semarang, through participatory education focusing on link scam detection and responsible AI usage. The program involved interactive lectures, case discussions, simulations, and pre-test and post-test evaluations with 18 participants from family groups, PKK cadres, and elderly residents. The results showed a significant increase in understanding, from an average pre-test score of 43% to a post-test score of 84%. Beyond knowledge improvement, participants demonstrated increased awareness and behavioral change toward safer digital practices. The findings suggest that community-based participatory approaches effectively enhance family-level digital resilience and can serve as a replicable empowerment model in other communities facing similar digital threats.

Abstrak

Transformasi digital telah meningkatkan ketergantungan masyarakat terhadap teknologi internet dalam komunikasi, transaksi keuangan, serta layanan publik. Namun perkembangan tersebut juga diiringi peningkatan risiko kejahatan siber, khususnya penipuan berbasis tautan palsu (*link scam*) dan penyalahgunaan kecerdasan buatan (*Artificial Intelligence/AI*). Rendahnya literasi digital pada tingkat keluarga menyebabkan masyarakat rentan terhadap phishing, kebocoran data pribadi, dan manipulasi informasi berbasis AI. Kegiatan pengabdian masyarakat ini bertujuan memperkuat literasi digital warga RW 03 Kelurahan Kalipancur Kota Semarang melalui pendekatan partisipatif yang berfokus pada deteksi link scam dan pemanfaatan AI secara bertanggung jawab. Metode yang digunakan meliputi ceramah interaktif, diskusi kasus, simulasi praktik, serta evaluasi pre-test dan post-test terhadap 18 peserta yang terdiri dari kader PKK, ibu rumah tangga, dan lansia. Hasil kegiatan menunjukkan peningkatan pemahaman peserta dari rata-rata 43% menjadi 84%. Selain peningkatan kognitif, terjadi perubahan sikap berupa meningkatnya kewaspadaan terhadap tautan mencurigakan dan kesadaran menjaga privasi digital. Program ini menunjukkan bahwa pendekatan berbasis komunitas efektif dalam membangun ketahanan digital keluarga dan dapat direplikasi pada komunitas lain dengan karakteristik serupa.

Kata Kunci: Keamanan Siber; Kecerdasan Buatan; Literasi Digital; Pemberdayaan Masyarakat; Penipuan Daring

1. PENDAHULUAN

Perkembangan teknologi digital telah mengubah pola kehidupan masyarakat secara signifikan. Aktivitas komunikasi, transaksi ekonomi, pendidikan, dan layanan kesehatan kini banyak bergantung pada sistem berbasis internet. Peningkatan penetrasi internet dan

penggunaan perangkat seluler di Indonesia menunjukkan bahwa masyarakat semakin terintegrasi dalam ekosistem digital. Namun, transformasi ini tidak selalu diiringi dengan peningkatan kapasitas literasi digital yang memadai.

Fenomena kejahatan siber menunjukkan tren peningkatan dari tahun ke tahun. Salah satu modus yang paling banyak menyasar masyarakat adalah link scam atau penipuan berbasis tautan palsu. Modus ini memanfaatkan rekayasa sosial dengan menyebarkan tautan yang menyerupai situs resmi guna mencuri informasi pribadi maupun data keuangan korban. Penelitian menunjukkan bahwa phishing dan scam digital menjadi ancaman dominan dalam lanskap keamanan siber global (Kaur et al., 2023). Dalam konteks nasional, kasus penipuan daring seringkali menargetkan kelompok masyarakat yang kurang memahami karakteristik keamanan digital (Kamran & Maskun, 2021).

Di sisi lain, kemajuan Artificial Intelligence (AI) menghadirkan peluang sekaligus risiko baru. AI mampu mendukung berbagai aktivitas produktif seperti analisis data kesehatan, sistem pembelajaran adaptif, serta otomasi layanan publik. Akan tetapi, teknologi ini juga digunakan untuk memproduksi konten manipulatif seperti deepfake, pesan phishing otomatis, serta penyebaran hoaks yang sulit diverifikasi (Gupta et al., 2023; Mutmainnah et al., 2024; Raza et al., 2022). Kondisi ini memperlihatkan bahwa literasi digital harus mencakup pemahaman etika dan risiko penggunaan AI.

Analisis situasi di RW 03 Kelurahan Kalipancur menunjukkan bahwa sebagian besar warga aktif menggunakan media sosial dan aplikasi pesan instan, namun belum memiliki pemahaman yang memadai terkait keamanan tautan digital. Beberapa warga mengaku pernah menerima pesan berisi tautan undian, informasi bantuan sosial, maupun promosi kesehatan yang mencurigakan. Minimnya pemahaman ini berpotensi menimbulkan kerugian finansial serta penyalahgunaan data pribadi.

Keluarga sebagai unit sosial terkecil memiliki peran penting dalam membangun budaya digital yang aman. Literasi digital keluarga tidak hanya melindungi individu, tetapi juga membangun ketahanan kolektif terhadap ancaman siber (Nisa et al., 2023). Menurut (Naufal, 2021), literasi digital mencakup kemampuan memahami, mengevaluasi, dan menggunakan informasi secara bertanggung jawab. Sementara itu, (Revilia & Irwansyah, 2020) menekankan pentingnya kesadaran keamanan dan privasi dalam penggunaan media digital.

Berdasarkan kondisi tersebut, kegiatan pengabdian masyarakat ini difokuskan pada penguatan literasi digital keluarga melalui edukasi deteksi link scam dan pemanfaatan AI secara etis (Eka Sila & Mochamad Taufik, 2023; Rico & FADJARINI SULISTYOWATI, 2024). Perubahan sosial yang diharapkan adalah meningkatnya kesadaran kolektif warga

terhadap risiko digital, perubahan perilaku dalam penggunaan teknologi, serta terbentuknya agen literasi digital di tingkat komunitas.

2. METODE

Kegiatan pengabdian masyarakat ini menggunakan pendekatan partisipatif berbasis pemberdayaan komunitas (*community empowerment approach*). Pendekatan ini dipilih karena menempatkan masyarakat sebagai subjek aktif dalam proses perencanaan, pelaksanaan, hingga evaluasi kegiatan, bukan hanya sebagai objek penerima materi (Akbar & Wijaya, 2024; Bulya & Izzati, 2024). Strategi ini diharapkan mampu membangun kesadaran kolektif serta mendorong perubahan perilaku digital secara berkelanjutan.

Subyek dan Lokasi Pengabdian

Subyek pengabdian adalah warga RW 03 Kelurahan Kalipancur, Kota Semarang, yang terdiri dari kader PKK, ibu rumah tangga, remaja, serta lansia. Total peserta yang terlibat sebanyak 18 orang yang merupakan perwakilan dari beberapa RT. Pemilihan lokasi didasarkan pada hasil komunikasi awal dengan pengurus RW yang menyampaikan adanya kebutuhan edukasi terkait maraknya pesan penipuan berbasis tautan yang diterima warga melalui aplikasi pesan instan.

Jumlah peserta yang terlibat dalam kegiatan ini sebanyak 18 orang. Karakteristik peserta didominasi oleh pengguna aktif media sosial dan aplikasi perpesanan, namun belum memiliki pengalaman mengikuti pelatihan keamanan digital secara formal.

Lokasi kegiatan dilaksanakan di Balai RW 03 Kalipancur. Tempat tersebut dipilih karena mudah diakses warga serta mendukung pelaksanaan kegiatan berbasis diskusi dan simulasi.

Proses Perencanaan dan Pengorganisasian Komunitas

Tahap perencanaan dilakukan melalui koordinasi awal antara tim dosen dengan Ketua RW dan kader PKK. Pada tahap ini dilakukan identifikasi kebutuhan (*needs assessment*) secara informal melalui diskusi kelompok kecil. Warga menyampaikan pengalaman menerima pesan undian palsu, tautan bantuan sosial, serta pesan promosi yang mencurigakan. Temuan ini memperkuat fokus program pada isu keamanan tautan digital dan pemanfaatan AI secara bijak.

Warga dilibatkan dalam proses perencanaan dengan memberikan masukan terkait isu digital yang sering mereka alami. Beberapa warga menyampaikan pernah menerima tautan undian palsu, informasi bantuan sosial yang tidak jelas sumbernya, serta pesan yang meminta verifikasi data pribadi. Pendekatan partisipatif ini bertujuan agar materi yang disampaikan bersifat kontekstual dan sesuai dengan kebutuhan nyata komunitas.

Tahapan Pelaksanaan Kegiatan

Pelaksanaan program pengabdian masyarakat ini dirancang secara sistematis melalui tahapan yang terstruktur dan berbasis pada prinsip pemberdayaan komunitas. Setiap tahapan tidak hanya bertujuan menyampaikan materi, tetapi juga membangun kesadaran kritis serta keterlibatan aktif peserta dalam memahami dan mengelola risiko digital yang mereka hadapi.

a. Tahap Identifikasi Kebutuhan dan Analisis Situasi

Tahap awal dilakukan melalui diskusi partisipatif bersama pengurus RW dan perwakilan warga untuk mengidentifikasi persoalan aktual yang dihadapi komunitas terkait penggunaan teknologi digital bersama dengan Ibu Ketua RW dan Ibu Kader PKK dapat dilihat pada Gambar 1. Proses ini bertujuan memperoleh gambaran objektif mengenai tingkat literasi digital, pengalaman warga terhadap penipuan daring, serta persepsi mereka terhadap teknologi kecerdasan buatan.

Hasil identifikasi menunjukkan bahwa sebagian besar warga pernah menerima pesan berisi tautan mencurigakan, namun belum memiliki kemampuan memadai untuk melakukan verifikasi keamanan digital. Selain itu, pemahaman mengenai potensi penyalahgunaan AI masih sangat terbatas dan cenderung dipersepsikan hanya sebagai teknologi hiburan. Temuan ini menjadi dasar dalam merumuskan fokus intervensi edukasi.



Gambar 1. Diskusi Persiapan.

b. Tahap Perencanaan Program dan Penyusunan Materi

Berdasarkan hasil analisis situasi, tim pengabdian menyusun rancangan program yang menitikberatkan pada dua fokus utama, yaitu deteksi link scam dan pemanfaatan AI secara etis. Materi disusun secara kontekstual dengan mempertimbangkan karakteristik peserta yang heterogen dari segi usia dan latar belakang pendidikan.

Penyusunan materi tidak hanya memuat aspek konseptual, tetapi juga praktik aplikatif seperti identifikasi struktur URL, pengenalan ciri-ciri *phishing*, serta demonstrasi

aktivasi autentikasi dua faktor (*two-factor authentication*). Pendekatan ini bertujuan agar peserta tidak hanya memahami secara teoritis, tetapi mampu mengimplementasikan keterampilan keamanan digital secara langsung

c. Tahap Implementasi Edukasi dan Simulasi Partisipatif

Tahap implementasi dilaksanakan melalui metode ceramah interaktif, diskusi kasus, serta simulasi praktik. Ceramah interaktif digunakan untuk membangun landasan konseptual, sedangkan diskusi kasus mendorong peserta merefleksikan pengalaman nyata yang pernah mereka alami.

Simulasi dilakukan dengan memperlihatkan contoh tautan palsu dan tautan resmi, kemudian peserta diminta mengidentifikasi perbedaannya. Strategi ini dipilih karena pembelajaran berbasis pengalaman (*experiential learning*) terbukti lebih efektif dalam meningkatkan pemahaman dan retensi informasi dibandingkan metode satu arah.

Selain itu, dilakukan demonstrasi penggunaan aplikasi berbasis AI yang bersifat produktif, sekaligus penjelasan mengenai risiko manipulasi konten berbasis *deepfake* dan otomatisasi *phishing*. Dengan demikian, peserta memperoleh perspektif yang seimbang antara manfaat dan risiko teknologi dengan pemaparan ditunjukkan pada Gambar 2.



Gambar 2. Pemaparan dan Diskusi Edukasi.

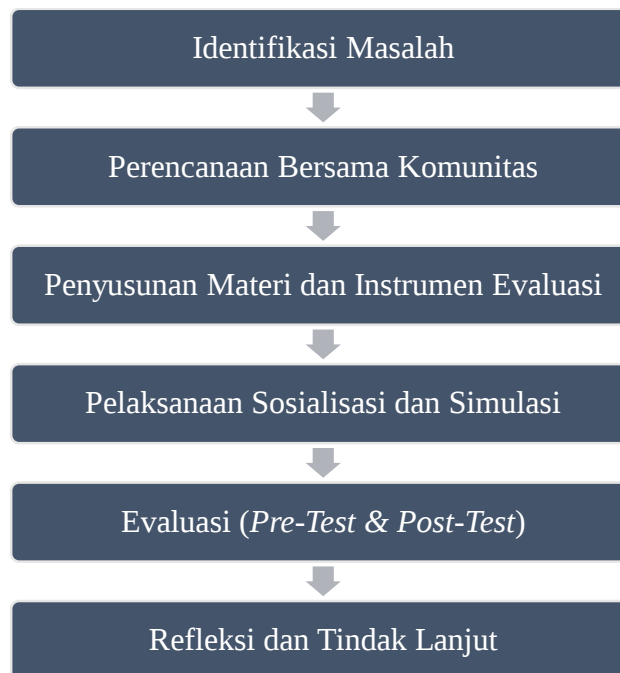
d. Tahap Evaluasi dan Refleksi Bersama

Evaluasi dilakukan melalui pemberian *pre-test* dan *post-test* untuk mengukur perubahan tingkat pemahaman peserta secara kuantitatif. Instrumen yang digunakan berbentuk pertanyaan dikotomis (YA/TIDAK) yang disesuaikan dengan konteks komunitas.

Selain evaluasi kuantitatif, dilakukan pula refleksi bersama untuk menggali perubahan persepsi dan komitmen peserta dalam menerapkan praktik digital yang lebih aman. Refleksi ini penting untuk memastikan bahwa intervensi tidak berhenti pada peningkatan pengetahuan, tetapi juga mendorong perubahan perilaku.

Untuk memperjelas tahapan kegiatan, berikut adalah Gambar 3 alur pelaksanaan

program:



Gambar 3. Alur Pelaksanaan Kegiatan Pengabdian.

Instrumen Evaluasi

Kuesioner terdiri dari 10 pertanyaan yang mengukur tiga indikator utama literasi digital, yaitu: pengetahuan dasar tentang link scam dan phishing, kesadaran keamanan data pribadi dan tautan digital, pemahaman risiko penyalahgunaan teknologi AI.

Model pertanyaan disusun dalam bentuk pernyataan sederhana agar mudah dipahami oleh peserta dari berbagai kelompok usia, termasuk lansia.

Tabel 1. Distribusi Indikator Literasi Digital pada Kuesioner.

Indikator	Nomor Soal	Jumlah
Pengetahuan Link Scam & Phishing	1, 2, 4 & 5	4
Ancaman <i>Malware</i> & <i>Fake Website</i>	6, 7 & 8	3
Perilaku Keamanan Digital & AI	3, 9, & 10	3

Skoring dilakukan dengan memberikan nilai 1 untuk jawaban benar dan 0 untuk jawaban salah. Total skor kemudian dikonversi menjadi persentase tingkat pemahaman.

Teknik Analisis Data

Data kuantitatif dianalisis menggunakan perhitungan persentase rata-rata skor *pre-test* dan *post-test* untuk mengetahui peningkatan pemahaman. Sementara itu, data kualitatif diperoleh melalui observasi partisipasi warga selama diskusi dan simulasi, serta dokumentasi respon peserta terhadap materi yang diberikan.

Pendekatan analisis ini bersifat deskriptif-komparatif, yaitu membandingkan kondisi sebelum dan sesudah intervensi edukasi.

3. HASIL

Pelaksanaan program penguatan literasi digital keluarga di RW 03 Kalipancur menunjukkan hasil yang signifikan baik secara kuantitatif maupun kualitatif. Hasil kegiatan tidak hanya tercermin pada peningkatan skor evaluasi, tetapi juga pada perubahan sikap dan kesadaran peserta terhadap praktik keamanan digital dalam kehidupan sehari-hari.

Dinamika Proses Pendampingan

Kegiatan berlangsung dalam suasana interaktif dan partisipatif. Pada tahap awal, sebagian besar peserta menunjukkan rasa ingin tahu yang tinggi, terutama ketika disampaikan contoh kasus nyata terkait pesan undian palsu dan tautan verifikasi data perbankan.

Diskusi awal mengungkap bahwa beberapa peserta pernah menerima pesan mencurigakan, bahkan ada yang hampir memberikan data pribadi karena tautan tersebut menyerupai situs resmi. Fakta ini mengonfirmasi bahwa risiko *link scam* bukan sekadar potensi, tetapi telah menjadi ancaman nyata di tingkat komunitas.

Selama sesi simulasi, peserta secara aktif mencoba membedakan tautan asli dan palsu melalui struktur URL dan domain. Pada tahap ini terlihat adanya proses pembelajaran kolektif, di mana peserta saling berdiskusi dan membandingkan pemahaman mereka.

Pendampingan tidak hanya berfokus pada aspek teknis, tetapi juga pada pembangunan kesadaran kritis bahwa keamanan digital merupakan tanggung jawab bersama dalam keluarga.

Hasil Evaluasi Kuantitatif

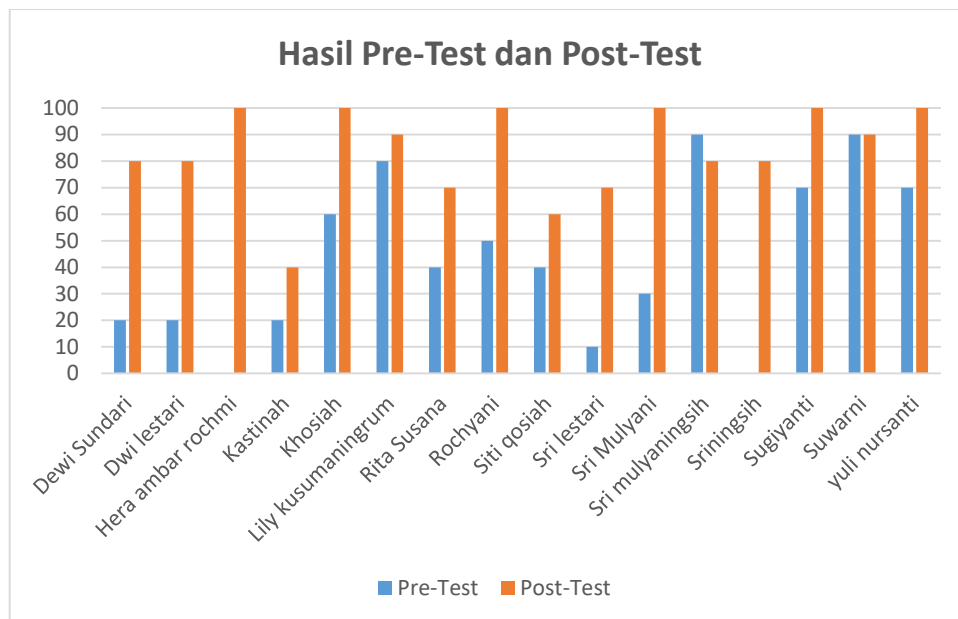
Evaluasi dilakukan melalui *pre-test* dan *post-test* menggunakan kuesioner 10 item dengan skala dikotomis (YA/TIDAK). Hasil analisis menunjukkan peningkatan yang signifikan seperti ditunjukkan pada Tabel 2.

Tabel 2. Perbandingan Hasil Pre-Test dan Post-Test.

Indikator	Pre-Test (%)	Post-Test (%)	Peningkatan
Pemahaman Link Scam	45	88	+43
Ancaman Malware & Fake Website	40	82	+42
Keamanan Data & Risiko AI	44	83	+39
Rata-rata Keseluruhan	43	84	+41

Hasil tersebut menunjukkan bahwa terjadi peningkatan rata-rata sebesar 41%. Kenaikan ini melampaui target minimal keberhasilan program yang ditetapkan sebesar 30%.

Secara khusus, indikator pemahaman link scam mengalami peningkatan paling tinggi. Hal ini menunjukkan bahwa metode simulasi visual dan studi kasus efektif dalam membantu peserta mengenali ciri-ciri tautan berbahaya. Sebaran hasil pre-test dan post-test dapat dilihat pada Gambar 4.



Gambar 4. Grafik Perbandingan Rata-Rata Pre-Test dan Post-Test.

Perubahan Perilaku dan Kesadaran Sosial

Selain peningkatan kognitif, program ini juga menghasilkan perubahan perilaku yang teramati selama dan setelah kegiatan berlangsung.

Beberapa perubahan yang teridentifikasi antara lain:

- Peserta menyatakan akan lebih berhati-hati sebelum mengklik tautan dalam pesan instan.
- Muncul komitmen untuk saling mengingatkan antarwarga jika menerima pesan mencurigakan.
- Peserta mulai memahami pentingnya autentikasi dua faktor dalam melindungi akun digital.

Perubahan ini menunjukkan bahwa intervensi tidak hanya berdampak pada aspek pengetahuan, tetapi juga mendorong transformasi perilaku digital. Kesadaran kolektif yang terbentuk menjadi modal sosial dalam membangun ketahanan digital komunitas.

Dampak terhadap Ketahanan Digital Keluarga

Hasil kegiatan mengindikasikan bahwa keluarga mulai memahami pentingnya:

- Melindungi data pribadi anggota keluarga, termasuk anak dan lansia
- Tidak membagikan kode OTP atau informasi sensitif
- Menggunakan teknologi AI secara produktif dan tidak mudah terpengaruh konten manipulatif

Dengan demikian, program ini berkontribusi dalam membangun ketahanan digital berbasis keluarga sebagai unit sosial terkecil. Ketahanan ini menjadi fondasi penting dalam menghadapi kompleksitas ancaman siber yang terus berkembang.

4. DISKUSI

Hasil kegiatan pengabdian masyarakat ini menunjukkan bahwa pendekatan edukasi partisipatif berbasis simulasi efektif dalam meningkatkan literasi digital keluarga, khususnya dalam konteks deteksi link scam dan pemanfaatan AI secara bertanggung jawab. Peningkatan skor rata-rata dari 43% menjadi 84% tidak hanya merefleksikan peningkatan pengetahuan, tetapi juga menunjukkan adanya proses internalisasi pemahaman yang lebih mendalam terhadap risiko digital.

Secara teoritik, temuan ini sejalan dengan konsep literasi digital sebagai kompetensi multidimensional yang mencakup aspek kognitif, kritis, dan etis (Naufal, 2021). Literasi digital tidak berhenti pada kemampuan menggunakan perangkat, melainkan mencakup kemampuan mengevaluasi informasi serta memahami risiko keamanan data. Peningkatan signifikan pada indikator pemahaman link scam menunjukkan bahwa peserta mulai memiliki kemampuan analitis dalam mengidentifikasi ciri-ciri tautan berbahaya, seperti domain tidak resmi, penggunaan simbol yang menyerupai institusi formal, dan permintaan data sensitif.

Dari perspektif keamanan siber, peningkatan kesadaran terhadap autentikasi dua faktor dan perlindungan data pribadi menunjukkan adanya perubahan dari perilaku pasif menjadi perilaku protektif. Hal ini relevan dengan temuan (Kaur et al., 2023) yang menekankan bahwa faktor manusia (*human factor*) merupakan titik paling rentan dalam sistem keamanan digital. Intervensi edukatif yang tepat dapat meminimalkan risiko tersebut melalui peningkatan kesadaran individu.

Temuan ini juga mendukung penelitian (Revilia & Irwansyah, 2020) yang menyatakan bahwa kesadaran privasi digital menjadi elemen penting dalam membangun budaya keamanan informasi. Dalam kegiatan ini, peserta tidak hanya memahami risiko, tetapi juga menunjukkan komitmen untuk menerapkan praktik keamanan sederhana seperti memeriksa URL sebelum mengklik tautan dan tidak membagikan kode OTP.

Dalam konteks pemanfaatan AI, hasil kegiatan menunjukkan adanya perubahan persepsi peserta terhadap teknologi tersebut. Sebelumnya, AI dipahami secara terbatas sebagai alat hiburan atau fitur media sosial. Setelah edukasi, peserta mulai memahami bahwa AI memiliki potensi ganda: sebagai alat produktif sekaligus sebagai sarana manipulasi digital seperti deepfake dan phishing otomatis. Pemahaman ini penting mengingat penelitian (Gupta et al., 2023; Raza et al., 2022) menegaskan bahwa AI telah menjadi instrumen baru dalam eskalasi serangan siber.

Pendekatan partisipatif yang digunakan dalam kegiatan ini turut berkontribusi terhadap efektivitas program. Pembelajaran berbasis pengalaman (*experiential learning*) melalui

simulasi dan studi kasus memungkinkan peserta terlibat secara aktif dalam proses pembelajaran. Model ini lebih efektif dibandingkan metode ceramah satu arah karena peserta tidak hanya menerima informasi, tetapi juga mempraktikkan keterampilan yang dipelajari. Proses diskusi kolektif juga memperkuat modal sosial komunitas dalam menghadapi ancaman digital secara bersama-sama.

Selain peningkatan aspek kognitif, temuan penting lainnya adalah munculnya kesadaran kolektif dan komitmen saling mengingatkan antarwarga. Hal ini menunjukkan bahwa intervensi literasi digital dapat berfungsi sebagai katalisator terbentuknya pranata sosial baru di tingkat komunitas, yaitu norma kehati-hatian dalam interaksi digital. Dalam perspektif pemberdayaan masyarakat, perubahan ini menjadi indikator keberhasilan karena mencerminkan transformasi sosial, bukan sekadar peningkatan pengetahuan individual.

Secara keseluruhan, hasil pengabdian ini mengindikasikan bahwa literasi digital berbasis keluarga merupakan pendekatan yang relevan dalam membangun ketahanan siber masyarakat. Integrasi antara edukasi deteksi link scam dan pemanfaatan AI secara etis menjadi kebaruan program ini dibandingkan kegiatan literasi digital yang umumnya hanya menekankan penggunaan teknologi.

Namun demikian, kegiatan ini memiliki keterbatasan pada jumlah peserta yang relatif terbatas dan lingkup komunitas yang spesifik. Oleh karena itu, generalisasi hasil perlu dilakukan secara hati-hati. Replikasi program pada komunitas dengan karakteristik berbeda diperlukan untuk memperkuat validitas model intervensi ini.

5. KESIMPULAN

Kegiatan pengabdian masyarakat yang dilaksanakan di RW 03 Kelurahan Kalipancur menunjukkan bahwa intervensi literasi digital berbasis komunitas efektif dalam meningkatkan pemahaman dan kesadaran warga terhadap ancaman link scam serta risiko penyalahgunaan teknologi kecerdasan buatan (AI). Peningkatan skor rata-rata dari 43% pada pre-test menjadi 84% pada post-test mengindikasikan adanya perubahan kognitif yang signifikan setelah pelaksanaan program edukasi.

Lebih dari sekadar peningkatan pengetahuan, kegiatan ini juga mendorong perubahan perilaku digital yang lebih protektif. Peserta menunjukkan peningkatan kewaspadaan terhadap tautan mencurigakan, kesadaran menjaga data pribadi, serta komitmen untuk menerapkan praktik keamanan sederhana seperti pemeriksaan URL dan penggunaan autentikasi dua faktor. Munculnya kader literasi digital di lingkungan PKK menjadi indikator terbentuknya agen perubahan lokal yang berpotensi menjaga keberlanjutan program.

Secara teoretis, hasil kegiatan ini memperkuat konsep literasi digital sebagai kompetensi multidimensional yang mencakup aspek pengetahuan, kesadaran kritis, dan etika penggunaan teknologi. Secara praktis, model edukasi partisipatif berbasis simulasi terbukti relevan dan adaptif untuk diterapkan pada komunitas dengan karakteristik heterogen. Integrasi materi deteksi link scam dan pemanfaatan AI secara etis menjadi kontribusi inovatif dalam program literasi digital tingkat komunitas.

Meskipun demikian, kegiatan ini memiliki keterbatasan pada jumlah peserta yang terbatas dan cakupan wilayah yang spesifik. Oleh karena itu, diperlukan replikasi program pada komunitas lain dengan karakteristik sosial berbeda untuk menguji konsistensi efektivitas model intervensi ini. Untuk selanjutnya, penguatan literasi digital perlu dilakukan secara berkelanjutan dengan topik yang mengikuti dinamika perkembangan teknologi dan ancaman siber yang terus berkembang.

PENGAKUAN/ACKNOWLEDGEMENTS

Penulis menyampaikan apresiasi dan terima kasih kepada Ketua RW 03 Kelurahan Kalipancur beserta seluruh warga yang telah berpartisipasi aktif dalam kegiatan pengabdian masyarakat ini. Ucapan terima kasih juga disampaikan kepada mahasiswa pendamping yang turut membantu proses pelaksanaan kegiatan serta dokumentasi. Dukungan dari Program Studi Informatika Medis Universitas Widya Husada Semarang dan Program Studi Teknik Informatika Universitas Semarang sangat berarti dalam kelancaran program ini.

DAFTAR REFERENSI

- Akbar, M., & Wijaya, G. (2024). Digital literacy of rural areas in Indonesia: Challenges and opportunities. *Proceedings of the 4th International Conference on Rural Socio-Economic Transformation (RUSSET 2023)*, 1 November 2023, Bogor, Indonesia. <https://doi.org/10.4108/eai.1-11-2023.2344347>
- Bulya, B., & Izzati, S. (2024). Indonesia's digital literacy as a challenge for democracy in the digital age. *The Journal of Society and Media*, 8(2), 640–661. <https://doi.org/10.26740/jsm.v8n2.p640-661>
- Eka Sila, G., & Mochamad Taufik, C. (2023). Literasi digital untuk melindungi masyarakat dari kejahatan siber. *KOMVERSAL*, 5(1), 112–123. <https://doi.org/10.38204/komversal.v5i1.1225>
- Gupta, G., Raja, K., Gupta, M., Jan, T., Whiteside, S. T., & Prasad, M. (2023). A comprehensive review of deepfake detection using advanced machine learning and fusion methods. *Electronics*, 13(1), 95. <https://doi.org/10.3390/electronics13010095>
- Kamran, M., & Maskun, M. (2021). Penipuan dalam jual beli online: Perspektif hukum telematika. *Balobe Law Journal*, 1(1), 41. <https://doi.org/10.47268/balobe.v1i1.501>

- Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, 97, 101804. <https://doi.org/10.1016/j.inffus.2023.101804>
- Mutmainnah, A., Suhandi, A. M., & Herlambang, Y. T. (2024). Problematika teknologi deepfake sebagai masa depan hoax yang semakin meningkat: Solusi strategis ditinjau dari literasi digital. *UPGRADE: Jurnal Pendidikan Teknologi Informasi*, 1(2), 67–72. <https://doi.org/10.30812/upgrade.v1i2.3702>
- Naufal, H. A. (2021). Literasi digital. *Perspektif*, 1(2), 195–202. <https://doi.org/10.53947/perspekt.v1i2.32>
- Nisa, U., Nisak, C. L. C., & Fatia, D. (2023). Literasi digital lansia pada aspek digital skill dan digital safety. *Jurnal Komunikasi Global*, 12(1), 143–167. <https://doi.org/10.24815/jkg.v12i1.31667>
- Raza, A., Munir, K., & Almutairi, M. (2022). A novel deep learning approach for deepfake image detection. *Applied Sciences*, 12(19), 9820. <https://doi.org/10.3390/app12199820>
- Revilia, D., & Irwansyah, N. (2020). Social media literacy: Millennial's perspective of security and privacy awareness. *Jurnal Penelitian Komunikasi dan Opini Publik*, 24(1). <https://doi.org/10.33299/jpkop.24.1.2375>
- Rico, E. R. O., & Sulistyowati, F. (2024). Peran literasi digital remaja dalam menghadapi penyebaran berita hoaks. *Jurnal Komunikasi Pemberdayaan*, 3(1), 38–46. <https://doi.org/10.47431/jkp.v3i1.401>