

PENINGKATAN LITERASI DIGITAL KELUARGA TERHADAP LINK SCAM DAN PEMANFAATAN AI DI WILAYAH RW 03 KALIPANCUR

Indra Abdam Muwakhid¹, Okti Tri Hastuti², Dewi Nurdiyah³

¹Prodi Informatika Medis, Universitas Widya Husada Semarang,
bdam.stiess@gmail.com

²Prodi Informatika Medis, Universitas Widya Husada Semarang,
okti.trihastuti@uwhs.ac.id

³Prodi Teknik Informatika, Universitas Semarang, nurdiyah@usm.ac.id

Abstrak

Berbagai manfaat telah dirasakan oleh masyarakat dengan adanya perkembangan teknologi digital, namun juga menimbulkan resiko keamanan seperti penipuan daring (*link scam*) dan penyalahgunaan kecerdasan buatan (AI). Kurangnya literasi digital di lingkungan keluarga berpotensi membawa kerugian finansial, kebocoran data, hingga penyalahgunaan teknologi. Kegiatan pengabdian masyarakat ini bertujuan untuk meningkatkan pemahaman warga RW 03 Kelurahan Kalipancur Kota Semarang terhadap ancaman *link scam* serta memanfaatkan AI dengan aman. Metode yang digunakan meliputi ceramah interaktif, diskusi, simulasi, *pre-test*, dan *post-test*. Hasil pemahaman warga menunjukkan peningkatan dari rata-rata *pre-test* 43% menjadi 84% pada saat *post-test*. Kegiatan ini efektif dalam meningkatkan literasi digital warga untuk mengantisipasi awal dugaan adanya *scam*.

Kata Kunci: literasi digital, link scam, kecerdasan buatan, pengabdian masyarakat, keamanan siber.

PENDAHULUAN

Teknologi digital saat ini terus berkembang dan membawa dampak yang besar dalam aspek kehidupan Masyarakat. Di satu sisi, untuk mempermudah aktivitas sosial, ekonomi, Pendidikan, hingga pelayanan Kesehatan semuanya bergantung pada kemajuan teknologi informasi dan komunikasi. Namun di sisi lainnya, kemajuan ini membuka celah terjadinya berbagai kejahatan digital seperti penipuan daring (*online scam/link scam*), pencurian identitas, dan penyalahgunaan data pribadi (Gupta et al., 2023; Mim et al., 2023). Salah satu modus kejahatan digital yang marak terjadi adalah *link scam*, yaitu penipuan dengan memanfaatkan tautan palsu untuk mencuri data pribadi, data perbankan, atau bahkan menyebarkan malware pada perangkat pengguna (Kaur et al., 2023).

Maraknya penggunaan AI dalam keseharian masyarakat juga membawa dampak ganda. Di satu sisi, AI dapat dimanfaatkan untuk mendukung aktivitas pendidikan, layanan kesehatan, hingga kebutuhan bisnis skala kecil. Namun di sisi lain, teknologi ini

juga berpotensi disalahgunakan, seperti pembuatan *deepfake*, penyebaran informasi palsu, atau pencurian data biometrik (Mutmainnah et al., 2024; Raza et al., 2022).

Fakta di lapangan menunjukkan bahwa masyarakat, khususnya di lingkungan keluarga, ibu rumah tangga, dan kelompok masyarakat lokal, masih memiliki tingkat literasi digital yang rendah. Hal ini memicu kasus penipuan online yang sangat tinggi, apalagi pada zaman saat ini alat dan teknologi juga semakin canggih (Kamran & Maskun, 2021). Kondisi ini diperparah dengan rendahnya pemahaman tentang etika pemanfaatan AI, sehingga masyarakat menjadi rentan terhadap berbagai bentuk ancaman digital.

Oleh sebab itu, perlu dilakukan upaya peningkatan literasi digital di kalangan masyarakat, terutama di lingkungan keluarga dan komunitas tingkat RT/RW, yang selama ini sering luput dari program edukasi digital formal. Literasi digital tidak hanya sebatas kemampuan menggunakan teknologi, tetapi juga mencakup kemampuan mengenali risiko digital, menerapkan keamanan data pribadi, serta memahami etika dan tanggung jawab dalam menggunakan teknologi AI (Naufal, 2021; Revilia & Irwansyah, 2020).

Kegiatan Pengabdian Kepada Masyarakat ini dilakukan sebagai upaya nyata untuk memberikan edukasi kepada warga RW 03 Kelurahan Kalipancur, Kota Semarang, mengenai ancaman *link scam* serta pemanfaatan AI secara bijak dalam kehidupan sehari-hari. Sasaran kegiatan ini adalah kelompok Tri Bina (lansia, ibu rumah tangga, remaja) serta kader PKK dan Posyandu yang memiliki peran strategis dalam edukasi keluarga dan lingkungan.

Kegiatan ini memanfaatkan metode edukasi partisipatif berbasis sosialisasi, diskusi interaktif, dan simulasi, sehingga warga dapat memahami ancaman yang dihadapi dan mengetahui cara-cara praktis dalam menghindari serta mengelola risiko digital di lingkungan mereka. Pelaksanaan kegiatan ini tidak hanya memberikan pengetahuan, tetapi juga membekali masyarakat dengan keterampilan praktis mengenali link scam dan memanfaatkan AI dengan aman dan bertanggung jawab (Eka Sila & Mochamad Taufik, 2023; Rico & Fadjarini Sulistyowati, 2024).

Diharapkan, kegiatan ini dapat berkontribusi terhadap peningkatan kapasitas literasi digital masyarakat, menciptakan lingkungan digital yang lebih aman, serta menumbuhkan budaya bijak bermedia digital di tingkat komunitas lokal. Selain itu, kegiatan ini dapat

menjadi model pengabdian berbasis literasi digital yang dapat direplikasi di wilayah perkotaan lain yang memiliki karakteristik sosial masyarakat serupa (Nisa et al., 2023).

METODE

Kegiatan pengabdian masyarakat ini menggunakan pendekatan edukasi partisipatif berbasis literasi digital, yang dirancang untuk meningkatkan pemahaman warga terhadap ancaman link scam dan pemanfaatan AI secara bijak dalam kehidupan sehari-hari. Metode yang dipilih disesuaikan dengan karakteristik sasaran kegiatan, yaitu warga RW 03 Kelurahan Kalipancur Kota Semarang, yang didominasi oleh ibu rumah tangga, kader PKK, lansia, dan remaja.

Desain kegiatan berbasis sosialisasi, diskusi, dan simulasi dipilih karena terbukti efektif dalam meningkatkan literasi digital komunitas lokal, khususnya di lingkungan masyarakat perkotaan dan perdesaan (Akbar & Wijaya, 2024; Bulya & Izzati, 2024). Bentuk edukasi partisipatif juga dapat meningkatkan keterlibatan warga dalam menyerap materi serta mendorong peserta untuk berbagi pengalaman tentang ancaman digital yang pernah dihadapi.

Kegiatan dilaksanakan melalui beberapa tahapan sebagai berikut:

1. Persiapan

- a. Penyusunan materi edukasi mengenai *link scam*, jenis-jenis ancaman siber, serta pemanfaatan AI yang aman.
- b. Koordinasi dengan Ketua RW dan kader PKK untuk menentukan jadwal, lokasi kegiatan, dan target peserta seperti yang ditunjukkan pada gambar 1.
- c. Pembuatan *pre-test* dan *post-test* untuk mengukur tingkat pemahaman warga sebelum dan sesudah kegiatan.
- d. Penyediaan media interaktif berupa slide presentasi, video edukasi, dan simulasi pendeteksian tautan *scam*.



Gambar 1. Diskusi Persiapan

2. Pelaksanaan Sosialisasi

- a. Pemaparan materi secara interaktif mengenai pengertian *link scam*, jenis-jenisnya, contoh kasus penipuan digital yang marak di masyarakat, serta manfaat dan risiko penggunaan AI, seperti ditunjukkan pada gambar 2.
- b. Penyajian studi kasus nyata tentang modus penipuan berbasis *link scam* yang pernah terjadi di Indonesia maupun internasional (Eze & Shamir, 2024).
- c. Edukasi tentang tips menghindari tautan berbahaya dan langkah-langkah sederhana menjaga privasi digital keluarga.
- d. Pengenalan aplikasi berbasis AI yang bermanfaat untuk kegiatan sehari-hari, sekaligus memberikan peringatan risiko penyalahgunaan AI.



Gambar 2. Proses Pemateri

3. Diskusi dan Simulasi

- a. Sesi tanya jawab seputar pengalaman warga terhadap ancaman siber, seperti ditunjukkan pada gambar 3.
- b. Simulasi langsung bagaimana mengenali link scam, mengecek tautan palsu, dan menggunakan fitur keamanan seperti autentikasi dua faktor (2FA).
- c. Simulasi pengenalan AI sederhana yang aman untuk kebutuhan pendidikan anak dan monitoring kesehatan lansia.



Gambar 3. Diskusi Masalah

4. Evaluasi

- a. Pelaksanaan *pre-test* sebelum kegiatan dimulai untuk mengukur pengetahuan awal peserta.
- b. Pelaksanaan *post-test* setelah materi disampaikan untuk mengukur peningkatan pemahaman.
- c. Analisis perbandingan hasil *pre-test* dan *post-test* menggunakan deskriptif sederhana berupa diagram batang.

5. Dokumentasi

Seluruh kegiatan didokumentasikan dalam bentuk foto, video, dan laporan pelaksanaan.

Instrumen utama yang digunakan dalam kegiatan ini berupa kuesioner *pre-test* dan *post-test* berisi pertanyaan pilihan ganda dan skenario sederhana tentang ancaman digital serta pemanfaatan AI. Teknik analisis data menggunakan perhitungan persentase rata-rata

skor *pre-test* dan *post-test*, yang kemudian dibandingkan untuk mengetahui peningkatan pemahaman peserta. Selain itu, evaluasi kualitatif dilakukan dengan mencatat partisipasi warga dalam diskusi serta permintaan terhadap pelaksanaan kegiatan serupa di masa mendatang. Seluruh proses pelaksanaan kegiatan telah memperhatikan prinsip etika, di mana peserta diberikan informasi mengenai tujuan kegiatan, jaminan kerahasiaan data evaluasi, serta hak untuk mengikuti atau tidak mengikuti *pre-test* dan *post-test*.

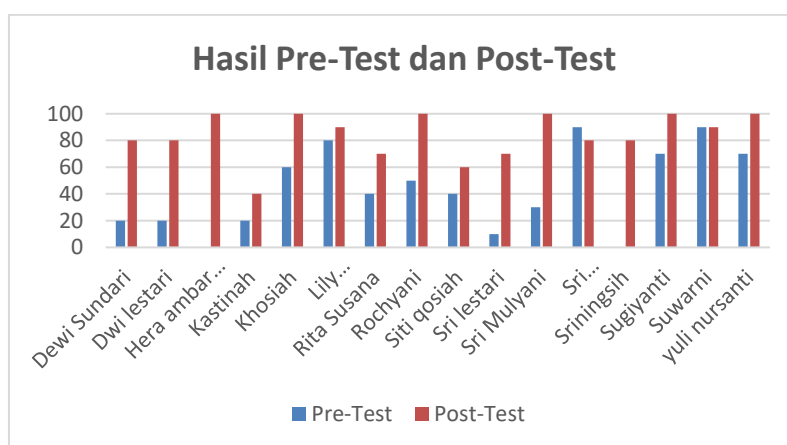
HASIL DAN PEMBAHASAN

Kegiatan pengabdian kepada masyarakat ini telah terlaksana dengan baik sesuai rencana yang ditetapkan. Kegiatan dilaksanakan pada tanggal 10 Maret 2025 di Balai RW 03 Kelurahan Kalipancur Kota Semarang dan dihadiri oleh warga dari beberapa RT di lingkungan RW 03, khususnya perwakilan kader PKK, posyandu, ibu rumah tangga, remaja, dan lansia. Jumlah peserta yang hadir sebanyak 18 orang. Pelaksanaan kegiatan berjalan lancar, dimulai dengan pembukaan oleh ibu ketua RW setempat, dilanjutkan penyampaian materi oleh tim pengabdian dari Program Studi Informatika Medis Universitas Widya Husada Semarang.

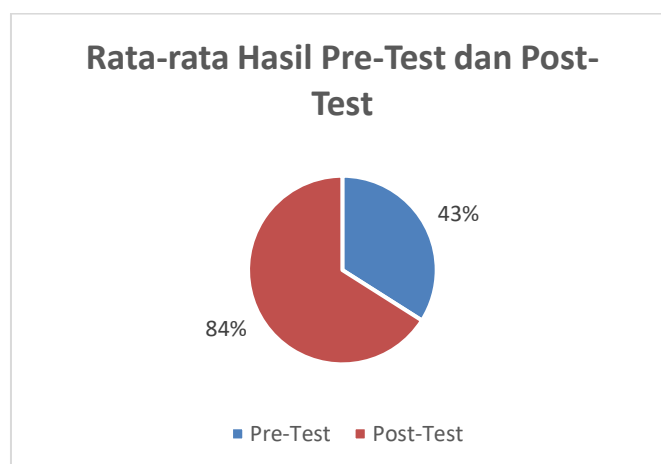
Secara umum, pelaksanaan kegiatan mendapat respon yang sangat positif dari warga. Antusiasme peserta terlihat sejak awal kegiatan, khususnya saat sesi penyampaian materi mengenai jenis-jenis *link scam* yang kerap muncul di media sosial, pesan instan, dan email. Beberapa peserta mengaku pernah menerima pesan tautan mencurigakan namun belum mengetahui cara memastikan keamanannya. Melalui simulasi sederhana yang ditampilkan, peserta dapat belajar membedakan tautan aman dan tautan berbahaya. Selain itu, materi mengenai kecerdasan buatan (AI) juga mendapatkan perhatian besar. Peserta baru mengetahui bahwa AI tidak hanya digunakan untuk keperluan hiburan, tetapi juga dapat dimanfaatkan dalam bidang pendidikan, kesehatan, hingga menjadi alat bagi pelaku kejahatan siber seperti *deepfake* dan *scam* berbasis AI.

Salah satu bagian penting dalam kegiatan ini adalah evaluasi pemahaman peserta yang dilakukan melalui *pre-test* sebelum kegiatan dan *post-test* setelah kegiatan. Grafik hasil pelaksanaan *pre-test* dan *post-test* dapat dilihat pada gambar 4. Hasil *pre-test* menunjukkan bahwa pemahaman awal warga terhadap ancaman *link scam* dan pemanfaatan AI secara bijak masih tergolong rendah, dengan rata-rata skor sebesar 43%.

Setelah penyampaian materi, simulasi, dan diskusi interaktif, terjadi peningkatan signifikan pada hasil *post-test* dengan rata-rata mencapai 84%. Hal ini menunjukkan adanya peningkatan pemahaman warga sebesar 41% terhadap materi yang disampaikan. Capaian ini melebihi target indikator keberhasilan yang ditetapkan sebelumnya, yakni peningkatan minimal 30%. Untuk hasil rata-rata pelaksanaan *Pre-Test* dan *Post-Test* dapat dilihat pada gambar 5.



Gambar 4. Grafik Hasil *Pre-Test* dan *Post-Test*



Gambar 5. Diagram Rata-Rata *Pre-Test* dan *Post-Test*

Selain evaluasi kuantitatif, observasi selama kegiatan juga menunjukkan bahwa warga sangat aktif dalam sesi diskusi. Banyak peserta yang berbagi pengalaman terkait upaya penipuan digital yang pernah mereka alami, mulai dari tautan undian berhadiah, info vaksin palsu, hingga *link* lowongan kerja tenaga medis ke luar negeri. Beberapa di antaranya bahkan mengaku baru mengetahui bahwa pesan-pesan tersebut merupakan modus *link scam*. Diskusi ini menjadi media edukasi langsung yang efektif, karena selain

memperdalam pemahaman materi, warga juga dapat saling berbagi cara sederhana untuk mencegah menjadi korban.

Dari kegiatan ini, dapat disimpulkan bahwa penyampaian materi dengan metode edukasi partisipatif berbasis simulasi dan diskusi sangat efektif untuk meningkatkan literasi digital masyarakat, khususnya di tingkat komunitas RW. Tidak hanya meningkatkan pengetahuan, kegiatan ini juga menumbuhkan kesadaran akan pentingnya menjaga keamanan data pribadi serta menggunakan teknologi AI secara bertanggung jawab. Selain itu, terdapat permintaan dari warga agar kegiatan serupa dapat diadakan kembali dengan topik-topik lanjutan seperti keamanan transaksi digital, literasi media sosial, serta penggunaan aplikasi kesehatan digital.

Dari hasil dokumentasi, materi edukasi telah diunggah ke laman daring yang dapat diakses warga kapan saja sebagai bahan belajar mandiri. Materi tersebut dapat diakses melalui tautan <https://downloadmateri.wordpress.com/2025/03/03/waspada-link-scam-dan-pemanfaatan-ai-kenali-ancaman-manfaatkan-teknologi-dengan-bijak/>. Dengan demikian, kegiatan ini tidak hanya berdampak pada peserta yang hadir, tetapi juga masyarakat luas yang dapat memanfaatkan materi tersebut di kemudian hari.

KESIMPULAN DAN SARAN

Kesimpulan

Pelaksanaan kegiatan pengabdian kepada masyarakat yang bertajuk “Peningkatan Literasi Digital Keluarga terhadap Link Scam dan Pemanfaatan AI di Wilayah RW 03 Kalipancur” di lingkungan RW 03 Kelurahan Kalipancur Kota Semarang terbukti efektif dalam meningkatkan literasi digital masyarakat, khususnya dalam hal mengenali ancaman *link scam* serta memanfaatkan kecerdasan buatan (AI) secara aman dalam kehidupan sehari-hari.

Hasil evaluasi menunjukkan adanya peningkatan signifikan pemahaman peserta, di mana rata-rata skor *pre-test* sebesar 43% meningkat menjadi 84% pada *post-test*. Peningkatan ini membuktikan bahwa metode edukasi partisipatif berbasis simulasi, diskusi interaktif, dan studi kasus nyata sangat efektif diterapkan di tingkat komunitas.

Selain itu, kegiatan ini berhasil menumbuhkan kesadaran masyarakat terhadap pentingnya menjaga keamanan data pribadi, mengenali modus penipuan digital, serta

memahami etika penggunaan teknologi AI. Warga juga menunjukkan antusiasme tinggi dalam diskusi, berbagi pengalaman terkait ancaman digital.

Saran

Berdasarkan hasil kegiatan, disarankan agar edukasi literasi digital di lingkungan RW dapat dilaksanakan secara rutin dan berkelanjutan, dengan topik yang disesuaikan perkembangan teknologi digital dan kebutuhan masyarakat. Materi kegiatan dapat diperluas ke isu-isu lain seperti keamanan transaksi daring, literasi media sosial, dan pemanfaatan aplikasi kesehatan berbasis AI.

Selain itu, diperlukan kerja sama lintas sektor antara perguruan tinggi, pemerintah kelurahan, pengurus RW, dan instansi terkait untuk menyelenggarakan program literasi digital yang terstruktur dan mudah diakses. Kegiatan ini diharapkan menjadi model pengabdian masyarakat berbasis literasi digital yang dapat direplikasi di wilayah lain guna memperkuat ketahanan masyarakat terhadap ancaman digital di era kecerdasan buatan.

DAFTAR PUSTAKA

- 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, RUSET 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>
- Eze, C. S., & Shamir, L. (2024). Analysis and Prevention of AI-Based Phishing Email Attacks. *Electronics*, 13(10), 1839. <https://doi.org/10.3390/electronics13101839>
- 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., Gabrijelčić, 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>
- Mim, S. A., Rahman, R., Asif, M. R. Al, Hasan, K. F., & Khondoker, R. (2023). *Cybersecurity Attacks and Vulnerabilities During COVID-19* (pp. 532–545). https://doi.org/10.1007/978-3-031-28694-0_50
- 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., & Fadjarini Sulistyowati. (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>