Cakrawala: Jurnal Pengabdian Masyarakat Global
Volume 5, Nomor 4, November 2026
E-ISSN: 2962-0848; P-ISSN: 2964-5271, Hal. 01-10
DOI: https://doi.org/10.30640/cakrawala.v5i4.7854
Tersedia: https://jurnaluniv45sby.ac.id/index.php/Cakrawala

Jangan Panik, Jangan Klik, Jangan Beri Kode: Penguatan Literasi Keamanan Digital untuk Pencegahan Penipuan pada Masyarakat Karang Malang Gunung Pati Semarang

Don't Panic, Don't Click, Don't Share Verification Codes: Strengthening Digital Security Literacy to Prevent Fraud among the Karang Malang Gunung Pati Semarang Community

Honorata Ratnawati Dwi Putranti[1*], Ribut Musprihadi[2]
[1-2]Fakultas Ekonomika da Bisnis Universitas 17 Agustus 1945 Semarang, Indonesia
**Penulis Korespondensi: Honorata-ratnawati@untagsmg.ac.id*

Riwayat Artikel:
Naskah Masuk: 20 Juni 2026;
Revisi: 25 Juli 2026;
Diterima: 28 Agustus 2026;
Terbit: 1 Novembr 2026.

Keywords: Community Service; Digital Fraud; Digital Security Literacy; Digital Verification; Participatory Education.

Abstract: *Digital fraud increasingly exploits trust, urgency, and emotional responses rather than technical weaknesses alone. This community service activity aimed to strengthen the digital security literacy of residents of Karang Malang, Gunungpati, Semarang. The activity was conducted on 19 August 2026 as part of the Community Service Program of Universitas 17 Agustus 1945 Semarang, using participatory education, case discussion, simulation, and the practical message 'Do Not Panic, Do Not Click, Do Not Share Codes.' A post-activity Kahoot quiz involving 30 participants consisted of 15 questions completed in 11 minutes. The overall correct-response rate was 71%, and all participants completed the quiz. However, only 7% answered correctly a question about an online contact requesting emergency money. The finding highlights the need for repeated scenario-based practice, simple verification procedures, and continuing dissemination through digital pocket guides and community communication channels.*

Abstrak

Penipuan digital semakin banyak memanfaatkan kepercayaan, tekanan waktu, dan respons emosional, bukan hanya kelemahan teknis. Kegiatan pengabdian ini bertujuan memperkuat literasi keamanan digital masyarakat Karang Malang, Gunungpati, Semarang. Kegiatan dilaksanakan pada 19 Agustus 2026 dalam rangka KKN Universitas 17 Agustus 1945 Semarang dengan pendekatan edukasi partisipatif, diskusi kasus, simulasi, dan pesan praktis "Jangan Panik, Jangan Klik, Jangan Beri Kode". Evaluasi setelah kegiatan menggunakan Kahoot yang diikuti 30 peserta, terdiri atas 15 pertanyaan dan berlangsung selama 11 menit. Persentase jawaban benar secara keseluruhan mencapai 71% dan seluruh peserta menyelesaikan kuis. Namun, hanya 7% peserta menjawab benar pertanyaan tentang permintaan uang darurat dari seseorang yang dikenal melalui internet. Temuan ini menunjukkan perlunya penguatan berulang melalui latihan berbasis skenario, prosedur verifikasi sederhana, serta penyebaran buku saku digital melalui saluran komunikasi warga.

Kata kunci: Edukasi Partisipatif; Literasi Keamanan Digital; Pengabdian Masyarakat; Penipuan Digital; Verifikasi Digital.

1. PENDAHULUAN

Perkembangan teknologi digital telah mengubah cara masyarakat berkomunikasi, memperoleh informasi, membangun relasi sosial, dan melakukan transaksi keuangan. Kemudahan tersebut sekaligus memperluas paparan terhadap pesan palsu, tautan berbahaya, pencurian data, dan berbagai bentuk penipuan daring. Karena itu, kecakapan digital tidak cukup dimaknai sebagai kemampuan mengoperasikan perangkat, tetapi juga mencakup kemampuan menilai risiko dan melindungi diri ketika berinteraksi di ruang digital (Adikara et al., 2021; Zhang-Kennedy & Chiasson, 2021).

Penipuan digital telah menjadi persoalan sosial yang membutuhkan perhatian bersama. Indonesia Anti-Scam Centre menerima 432.637 laporan penipuan sejak 22 November 2024 hingga 14 Januari 2026, dengan nilai kerugian yang dilaporkan mencapai Rp9,1 triliun (Otoritas Jasa Keuangan [OJK], 2026). Besarnya laporan tersebut menunjukkan bahwa risiko penipuan tidak hanya berdampak pada kehilangan uang, tetapi juga dapat menimbulkan kecemasan, rasa malu, keretakan hubungan sosial, dan menurunnya kepercayaan masyarakat terhadap layanan digital.

Salah satu karakter utama penipuan digital adalah penggunaan social engineering, yaitu manipulasi psikologis untuk mendorong korban melakukan tindakan yang menguntungkan pelaku. Pelaku dapat menciptakan rasa mendesak, ketakutan, rasa kasihan, ketertarikan emosional, atau kesan sebagai pihak yang berwenang agar korban mengeklik tautan, mentransfer uang, atau memberikan OTP, PIN, kata sandi, dan kode verifikasi. Kajian menunjukkan bahwa kerentanan manusia, tekanan situasional, dan kurangnya kesadaran menjadi titik masuk penting dalam serangan semacam ini (Aldawood & Skinner, 2019; Siddiqi et al., 2022; Syafitri et al., 2022).

Kerentanan tersebut tidak identik dengan ketidakmampuan korban. Serangan *social engineering* dirancang untuk memanfaatkan kebiasaan mengambil keputusan cepat, kepercayaan kepada orang lain, kepatuhan terhadap otoritas, kelelahan informasi, dan respons emosional. Oleh karena itu, pertahanan keamanan digital perlu membangun *'human fir*ewall', yakni kebiasaan berhenti sejenak, memeriksa sumber, memverifikasi permintaan melalui saluran lain, dan melaporkan kejadian mencurigakan (Tsauri, 2025).

Permintaan uang darurat dari seseorang yang dikenal melalui internet merupakan salah satu contoh manipulasi yang perlu dikenali. Modus ini dapat muncul dalam berbagai bentuk, termasuk penyamaran sebagai teman atau keluarga, akun yang diretas, pinjaman fiktif, maupun love scam. Pada love scam, pelaku membangun kedekatan emosional sebelum mengajukan permintaan uang sehingga keputusan korban dipengaruhi kepercayaan dan keterikatan yang telah dibentuk (Drew & Webster, 2024). Dengan demikian, edukasi perlu membahas love scam sebagai salah satu bagian dari spektrum penipuan digital, bukan sebagai satu-satunya fokus kegiatan.

Masyarakat Karang Malang, Gunungpati, Semarang, dipilih sebagai lokasi kegiatan karena merupakan lokasi pelaksanaan KKN mahasiswa Universitas 17 Agustus 1945 Semarang dan berada pada kawasan pinggiran/perbatasan kota. Kondisi tersebut memberi peluang bagi perguruan tinggi untuk mendekatkan edukasi keamanan digital kepada warga melalui kegiatan yang kontekstual dan mudah diakses. Informasi rinci mengenai pola

penggunaan media digital dan pengalaman penipuan warga masih memerlukan pemetaan lebih lanjut melalui komunikasi non formal bersama kepala desa dan beberapa masyarakat setempat.

Edukasi keamanan digital perlu menggunakan pesan yang sederhana, relevan dengan pengalaman sehari-hari, dan dapat segera dipraktikkan. Program kesadaran keamanan lebih bermanfaat ketika tidak berhenti pada penyampaian informasi, tetapi mengarahkan peserta pada tindakan yang jelas dan membangun kebiasaan aman (Alshaikh et al., 2021). Kampanye publik juga perlu menyebutkan perilaku sasaran secara konkret, misalnya menunda respons, memeriksa alamat tautan, menjaga kode rahasia, dan melakukan verifikasi melalui kanal resmi (van Steen et al., 2020).

Atas dasar kebutuhan tersebut, pada 19 Agustus 2026 dilaksanakan kegiatan pengabdian kepada masyarakat dalam rangka KKN Universitas 17 Agustus 1945 Semarang di Karang Malang, Gunungpati, Semarang. Kegiatan mengangkat pesan utama “Jangan Panik, Jangan Klik, Jangan Beri Kode” melalui paparan singkat, diskusi kasus, simulasi, dan kuis Kahoot. Kegiatan ini bertujuan memperkuat kemampuan warga dalam mengenali tanda penipuan, melindungi data pribadi, memverifikasi permintaan, menolak pemberian kode rahasia, serta mengambil langkah aman ketika menemukan pesan atau transaksi yang mencurigakan.





Gambar 1. Poster pesan utama edukasi keamanan digital bagi warga

2. METODE

Kegiatan pengabdian kepada masyarakat ini menggunakan pendekatan edukasi partisipatif berbasis kasus dan simulasi. Pendekatan tersebut menempatkan peserta sebagai pihak yang aktif mengidentifikasi tanda bahaya, mendiskusikan pilihan tindakan, dan mencoba langkah verifikasi. Kegiatan dilaksanakan pada 19 Agustus 2026 di Karang Malang,

Gunungpati, Semarang, dalam rangka KKN Universitas 17 Agustus 1945 Semarang. Peserta kegiatan berjumlah 30 orang warga yang hadir pada saat pelaksanaan.

Pelaksanaan kegiatan terdiri atas lima tahap, yaitu: (1) identifikasi kebutuhan dan penyusunan contoh kasus yang dekat dengan pengalaman warga; (2) persiapan materi, poster, skenario percakapan, dan kuis Kahoot; (3) penyampaian materi mengenai ciri penipuan, social engineering, perlindungan data pribadi, dan mekanisme verifikasi; (4) diskusi serta simulasi respons terhadap pesan mencurigakan; dan (5) evaluasi pemahaman setelah kegiatan serta penyusunan rencana tindak lanjut. Tahapan tersebut disajikan pada Gambar 2.

Materi disampaikan menggunakan pesan utama “Jangan Panik, Jangan Klik, Jangan Beri Kode”. “Jangan Panik” mengarahkan peserta untuk berhenti sejenak ketika menerima pesan yang mendesak atau menakutkan. “Jangan Klik” mengingatkan peserta agar tidak membuka tautan atau berkas sebelum memeriksa sumbernya. “Jangan Beri Kode” menegaskan bahwa OTP, PIN, kata sandi, CVV, dan kode verifikasi tidak boleh diberikan kepada siapa pun. Peserta kemudian berlatih menerapkan tiga prinsip tersebut pada contoh pesan hadiah palsu, akun yang menyamar sebagai kerabat, permintaan uang darurat, serta pendekatan emosional di internet.



Gambar 2. Tahapan pelaksanaan edukasi keamanan digital

Evaluasi dilakukan sekali setelah penyampaian materi dan simulasi menggunakan kuis interaktif Kahoot. Kuis berjudul “Waspada Jebakan Cinta Online: Kenali Modus Penipu!” terdiri atas 15 pertanyaan yang mengukur kemampuan mengenali tanda penipuan, menjaga informasi rahasia, memverifikasi identitas dan permintaan, serta memilih tindakan aman. Data dianalisis secara deskriptif menggunakan jumlah peserta, persentase jawaban benar keseluruhan, ketuntasan penyelesaian, waktu pelaksanaan, dan pertanyaan yang paling sulit. Karena tidak terdapat pretest, hasil tidak ditafsirkan sebagai peningkatan pengetahuan, melainkan sebagai gambaran capaian pemahaman setelah edukasi.

3. HASIL

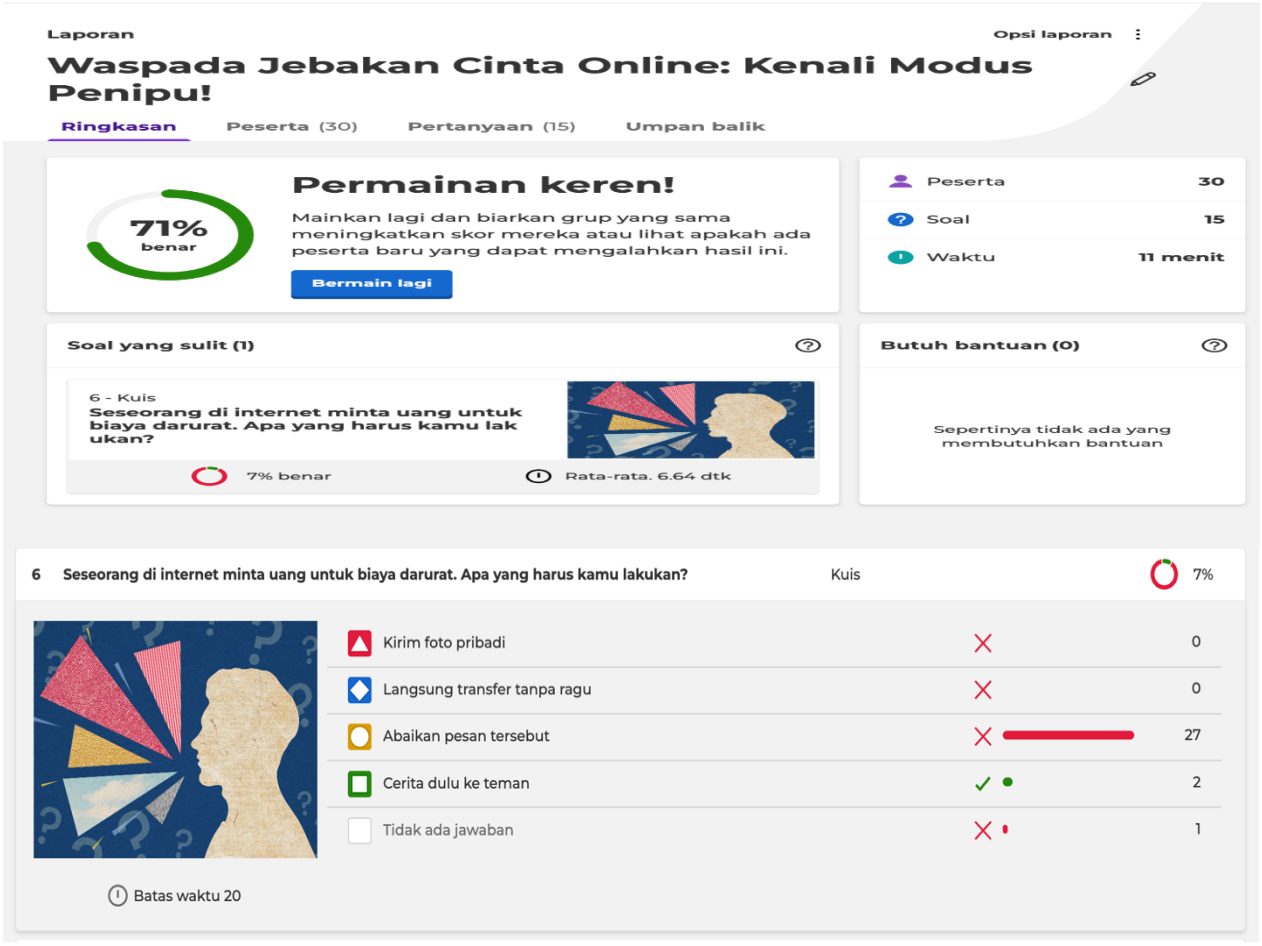
Hasil Evaluasi Pemahaman Peserta melalui Kahoot

Evaluasi setelah kegiatan diikuti oleh 30 peserta melalui 15 pertanyaan Kahoot dan berlangsung selama 11 menit. Laporan menunjukkan persentase jawaban benar secara keseluruhan sebesar 71%. Seluruh peserta menyelesaikan kuis, tidak terdapat peserta yang tercatat membutuhkan bantuan, dan satu pertanyaan dikategorikan sulit. Ringkasan hasil disajikan pada Tabel 1

Tabel 1. Ringkasan hasil evaluasi melalui Kahoot

Indikator	Hasil
Jumlah peserta	30 orang
Jumlah pertanyaan	15 soal
Durasi pelaksanaan	11 menit
Persentase jawaban benar	71%
Jumlah soal yang tergolong sulit	1 soal
Peserta yang tidak menyelesaikan kuis	0 orang

Capaian 71% menunjukkan bahwa sebagian besar jawaban peserta setelah edukasi telah sesuai dengan materi. Meskipun demikian, masih terdapat sekitar 29% jawaban yang belum tepat secara agregat. Data ini tidak menunjukkan perubahan sebelum dan sesudah kegiatan karena evaluasi hanya dilakukan pada akhir sesi.



Gambar 3. Ringkasan hasil evaluasi peserta melalui Kahoot pada 19 Agustus 2026

Gambar 3 memperlihatkan identitas waktu pelaksanaan, jumlah peserta, jumlah pertanyaan, durasi, dan persentase jawaban benar. Tangkapan layar dipertahankan secara utuh agar tanggal 19 Agustus 2026 tetap terbaca sebagai bagian dari dokumentasi kegiatan.

Analisis Pertanyaan yang Sulit

Laporan Kahoot mengidentifikasi pertanyaan keenam sebagai pertanyaan paling sulit: "Seseorang di internet meminta uang untuk biaya darurat. Apa yang harus kamu lakukan?" Hanya 7% peserta menjawab benar, dengan waktu respons rata-rata 6,64 detik. Hasil tersebut menunjukkan bahwa skenario permintaan uang yang memanfaatkan rasa kasihan dan situasi

mendesak masih sulit direspons secara aman.

Temuan tersebut menjadi dasar untuk menegaskan kembali tindakan yang disarankan: tidak langsung mentransfer uang, menghentikan percakapan sementara, memeriksa identitas melalui saluran komunikasi lain, meminta bantuan orang yang dipercaya, dan melaporkan akun apabila terdapat indikasi penipuan. Love scam dapat digunakan sebagai salah satu contoh, tetapi prinsip verifikasi yang sama juga berlaku pada penyamaran sebagai teman, kerabat, petugas, atau pihak lain.

Kegiatan edukasi dilaksanakan secara tatap muka dengan melibatkan 30 peserta. Materi disampaikan melalui penjelasan singkat, contoh kasus, diskusi, dan simulasi respons terhadap pesan mencurigakan. Peserta juga mengikuti evaluasi interaktif menggunakan Kahoot setelah penyampaian materi. Dokumentasi pelaksanaan kegiatan ditampilkan pada Gambar 4.



(a) (b)

Gambar 4. Pelaksanaan edukasi keamanan digital di Karang Malang

(a) penyampaian materi mengenai modus penipuan digital

(b) peserta mengikuti evaluasi melalui Kahoot.Hasil evaluasi menunjukkan bahwa 30 peserta menyelesaikan 15 pertanyaan dalam waktu 11 menit dengan persentase

Jawaban benar keseluruhan sebesar 71%. Capaian tersebut menggambarkan adanya pemahaman dasar setelah edukasi, terutama karena seluruh peserta berhasil mengikuti evaluasi sampai selesai. Namun, sekitar 29% jawaban yang belum tepat secara agregat menunjukkan bahwa pemahaman belum merata. Literasi keamanan digital mencakup kemampuan mengenali risiko sekaligus menerapkan tindakan perlindungan ketika menghadapi situasi nyata; karena itu, hasil kuis perlu dibaca sebagai capaian awal, bukan bukti perubahan perilaku jangka

panjang (Vuorikari et al., 2022).

Temuan paling menonjol terdapat pada pertanyaan mengenai seseorang di internet yang meminta uang untuk biaya darurat; hanya 7% peserta menjawab benar. Pola tersebut memperlihatkan bahwa tekanan emosional dan rasa mendesak dapat mengurangi kehati-hatian, sejalan dengan kajian yang menempatkan faktor manusia sebagai unsur penting dalam kerentanan keamanan siber (Khadka & Ullah, 2025). Permintaan semacam itu dapat muncul dalam peniruan identitas, akun yang diretas, atau love scam. Dalam love scam, kedekatan emosional dibangun sebelum permintaan uang diajukan sehingga korban lebih sulit melakukan penilaian secara objektif (Coluccia et al., 2020).

Penggunaan contoh kasus dan simulasi relevan karena peserta tidak hanya diminta mengingat definisi, tetapi juga memilih tindakan ketika menghadapi pesan yang menyerupai situasi sehari-hari. Tinjauan sistematis menunjukkan bahwa pelatihan kesadaran keamanan perlu dirancang berdasarkan konteks, kelompok sasaran, metode penyampaian, dan evaluasi yang jelas agar pengetahuan dapat diterjemahkan menjadi perilaku aman (Prümmer et al., 2024). Oleh karena itu, simulasi selanjutnya perlu memperbanyak variasi kasus, misalnya permintaan uang darurat, hadiah palsu, tautan pembaruan akun, serta permintaan OTP oleh pihak yang mengaku petugas.

Penggunaan Kahoot mendukung keterlibatan peserta dan memberi umpan balik langsung mengenai topik yang belum dipahami. Meta-analisis menunjukkan bahwa Kahoot secara umum dapat memberikan pengaruh positif pada hasil belajar, motivasi, keterlibatan, dan dinamika kelas, meskipun efektivitasnya tetap dipengaruhi rancangan soal dan konteks penerapan (Özdemir, 2025). Pada kegiatan ini, identifikasi satu pertanyaan sulit memberi manfaat diagnostik untuk menentukan materi yang perlu dijelaskan kembali.

Prinsip “Jangan Panik, Jangan Klik, Jangan Beri Kode” berfungsi sebagai pengingat tindakan yang ringkas. Pesan ini mengubah konsep keamanan digital menjadi tiga langkah: menahan respons emosional, menghindari interaksi teknis yang berisiko, dan menjaga informasi autentikasi. Tinjauan mengenai pembelajaran keamanan siber berbasis permainan menunjukkan bahwa unsur interaktif dapat mendukung kesadaran dan pembelajaran, tetapi perlu dirancang dengan tujuan serta evaluasi yang terukur (Weeratunge et al., 2026). Karena itu, pesan tiga langkah perlu diulang melalui poster, buku saku digital, grup WhatsApp warga, dan simulasi berkala.

Kegiatan ini memiliki keterbatasan karena evaluasi hanya dilakukan setelah materi, tanpa pretest, kelompok pembanding, dan pengukuran lanjutan. Hasil 71% tidak dapat digunakan untuk menyatakan peningkatan pengetahuan akibat kegiatan. Evaluasi berikutnya disarankan menggunakan pretest dan posttest dengan pertanyaan yang setara, disertai tindak

lanjut setelah beberapa minggu untuk menilai retensi dan penerapan perilaku aman. Rencana tindak lanjut dapat melibatkan pengurus RT/RW, mahasiswa KKN, dan perguruan tinggi untuk memperbarui contoh modus, membagikan buku saku digital, serta menyediakan jalur rujukan pelaporan.

4. KESIMPULAN

Kegiatan pengabdian kepada masyarakat melalui edukasi "Jangan Panik, Jangan Klik, Jangan Beri Kode" memberikan panduan praktis kepada masyarakat Karang Malang untuk mengenali dan merespons penipuan digital. Pendekatan partisipatif berbasis kasus dan simulasi membantu menghubungkan materi tentang social engineering, perlindungan data pribadi, dan verifikasi identitas dengan situasi yang mungkin dijumpai warga dalam komunikasi sehari-hari.

Evaluasi Kahoot yang diikuti 30 peserta menunjukkan persentase jawaban benar keseluruhan sebesar 71%, dan seluruh peserta menyelesaikan 15 pertanyaan dalam waktu 11 menit. Pertanyaan tentang permintaan uang darurat dari seseorang yang dikenal melalui internet hanya dijawab benar oleh 7% peserta. Temuan tersebut memperlihatkan bahwa manipulasi berbasis rasa kasihan dan urgensi perlu menjadi fokus penguatan berikutnya. Karena evaluasi hanya dilakukan setelah kegiatan, hasil ini menggambarkan capaian pemahaman pascaedukasi dan tidak dapat ditafsirkan sebagai peningkatan pengetahuan.

Keberlanjutan kegiatan dapat dilakukan melalui penyebaran poster dan buku saku digital, pengulangan pesan tiga langkah dalam grup WhatsApp warga, simulasi berkala, serta pelibatan pengurus RT/RW, mahasiswa KKN, dan perguruan tinggi. Evaluasi mendatang perlu menggunakan pretest–posttest dan pengukuran lanjutan agar perubahan pengetahuan, retensi, dan penerapan perilaku aman dapat dinilai secara lebih kuat.

PENGAKUAN/ACKNOWLEDGEMENTS

Penulis menyampaikan terima kasih kepada perangkat wilayah Karang Malang, Kecamatan Gunungpati, Kota Semarang, dosen pembimbing lapangan, serta mahasiswa KKN Universitas 17 Agustus 1945 Semarang atas dukungan dan kerja sama dalam pelaksanaan kegiatan ini. Apresiasi juga disampaikan kepada seluruh warga Karang Malang yang telah berpartisipasi aktif dalam kegiatan edukasi keamanan digital dan evaluasi.

REFERENSI

Adikara, G. J., Kurnia, N., Adhrianti, L., Astuty, S., Wijayanto, X. A., Desiana, F., & Astuti, S. I. (2021). Aman bermedia digital. Direktorat Jenderal Aplikasi Informatika, Kementerian Komunikasi dan Informatika. https://literasidigital.id/books/modul-aman-bermedia-digital

Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. Future Internet, 11(3), Article 73. https://doi.org/10.3390/fi11030073

Alshaikh, M., Maynard, S. B., & Ahmad, A. (2021). Applying social marketing to evaluate current security education training and awareness programs in organisations. Computers & Security, 100, Article 102090. https://doi.org/10.1016/j.cose.2020.102090

Coluccia, A., Pozza, A., Ferretti, F., Carabellese, F., Masti, A., & Gualtieri, G. (2020). Online romance scams: Relational dynamics and psychological characteristics of the victims and scammers. A scoping review. Clinical Practice & Epidemiology in Mental Health, 16, 24–35. https://doi.org/10.2174/1745017902016010024

Drew, J. M., & Webster, J. (2024). The victimology of online fraud: A focus on romance fraud victimisation. Journal of Economic Criminology, 3, Article 100053. https://doi.org/10.1016/j.jeconc.2024.100053

Khadka, K., & Ullah, A. B. (2025). Human factors in cybersecurity: An interdisciplinary review and framework proposal. International Journal of Information Security, 24, Article 119. https://doi.org/10.1007/s10207-025-01032-0

Otoritas Jasa Keuangan. (2026). Indonesia Anti-Scam Centre berhasil kembalikan Rp161 miliar dana masyarakat korban scam. https://www.ojk.go.id/id/berita-dan-kegiatan/siaran-pers/Pages/Indonesia-Anti-Scam-Centre-Berhasil-Kembalikan-Rp161-Miliar-Dana-Masyarakat-Korban-Scam.aspx

Özdemir, O. (2025). Kahoot! game-based digital learning platform: A comprehensive meta-analysis. Journal of Computer Assisted Learning, 41(1), Article e13084. https://doi.org/10.1111/jcal.13084

Prümmer, J., van Steen, T., & van den Berg, B. (2024). A systematic review of current cybersecurity training methods. Computers & Security, 136, Article 103585. https://doi.org/10.1016/j.cose.2023.103585

Siddiqi, M. A., Pak, W., & Siddiqi, M. A. (2022). A study on the psychology of social engineering-based cyberattacks and existing countermeasures. Applied Sciences, 12(12), Article 6042. https://doi.org/10.3390/app12126042

Syafitri, W., Shukur, Z., Mokhtar, U. A., Sulaiman, R., & Ibrahim, M. A. (2022). Social engineering attacks prevention: A systematic literature review. IEEE Access, 10, 39325–39343. https://doi.org/10.1109/ACCESS.2022.3162594

Tsauri, M. S. (2025). Human vulnerabilities to social engineering attacks: A systematic literature review for building a human firewall. Journal of Applied Informatics and Computing, 9(4), 1127–1136. https://doi.org/10.30871/jaic.v9i4.9585

van Steen, T., Norris, E., Atha, K., & Joinson, A. (2020). What (if any) behaviour change techniques do government-led cybersecurity awareness campaigns use? Journal of Cybersecurity, 6(1), Article tyaa019. https://doi.org/10.1093/cybsec/tyaa019

Vuorikari, R., Kluzer, S., & Punie, Y. (2022). DigComp 2.2: The digital competence framework for citizens—with new examples of knowledge, skills and attitudes. Publications Office of the European Union. https://doi.org/10.2760/115376

Weeratunge, H., Hjelsvold, R., & Katt, B. (2026). Game-based learning and gamification for cybersecurity awareness and education: A systematic scoping review. International Journal of Information Security, 25, Article 71. https://doi.org/10.1007/s10207-026-01239-9

Zhang-Kennedy, L., & Chiasson, S. (2021). A systematic review of multimedia tools for cybersecurity awareness and education. ACM Computing Surveys, 54(1), Article 12, 1–39. https://doi.org/10.1145/3427920