ABDIRA Volume 7 Nomor 1 Tahun 2027 Halaman 117-127
JURNAL PENGABDIAN MASYARAKAT
Research & Learning in Faculty of Education
ISSN: 2798-0847 (Printed); 2798-4591 (Online)

Sosialisasi Keamanan Informasi dan Pemanfaatan AI untuk Mencegah Phishing dan Penipuan Digital

Risah Subariah[1], Galuh Oka Safitri[2], Chandra Hermawan[3], Anelka Ivan Martin[4], Afira Dinanti[5], Kalila Aimeealika Kei Al Ansah[6], Muhamad Rizqi Heriawan[7], Presha Fitriyani[8]

Program Studi Sistem Informasi, Universitas Pamulang
e-mail: risahsubariah@unpam.ac.id

Abstrak

Penipuan digital dan pengambilalihan akun media sosial menjadi masalah yang dihadapi masyarakat, termasuk remaja Karang Taruna Kelurahan Cipayung, Kecamatan Ciputat, Kota Tangerang Selatan. Dalam diskusi awal, mitra menyampaikan bahwa peserta pernah menerima pesan atau tautan mencurigakan, sedangkan edukasi keamanan siber secara khusus belum pernah diselenggarakan di wilayah itu. Kegiatan pengabdian ini bertujuan memberikan edukasi tentang keamanan informasi, pencegahan *phishing* dan penipuan digital, serta pemanfaatan kecerdasan buatan (AI) secara bijak. Pendekatannya edukatif partisipatif, yaitu sosialisasi tatap muka yang diisi presentasi interaktif, pembahasan contoh kasus, diskusi, dan tanya jawab. Kegiatan berlangsung pada 3 Oktober 2026 dan diikuti lebih dari 20 remaja. Seluruh materi yang direncanakan dapat disampaikan, dan peserta aktif membahas pelindungan data pribadi serta kata sandi sambil berbagi pengalaman menerima pesan mencurigakan. Kegiatan ini diharapkan menjadi landasan bagi edukasi keamanan digital yang berkelanjutan di lingkungan Karang Taruna Kelurahan Cipayung.

Kata Kunci: *Keamanan Informasi, Phishing, Penipuan Digital, Kecerdasan Buatan, Karang Taruna, Pengabdian Masyarakat.*

Abstract

Digital fraud and social media account takeovers have become issues affecting communities, including the youth of Karang Taruna in Cipayung Urban Village, Ciputat District, South Tangerang City. Preliminary discussions with the community partner indicated that participants had received suspicious messages or links, while specific cybersecurity education had not previously been conducted in the area. This community service activity aimed to provide education on information security, phishing and digital fraud prevention, and the responsible use of artificial intelligence (AI). The activity employed an educational participatory approach through face-to-face socialization, interactive presentations, case example discussions, group discussions, and question-and-answer sessions. It was conducted on October 3, 2026, involving more than 20 teenagers. The results showed that all planned materials were delivered, participants actively discussed personal data and password protection, and shared their experiences of receiving suspicious messages. This activity is expected to provide a foundation for strengthening digital security education on an ongoing basis within Karang Taruna in Cipayung Urban Village.

Kata Kunci: *Information Security, Phishing, Digital Fraud, Artificial Intelligence, Digital Literacy, Youth Organization.*

PENDAHULUAN

Perkembangan penggunaan internet di Indonesia menunjukkan semakin luasnya aktivitas masyarakat di ruang digital. Berdasarkan Survei Penetrasi Internet dan Perilaku Penggunaan Internet 2025, jumlah pengguna internet di Indonesia mencapai 229.428.417 jiwa atau sekitar 80,66% dari total populasi (Asosiasi Penyelenggara Jasa Internet Indonesia [APJII], 2025). Internet kini menjadi bagian penting dari aktivitas sehari-hari, tetapi pertambahan penggunanya perlu diimbangi pemahaman tentang keamanan informasi dan pelindungan data pribadi. Laporan Indeks Masyarakat Digital Indonesia (IMDI) 2025 mencatat skor nasional sebesar 44,53, naik 1,19 poin dari skor 43,34 pada 2024 (Badan Pengembangan Sumber Daya Manusia Komunikasi dan Digital [BPSDM Komdigi], 2025). IMDI mengukur perkembangan masyarakat digital melalui empat pilar, yaitu infrastruktur dan ekosistem, literasi digital, pemberdayaan, serta pekerjaan. Gambaran ini memperkuat perlunya edukasi keamanan informasi, khususnya bagi remaja, agar mereka mampu mengenali risiko penipuan digital dan melindungi data pribadi ketika beraktivitas di internet (Sales et al., 2024).

Keamanan informasi tidak hanya soal perangkat keras dan perangkat lunak. Pada tingkat individu, prinsip kerahasiaan, integritas, dan ketersediaan informasi diwujudkan lewat kebiasaan harian: menjaga kerahasiaan kata sandi dan kode *one-time password* (OTP) serta membatasi data pribadi yang dipublikasikan. Kurniawan et al. (2023) menemukan bahwa pengguna media sosial yang aktif cenderung lebih banyak mengunggah data pribadi demi manfaat sosial, sementara usia muda menempati proporsi pengguna terbesar. Di Indonesia, landasan hukum pelindungan data pribadi adalah Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (Republik Indonesia, 2022).

Phishing adalah bentuk serangan siber yang paling umum dan berdampak luas, sebab sasarannya sisi psikologis pengguna melalui rekayasa sosial (Jabir et al., 2025). Nur'aini dan Simanjuntak (2025) memaparkan bahwa *phishing* menempati peringkat teratas kejahatan siber di Indonesia pada periode 2017–2022, sedangkan Loh et al. (2024) mencatat sedikitnya 323.972 korban *phishing* secara global pada 2021 meskipun pemblokiran otomatis telah luas diterapkan. Pelaku memanfaatkan pemicu emosi berupa rasa takut, keserakahan, rasa ingin tahu, dan keinginan menolong. Pesannya dapat berupa kabar pemblokiran rekening atau hadiah undian, juga berkas aplikasi berekstensi .apk yang dikirim lewat aplikasi pesan instan. Pengetahuan tentang pola *phishing* berhubungan positif dengan kewaspadaan pengguna (Nur'aini & Simanjuntak, 2025).

Kecerdasan buatan (*artificial intelligence*, AI) menghadirkan dua sisi bagi keamanan siber. Di satu sisi, sistem deteksi *phishing* berbasis pembelajaran mesin dapat membantu mengenali ancaman, tetapi masih menghadapi persoalan

akurasi, positif palsu, negatif palsu, dan tingkat kepercayaan pengguna (Shahbazi et al., 2025). Di sisi lain, AI generatif memungkinkan pelaku menyusun pesan penipuan dengan tata bahasa yang rapi (Jabir et al., 2025; Schmitt & Flechais, 2024), sehingga kesalahan ketik tidak lagi dapat dijadikan satu-satunya penanda pesan palsu. Panduan National Institute of Standards and Technology [NIST] (2026) juga memandang AI dari dua arah: dampak adopsinya terhadap risiko keamanan siber dan privasi, serta pengaruh pertimbangan keamanan terhadap batas pemanfaatan AI. Karena itu, pengguna perlu dibekali kemampuan memverifikasi informasi, dan AI dapat diperkenalkan sebagai alat bantu pemeriksaan awal yang hasilnya tetap harus diverifikasi (Loh et al., 2024).

Remaja intens memakai gawai untuk belajar, bersosialisasi, mencari hiburan, dan bertransaksi, sehingga mereka rentan terhadap manipulasi digital. Karang Taruna sebagai wadah pembinaan pemuda di tingkat kelurahan memiliki jaringan sosial yang luas dan berpotensi menyebarkan pengetahuan kepada keluarga dan teman sebaya. Pengabdian terdahulu pada Karang Taruna di Benda Baru, Pamulang (Susanti et al., 2022) dan di Baturraden (Fajarwati & Suhartono, 2024) berfokus pada keamanan data pribadi, kerahasiaan OTP, dan kewaspadaan terhadap tautan yang tidak jelas. Pengabdian pada pelajar oleh Hidayat et al. (2025) memadukan sosialisasi, simulasi, dan diskusi. Dalam telaah penulis, kegiatan-kegiatan tersebut belum memuat pemanfaatan AI sebagai alat bantu pemeriksaan pesan mencurigakan.

Dari tiga kegiatan terdahulu yang ditelaah dalam artikel ini, fokus edukasinya umumnya adalah pelindungan data pribadi, kerahasiaan OTP, dan pencegahan *phishing* melalui sosialisasi, pelatihan, serta pembahasan contoh kasus. Kegiatan ini menambahkan pengenalan AI sebagai alat bantu pemeriksaan awal terhadap pesan mencurigakan, dengan tetap menekankan verifikasi melalui sumber resmi. Pengenalan AI itulah yang menjadi pembeda kegiatan ini dari kegiatan terdahulu yang dijadikan pembanding.

Dalam diskusi awal, mitra menyampaikan bahwa penipuan digital dan pengambilalihan akun media sosial pernah dialami warga, sedangkan edukasi keamanan siber secara khusus belum pernah diselenggarakan di wilayah tersebut. Peserta juga menyampaikan bahwa mereka pernah menerima pesan atau tautan mencurigakan. Atas dasar itu, kegiatan ini bertujuan (1) membangun pemahaman tentang pentingnya keamanan informasi dan pelindungan data pribadi; (2) meningkatkan pemahaman tentang risiko dan ancaman pada media sosial, pesan instan, dan platform digital; (3) meningkatkan kemampuan mengenali karakteristik *phishing* dan penipuan digital; dan (4) mengenalkan pemanfaatan AI sebagai alat bantu yang bijak dan bertanggung jawab.

METODE

Kegiatan pengabdian ini memakai pendekatan edukatif partisipatif berupa sosialisasi tatap muka yang memadukan ceramah terpandu, pembahasan contoh kasus, dan diskusi dua arah. Mitranya adalah Remaja Karang Taruna Kelurahan Cipayung, Kecamatan Ciputat, Kota Tangerang Selatan, Provinsi Banten. Kegiatan

berlangsung secara luring pada Sabtu, 3 Oktober 2026, di kediaman Ketua Karang Taruna. Lokasi ini dipilih karena mudah dijangkau peserta, ruangnya cukup memadai untuk pemaparan materi visual, dan suasananya akrab sehingga mendukung dialog. Pesertanya lebih dari 20 remaja anggota Karang Taruna.

Kegiatan dilaksanakan dalam lima tahap. Pertama, observasi awal dan penetapan topik untuk memetakan kondisi mitra dan kebutuhan edukasi keamanan siber. Kedua, pra-survei berupa diskusi awal dengan pimpinan mitra untuk menggali pengalaman peserta menerima pesan mencurigakan, tautan tidak dikenal, atau akun tiruan, yang hasilnya dipakai untuk menyesuaikan materi dan contoh kasus. Ketiga, persiapan yang meliputi perizinan, koordinasi teknis dengan Ketua Karang Taruna, dan penyusunan materi presentasi. Keempat, pelaksanaan sosialisasi. Kelima, evaluasi, pelaporan, dan penyusunan luaran publikasi.

Materi disampaikan lewat presentasi yang terbagi atas empat bagian. Bagian pertama membahas keamanan informasi dan pelindungan data pribadi, mencakup jenis informasi yang perlu dilindungi, risiko penyalahgunaannya, kata sandi yang kuat, autentikasi tambahan, dan kerahasiaan kode OTP. Bagian kedua menguraikan ancaman digital dan karakteristik *phishing* pada media sosial, pesan instan, surel, panggilan telepon, dan situs web tiruan. Bagian ketiga berisi langkah pencegahan, yaitu verifikasi sumber, pemeriksaan tautan dan nama domain, serta sikap tenang terhadap pesan yang mendesak. Bagian keempat memperkenalkan AI sebagai alat bantu pemeriksaan awal, dengan penekanan pada verifikasi melalui sumber resmi. Setelah itu, presentasi dilanjutkan dengan penjelasan dan pembahasan contoh kasus, diskusi, tanya jawab, dan pembagian *slide* materi kepada peserta.

Evaluasi bersifat formatif dan memakai tiga teknik: pengamatan, tanya jawab, dan pembahasan contoh kasus. Tim pengabdian mengamati peserta selama kegiatan, dengan memperhatikan kehadiran, perhatian terhadap materi, keterlibatan dalam diskusi, serta respons terhadap penjelasan contoh permasalahan keamanan digital. Hasil pengamatan dicatat untuk mengidentifikasi keterlibatan dan respons peserta.

Tanya jawab berlangsung setelah penyampaian materi pada setiap sesi, lalu berlanjut dalam diskusi terbuka. Pertanyaannya diarahkan pada pemahaman peserta tentang informasi pribadi yang perlu dilindungi, cara menjaga keamanan kata sandi dan kode OTP, serta langkah yang perlu diambil ketika menerima pesan atau tautan mencurigakan. Dari pertanyaan dan tanggapan itu, tim melihat topik yang sudah dipahami dan hal yang masih memerlukan penjelasan.

Pemateri memandu pembahasan dua contoh kasus, yaitu pesan yang meminta kode OTP atau kata sandi dan pesan yang menyertakan tautan atau berkas APK mencurigakan. Untuk tiap contoh, pemateri menjelaskan isi pesan, indikasi yang patut dicurigai, dan tindakan yang sebaiknya dilakukan. Peserta menyimak penjelasan itu dan mengikuti diskusi tentang pemeriksaan identitas pengirim, kewaspadaan terhadap permintaan data rahasia, pemeriksaan tautan

atau domain, serta verifikasi melalui saluran resmi. Peserta tidak diminta mengidentifikasi pesan secara mandiri.

Data evaluasi dianalisis secara deskriptif-kualitatif dalam tiga tahap: mengelompokkan respons berdasarkan aspek evaluasi, menelaah kesesuaian respons dengan materi yang disampaikan, lalu menarik kesimpulan tentang keterlibatan dan pemahaman peserta yang teramati. Aspek evaluasinya adalah partisipasi, pemahaman keamanan informasi, kemampuan mengenali indikasi *phishing*, dan pemahaman tentang penggunaan AI sebagai alat bantu pemeriksaan awal. Hasil analisis disajikan sebagai uraian deskriptif berdasarkan catatan pengamatan, pertanyaan, tanggapan, dan pembahasan kasus selama kegiatan.

Tabel 1. Aspek, indikator, dan teknik evaluasi

Aspek	Indikator	Teknik
Partisipasi	Kehadiran, perhatian, dan keterlibatan peserta dalam diskusi	Pengamatan
Keamanan informasi	Pertanyaan atau tanggapan mengenai data pribadi, kata sandi, dan OTP	Tanya jawab dan diskusi
Pengenalan phishing	Respons peserta ketika membahas indikasi mencurigakan dalam contoh pesan atau tautan	Pembahasan contoh kasus dan diskusi
Pemanfaatan AI	Pemahaman mengenai fungsi AI sebagai alat bantu dan perlunya verifikasi hasil	Tanya jawab dan diskusi

HASIL DAN PEMBAHASAN

Persiapan dan Pra-Survei

Persiapan diawali dengan pembagian peran di dalam tim, koordinasi dengan Ketua Karang Taruna Kelurahan Cipayung tentang tujuan, jadwal, tempat, dan peserta, lalu penyusunan materi presentasi. Pimpinan mitra menyambut baik kegiatan ini karena penipuan digital dan pengambilalihan akun media sosial pernah dialami sebagian pemuda dan warga, sedangkan edukasi formal tentang keamanan siber belum pernah diselenggarakan secara khusus di wilayah itu.

Pra-survei berupa diskusi awal dengan mitra, dan hasilnya menunjukkan bahwa peserta pernah menerima pesan atau tautan yang mencurigakan. Informasi itu menjadi dasar pemilihan contoh kasus yang dibahas selama kegiatan, yaitu pesan yang meminta kode OTP atau kata sandi serta pesan yang menyertakan tautan atau berkas APK mencurigakan. Kedua contoh dipilih karena dekat dengan pengalaman peserta dan berisiko terhadap keamanan akun maupun data pribadi.

Pelaksanaan Kegiatan

Sosialisasi berlangsung secara luring pada Sabtu, 3 Oktober 2026, di kediaman Ketua Karang Taruna Kelurahan Cipayung. Kegiatan berjalan kurang lebih dua jam dan diikuti oleh lebih dari 20 remaja anggota Karang Taruna.

Acara diawali dengan registrasi peserta, pembukaan, dan sambutan Ketua Karang Taruna, lalu dilanjutkan dengan penyampaian materi dalam empat

bagian. Materi pertama membahas keamanan informasi dan pelindungan data pribadi, termasuk jenis data yang perlu dijaga, kata sandi yang kuat, autentikasi tambahan, dan kerahasiaan kode OTP. Materi kedua mengenai ancaman digital dan ciri *phishing* melalui media sosial, pesan instan, surel, panggilan telepon, dan situs web tiruan. Materi ketiga menjelaskan langkah pencegahan, yaitu memeriksa identitas pengirim, memeriksa tautan dan nama domain, serta tidak terburu-buru menanggapi pesan yang mendesak. Materi keempat memperkenalkan AI sebagai alat bantu pemeriksaan awal terhadap pesan mencurigakan, dengan tetap menekankan verifikasi melalui sumber resmi.

Setelah materi disampaikan, pemateri menjelaskan dua contoh kasus, kemudian kegiatan dilanjutkan dengan diskusi dan tanya jawab. Contoh pertama berupa pesan yang meminta kode OTP atau kata sandi, sedangkan contoh kedua berupa pesan yang menyertakan tautan atau berkas APK mencurigakan. Peserta menyimak penjelasan tentang indikasi yang perlu diwaspadai dan mendiskusikan tindakan pencegahan yang dapat dilakukan. Kegiatan diakhiri dengan penutupan dan pembagian *slide* materi kepada peserta sebagai bahan rujukan.

Tabel 2. Alur pelaksanaan kegiatan (Sabtu, 3 Oktober 2026)

Sesi	Agenda	Luaran
1	Registrasi peserta, pembukaan oleh pembawa acara, sambutan Ketua Karang Taruna, dan pengantar dari ketua tim pengabdian	Peserta siap mengikuti kegiatan
2	Penyampaian materi keamanan informasi dan pelindungan data pribadi serta ancaman digital dan karakteristik *phishing*	Pengetahuan dasar mengenai data pribadi, risiko, dan modus penipuan digital
3	Penyampaian materi langkah pencegahan dan pemanfaatan AI sebagai alat bantu pemeriksaan awal	Pengetahuan mengenai langkah pencegahan dan penggunaan AI yang tetap memerlukan verifikasi
4	Penjelasan dan pembahasan contoh kasus permintaan OTP atau kata sandi serta tautan atau berkas APK mencurigakan, diskusi dan tanya jawab, pembagian *slide* materi, dan penutupan	Peserta memperoleh penjelasan mengenai indikasi pesan mencurigakan dan tindakan pencegahan



Gambar 1. Pelaksanaan Kegiatan PKM

Capaian terhadap Tujuan Kegiatan

a) Pemahaman keamanan informasi dan data pribadi.

Materi tentang keamanan informasi dan pelindungan data pribadi telah disampaikan kepada peserta. Selama sesi berlangsung, peserta bertanya tentang cara mengamankan data pribadi dan kata sandi. Pertanyaan itu menunjukkan

bahwa peserta memperhatikan pelindungan informasi yang mereka pakai dalam aktivitas digital sehari-hari.

Pemateri menekankan pentingnya menjaga kerahasiaan kata sandi dan kode OTP, memakai kata sandi yang kuat, serta membatasi penyebaran informasi pribadi di media sosial. Pembahasan ini berkaitan dengan temuan Kurniawan et al. (2023) tentang kesadaran keamanan data pribadi pengguna media sosial, khususnya mahasiswa dan pengguna muda. Materi itu juga dikaitkan dengan ketentuan pelindungan data pribadi di Indonesia, yaitu Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (Republik Indonesia, 2022).

b) Pemahaman risiko dan ancaman pada media digital.

Materi tentang ancaman digital disampaikan dengan menjelaskan berbagai bentuk penipuan yang dapat dijumpai di media sosial, aplikasi pesan instan, surel, dan platform digital lainnya. Peserta juga berbagi pengalaman tentang pesan atau tautan mencurigakan yang pernah mereka terima.

Berbagi pengalaman itu menjadi bagian penting dalam diskusi karena menghubungkan materi dengan situasi yang dekat dengan kehidupan peserta. Pemateri menjelaskan bahwa pengguna perlu berhati-hati terhadap pesan yang meminta informasi pribadi, menawarkan hadiah yang tidak jelas sumbernya, atau memberikan instruksi yang mendesak. Dari situ peserta memperoleh gambaran tentang risiko yang dapat muncul ketika informasi digital diterima tanpa diperiksa lebih dulu.

c) Pengenalan *phishing* dan penipuan digital

Pengenalan *phishing* dilakukan lewat penjelasan pemateri dan pembahasan dua contoh kasus, yaitu pesan yang meminta kode OTP atau kata sandi serta pesan yang menyertakan tautan atau berkas APK mencurigakan. Pemateri menjelaskan indikasi yang perlu diwaspadai dan tindakan pencegahan yang dapat dilakukan. Peserta kemudian berdiskusi tentang pentingnya menjaga kerahasiaan kode OTP, memeriksa identitas pengirim, dan memverifikasi melalui sumber resmi. Pembahasan ini menghubungkan materi dengan pengalaman peserta yang sebelumnya pernah menerima pesan atau tautan mencurigakan.

Pada sesi ini pemateri menekankan bahwa pesan penipuan dapat memanfaatkan rekayasa sosial, terutama lewat desakan waktu, ancaman, atau iming-iming imbalan. Karena itu, penerima pesan disarankan tidak terburu-buru bertindak, memeriksa identitas pengirim, memperhatikan alamat tautan atau nama domain, serta tidak memberikan kode OTP dan kata sandi kepada pihak lain. Pemeriksaan pesan juga tidak cukup bertumpu pada kesalahan ejaan atau tata bahasa, sebab AI generatif memungkinkan pesan penipuan disusun dengan bahasa yang lebih meyakinkan (Jabir et al., 2025). Hal ini sejalan dengan pembahasan Neil et al. (2023) tentang beragam isyarat yang ditemukan pada pesan *phishing* di dunia nyata.

d) Pemanfaatan AI secara bijak

Pada materi pemanfaatan AI, peserta diperkenalkan dengan kecerdasan buatan sebagai alat bantu pemeriksaan awal terhadap pesan yang mencurigakan. Pemateri menjelaskan bahwa AI dapat membantu menelaah isi pesan dan memberikan pertimbangan awal tentang kemungkinan adanya indikasi penipuan. Namun, hasil pemeriksaan AI tidak boleh dijadikan satu-satunya dasar pengambilan keputusan.

Peserta mendapat penjelasan bahwa hasil analisis AI tetap perlu diperiksa kembali lewat sumber resmi atau saluran komunikasi yang dapat dipercaya. Penekanan ini perlu karena sistem berbasis AI dapat menghasilkan kesimpulan yang kurang tepat, termasuk salah mengenali pesan yang sebenarnya aman maupun yang berbahaya (Shahbazi et al., 2025). Selain itu, pelaku kejahatan dapat memakai AI generatif untuk menyusun pesan penipuan yang lebih meyakinkan (Jabir et al., 2025). Karena itu, AI diperkenalkan sebagai alat bantu pertimbangan, sedangkan keputusan akhir tetap memerlukan pemeriksaan dan pertimbangan pengguna. Pendekatan ini sejalan dengan gagasan menggabungkan teknologi dan edukasi pengguna dalam pencegahan *phishing* (Loh et al., 2024).

Secara keseluruhan, materi yang direncanakan telah disampaikan lewat presentasi, penjelasan contoh kasus, diskusi, dan tanya jawab. Dari pengamatan selama kegiatan, peserta tampak terlibat: mereka bertanya tentang pelindungan data pribadi dan kata sandi serta berbagi pengalaman menerima pesan mencurigakan. Temuan ini hanya menggambarkan respons peserta secara deskriptif, sehingga tidak dapat dibaca sebagai bukti kuantitatif peningkatan pengetahuan atau keterampilan.

Posisi Kegiatan terhadap Pengabdian Terdahulu

Kegiatan ini sejalan dengan beberapa pengabdian terdahulu tentang keamanan informasi dan pencegahan penipuan digital. Susanti et al. (2022) serta Fajarwati dan Suhartono (2024), misalnya, menyasar Karang Taruna dengan perhatian pada keamanan data pribadi. Adapun Hidayat et al. (2025) membahas edukasi pelindungan data dan pencegahan *phishing* di lingkungan pendidikan.

Perbedaannya terletak pada tambahan materi tentang pemanfaatan AI sebagai alat bantu pemeriksaan awal terhadap pesan mencurigakan. Kegiatan ini juga dilaksanakan bersama remaja Karang Taruna di lingkungan kemasyarakatan nonformal. Perbandingan kegiatan ini dengan pengabdian terdahulu disajikan pada Tabel 3.

Tabel 3. Perbandingan kegiatan ini dengan pengabdian terdahulu

Kegiatan	**Sasaran**	**Pendekatan**	**Fokus materi**	**Perbedaan dengan kegiatan ini**
Susanti et al. (2022)	Karang Taruna Benda Baru, Pamulang	Sosialisasi	Keamanan data, OTP, dan tautan tidak jelas	Belum memuat pemanfaatan AI
Fajarwati dan Suhartono (2024)	Karang Taruna "Taruna Jaya 2", Baturraden	Pelatihan dan evaluasi melalui wawancara	Pengamanan data pribadi	Belum memuat pemanfaatan AI
Hidayat et al. (2025)	Siswa dan guru pendidikan menengah	Sesi kesadaran, lokakarya, simulasi, dan pendampingan	Perlindungan data dan pencegahan phishing	Sasaran kegiatan berada pada lingkungan pendidikan; belum memuat pemanfaatan AI
Kegiatan ini	Remaja Karang Taruna Kelurahan Cipayung	Sosialisasi, penjelasan contoh kasus, diskusi, dan tanya jawab	Keamanan informasi, phishing, penipuan digital, dan pemanfaatan AI	Memperkenalkan AI sebagai alat bantu pemeriksaan awal terhadap pesan mencurigakan

Dari perbandingan itu tampak bahwa kegiatan ini melengkapi pendekatan edukasi keamanan digital yang sudah ada dengan memperkenalkan penggunaan AI secara bijak. Materi tersebut diharapkan menambah bekal peserta dalam menghadapi pesan mencurigakan, dengan tetap mengutamakan pemeriksaan melalui sumber resmi.

SIMPULAN

Sosialisasi keamanan informasi dan pemanfaatan AI untuk mencegah *phishing* dan penipuan digital telah dilaksanakan pada 3 Oktober 2026 di kediaman Ketua Karang Taruna Kelurahan Cipayung. Kegiatan berlangsung sekitar dua jam dan diikuti lebih dari 20 remaja. Seluruh tujuan kegiatan telah dijawab melalui penyampaian materi keamanan informasi, ancaman digital dan *phishing*, langkah pencegahan, serta pemanfaatan AI sebagai alat bantu pemeriksaan awal yang hasilnya tetap perlu diverifikasi, dilengkapi penjelasan contoh kasus dan diskusi. Peserta aktif bertanya tentang pengamanan data pribadi dan kata sandi serta berbagi pengalaman menerima pesan mencurigakan. Karena evaluasi bertumpu pada pengamatan tanpa pengukuran sebelum dan sesudah kegiatan, peningkatan pengetahuan dan keterampilan peserta tidak dapat dinyatakan secara kuantitatif. Faktor pendukung kegiatan adalah kesesuaian materi dengan kebutuhan peserta, sedangkan kendalanya adalah waktu pelaksanaan yang terbatas.

Bagi mitra, disarankan memakai *slide* materi sebagai rujukan, membiasakan verifikasi sumber sebelum membuka tautan, memasang berkas, atau memberikan data, serta meneruskan pemahaman ini kepada keluarga dan

teman. Bagi tim pelaksana, disarankan menambah durasi kegiatan, menambahkan pengukuran sebelum dan sesudah kegiatan lewat kuesioner singkat atau *pre-test* dan *post-test*, menyelenggarakan sesi praktik terbimbing pemanfaatan AI untuk memeriksa pesan mencurigakan dengan tetap menekankan verifikasi, serta memperluas contoh kasus pada jenis penipuan lain yang relevan dengan aktivitas digital remaja. Untuk pengembangan berkelanjutan, disarankan pula menyusun materi lanjutan tentang pengamanan data pribadi dan kata sandi serta melaksanakan kegiatan lanjutan atau pendampingan singkat secara berkala.

DAFTAR PUSTAKA

Asosiasi Penyelenggara Jasa Internet Indonesia. (2025). *Survei penetrasi internet dan perilaku penggunaan internet tahun 2025*.

Badan Pengembangan Sumber Daya Manusia Komunikasi dan Digital. (2025). *Indeks masyarakat digital Indonesia 2025*. Kementerian Komunikasi dan Digital Republik Indonesia.

Fajarwati, S., & Suhartono, D. (2024). Pelatihan pengamanan data probadi di dunia cyber bagi anggota Karang Taruna. *J-ABDIPAMAS (Jurnal Pengabdian Kepada Masyarakat), 8*(2), 94–97.

Hidayat, W., Wahid, S. N., & Nasrullah, A. H. (2025). Enhancing students' digital security awareness through data protection and phishing prevention education in a secondary education institution. *Jurnal Sipakatau, 3*(1), 387–395. https://doi.org/10.66314/sipakatau.v3i1.264

Jabir, R., Le, J., & Nguyen, C. (2025). Phishing attacks in the age of generative artificial intelligence: A systematic review of human factors. *AI, 6*(8), Article 174. https://doi.org/10.3390/ai6080174

Kurniawan, Y., Santoso, S. I., Wibowo, R. R., Anwar, N., Bhutkar, G., & Halim, E. (2023). Analysis of higher education students' awareness in Indonesia on personal data security in social media. *Sustainability, 15*(4), Article 3814. https://doi.org/10.3390/su15043814

Loh, P. K. K., Lee, A. Z. Y., & Balachandran, V. (2024). Towards a hybrid security framework for phishing awareness education and defense. *Future Internet, 16*(3), Article 86. https://doi.org/10.3390/fi16030086

National Institute of Standards and Technology. (2026). *Cybersecurity, privacy, and AI*. U.S. Department of Commerce.

Neil, L., Dawkins, S., Jacobs, J., & Sharp, J. (2023). Peering into the phish bowl: An analysis of real-world phishing cues. In *Proceedings of the Nineteenth Symposium on Usable Privacy and Security*.

Nur'aini, R. J., & Simanjuntak, M. (2025). Phishing awareness and security concerns: Analyzing the role of anti-phishing knowledge and internet experience in online banking users. *Jurnal Ilmu Keluarga dan Konsumen, 18*(2), 121–134. https://doi.org/10.24156/jikk.2025.18.2.121

Republik Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*.

Sales, J. N., Tiongco, R., Lu, S., Ruiz, M. J., Cruz, J., & Prudente, M. (2024). Personal privacy and cyber security: Student attitudes, awareness, and perception on

the use of social media. *International Journal of Curriculum and Instruction, 16*(1), 175–190.

Schmitt, M., & Flechais, I. (2024). Digital deception: Generative artificial intelligence in social engineering and phishing. *Artificial Intelligence Review, 57*, Article 324. https://doi.org/10.1007/s10462-024-10973-2

Shahbazi, M., Jalali, S. M. J., & Molaeevand, M. (2025). AI-based phishing detection and student cybersecurity awareness in the digital age. *Big Data and Cognitive Computing, 9*(8), Article 210. https://doi.org/10.3390/bdcc9080210

Susanti, et al. (2023). Sosialisasi pentingnya cyber security guna mengurangi risiko tingkat pencurian data yang berimbas pada tindak penipuan kepada para Karang Taruna Benda Baru Pamulang. *JAMAIKA: Jurnal Abdi Masyarakat Universitas Pamulang, 3*(2), 207–214.