

Transformasi Kesadaran Digital Di Era Artificial Intelligence Sebagai Upaya Pencegahan Social Engineering Di Media Sosial Seperti Whatsapp Dan Facebook Bagi Siswa Paket C Pada Pkbn Bina Insan Kamil

¹Christien Rozali, ²Samso Supriyatna, ³Syifaurachman

Program Studi Sistem Informasi, Fakultas Ilmu Komputer

Universitas Pamulang, Kota Tangerang Selatan, Indonesia

¹dosen02828@unpam.ac.id , ²dosen2830@unpam.ac.id, ³dosen03181@unpam.ac.id

Abstract

The advancement of digital technology and the growing popularity of social media pose substantial problems to cybersecurity, particularly for those with low digital literacy. One subject of developing concern is social engineering, a technique for manipulating mental information in order to access sensitive data via digital media. PKBM Bina Insan Kamil, a non-formal educational institution, has pupils who are exposed to digital fraud because they lack cybersecurity skills. This Community Service activity seeks to increase digital literacy, foster a knowledge of social engineering, and provide students with practical methods for securing social media accounts. Outreach, simulations, and direct mentoring are among the approaches employed, along with an explanation of the significance of artificial intelligence in modern cybercrime patterns. Pre- and post-tests, as well as participant satisfaction surveys, are used in the evaluation. This initiative is aimed to raise awareness of digital security and foster change within the PKBM ecosystem.

Keywords: artificial intelligence; social engineering; cybersecurity;

Abstrak

Kemajuan teknologi digital dan meningkatnya popularitas media sosial menimbulkan masalah besar bagi keamanan siber, terutama bagi mereka yang memiliki literasi digital rendah. Salah satu masalah yang semakin mendapat perhatian adalah rekayasa sosial, yaitu teknik untuk memanipulasi informasi mental guna mengakses data sensitif melalui media digital. PKBM Bina Insan Kamil, sebuah lembaga pendidikan non-formal, memiliki peserta didik yang terpapar pada penipuan digital karena kurangnya keterampilan dalam keamanan siber. Kegiatan Pengabdian Masyarakat ini bertujuan untuk meningkatkan literasi digital, memperkenalkan pemahaman tentang rekayasa sosial, dan memberikan metode praktis kepada siswa untuk mengamankan akun media sosial mereka. Pendekatan yang digunakan meliputi penyuluhan, simulasi, dan pendampingan langsung, serta penjelasan tentang pentingnya kecerdasan buatan dalam pola kejahatan siber modern. Evaluasi dilakukan melalui pre-test dan post-test, serta survei kepuasan peserta. Inisiatif ini bertujuan untuk meningkatkan kesadaran tentang keamanan digital dan mendorong perubahan dalam ekosistem PKBM.

Kata kunci: kecerdasan buatan; rekayasa sosial; keamanan siber;

PENDAHULUAN

Perkembangan teknologi informasi telah merevolusi cara manusia dalam berinteraksi, bekerja, belajar, dan memperoleh informasi. Menurut laporan APJII (2023), jumlah pengguna internet di Indonesia telah melampaui 215 juta orang, yang

setara dengan sekitar 78% dari total populasi. Besarnya penetrasi internet ini mendorong terjadinya peningkatan interaksi masyarakat di platform digital seperti WhatsApp, Facebook, dan media sosial lainnya. Namun, tingginya penggunaan teknologi digital belum sepenuhnya diimbangi dengan tingkat literasi digital yang memadai, terutama di kalangan masyarakat yang berada dalam pendidikan nonformal. Keadaan ini membuat mereka lebih rentan terhadap kejahatan digital, termasuk serangan *social engineering*.

Social engineering merupakan pendekatan manipulatif yang mengeksploitasi kelemahan manusia untuk mendapatkan akses informasi atau memicu tindakan tertentu tanpa disadari oleh korban. Serangan ini memanfaatkan psikologi melalui rekayasa pesan, narasi darurat, atau penipuan berbasis identitas, sehingga seringkali lebih efektif dibandingkan serangan teknis biasa. Allahyari dan Zarrabi (2021) menjelaskan bahwa *social engineering* adalah ancaman strategis dalam keamanan siber karena serangan ini memanfaatkan manusia sebagai titik lemah utama dalam sistem digital. Dalam hal ini, Saini (2022) mencatat bahwa jenis serangan ini terus berkembang dengan teknik-teknik baru yang semakin sulit dikenali oleh pengguna awam.

Kemajuan teknologi Kecerdasan Buatan (AI) juga menambah kompleksitas ancaman *social engineering*. AI saat ini mampu menciptakan konten palsu yang sangat meyakinkan, mulai dari pesan teks yang realistis hingga suara imitasi (*voice cloning*), gambar yang dimanipulasi, sampai video deepfake (O'Boyle, 2020). Pelaku kejahatan digital dapat memanfaatkan algoritma AI untuk merancang skenario penipuan yang lebih canggih, meniru gaya komunikasi seseorang, atau menargetkan korban dengan cara yang lebih personal. Coughlin dan Coughlin (2019) menyatakan bahwa perkembangan teknik *social engineering* berbasis AI meningkatkan efektivitas serangan dan memperluas target korban hingga ke kelompok dengan literasi digital yang rendah.

Fenomena ini menjadi perhatian penting bagi lembaga pendidikan nonformal seperti PKBM Bina Insan Kamil, yang tidak hanya berfungsi sebagai penyedia layanan pendidikan, tetapi juga berperan dalam membekali masyarakat dengan keterampilan digital yang aman. Peserta didik Paket C datang dari beragam latar belakang sosial, ekonomi, dan usia, banyak di antara mereka yang belum memiliki pemahaman mendalam tentang keamanan digital. Observasi awal oleh tim PKM menunjukkan bahwa sebagian besar siswa PKBM tidak mampu membedakan pesan penipuan, belum memahami fungsi keamanan dasar seperti autentikasi dua faktor (2-FA), dan sering kali membagikan data pribadi dengan sembarangan. Ini menguatkan argumen bahwa kelompok rentan membutuhkan intervensi pendidikan digital yang tepat.

Usaha peningkatan literasi digital di kalangan masyarakat pendidikan nonformal sangat relevan dengan tuntutan era Digital 5.0, di mana kemampuan untuk beradaptasi dengan perubahan teknologi menjadi kebutuhan penting bagi seluruh lapisan masyarakat. Anas dan Zakir (2024) menekankan bahwa kemajuan AI tidak hanya membawa tantangan, tetapi juga peluang untuk pembelajaran jika digunakan secara bijak. Namun, tanpa pemahaman yang tepat, AI berpotensi menjadi alat manipulatif yang berbahaya. Oleh karena itu, pelatihan literasi digital dalam konteks

keamanan siber sangat diperlukan agar peserta didik dapat memahami risiko serta mengelola teknologi dengan aman dan produktif.

Program Pengabdian kepada Masyarakat ini dirancang sebagai intervensi strategis untuk memenuhi kebutuhan tersebut. Melalui pendekatan penyuluhan, simulasi kasus *social engineering*, serta pendampingan praktik keamanan digital, diharapkan peserta didik dapat meningkatkan pengetahuan dan keterampilan yang nyata. Kegiatan ini juga mengikuti prinsip pemberdayaan masyarakat sesuai amanat UU Sistem Pendidikan Nasional (Kemdikbud, 2003), yang mengharuskan pihak-pihak terkait untuk membekali warga belajar dengan kecakapan hidup yang relevan dengan perkembangan zaman. Berbagai penelitian PKM lainnya menunjukkan bahwa kegiatan yang berbasis praktik dan teknologi secara signifikan meningkatkan kompetensi digital masyarakat (Rozali et al., 2024; Sunardi & Rozali, 2025), sehingga pendekatan serupa diterapkan dalam program ini.

Dengan demikian, kegiatan PKM terkait pencegahan *social engineering* dan ancaman AI di PKBM Bina Insan Kamil tidak hanya memberikan pengetahuan konseptual, tetapi juga keterampilan praktis yang diperlukan oleh peserta didik untuk menghadapi risiko kejahatan digital yang semakin kompleks. Pelatihan ini diharapkan mampu mengurangi kerentanan masyarakat pendidikan nonformal terhadap penipuan digital sekaligus mendorong terciptanya budaya aman dalam pemanfaatan teknologi.

METODE

Metode pelaksanaan program terdiri dari empat tahap utama sebagaimana pada Gambar 1, yaitu: (1) persiapan dan perencanaan, (2) pelaksanaan kegiatan, (3) monitoring dan evaluasi, serta (4) tindak lanjut. Tahap persiapan dimulai dengan analisis kebutuhan yang diperoleh melalui observasi di lapangan dan wawancara dengan pengelola PKBM Bina Insan Kamil. Analisis ini bertujuan untuk mengidentifikasi tingkat literasi digital peserta, pemahaman mereka terhadap ancaman *social engineering*, serta platform digital yang paling sering mereka gunakan dalam aktivitas sehari-hari. Hasil identifikasi menunjukkan bahwa peserta memiliki pemahaman yang masih terbatas mengenai isu-isu keamanan digital, sehingga intervensi edukatif yang terstruktur dan aplikatif sangat diperlukan.



Gambar 1. Metode Pengembangan Pelaksanaan

Berdasarkan penemuan tersebut, tim pelaksana menyusun materi pelatihan dalam format slide, infografis, video edukasi, dan modul praktis. Materi tersebut mencakup hal-hal utama yang meliputi pengenalan konsep social engineering, identifikasi pola manipulasi digital, pemahaman terhadap ancaman yang terkait dengan Artificial Intelligence (AI), serta langkah-langkah perlindungan akun digital seperti penerapan Two-Factor Authentication (2FA), pengelolaan kata sandi, dan pengaturan privasi di media sosial. Selanjutnya, instrumen evaluasi di desain dalam bentuk pre-test, post-test, lembar observasi, dan kuesioner kepuasan peserta untuk secara komprehensif mengukur efektivitas pelatihan melalui pendekatan kuantitatif dan kualitatif. Proses persiapan dan perencanaan secara teknis meliputi hal berikut:

1. Tahap Persiapan dan Perencanaan

Tahap ini dilakukan untuk memastikan kegiatan tepat sasaran, terdiri atas proses kerja sebagai berikut:

a. Identifikasi Kebutuhan Mitra

Tim PKM melakukan observasi dan wawancara dengan pengelola PKBM untuk memahami kondisi literasi digital peserta, tingkat risiko terhadap social engineering, dan pemahaman terkait AI dalam kejahatan siber.

b. Penyusunan Modul Pelatihan

Modul pelatihan disusun dalam bentuk slide, infografis, dan booklet yang mencakup, konsep dasar literasi digital, jenis-jenis social engineering, Dampak negatif penggunaan AI dalam serangan digital maupun serangan siber, studi kasus penipuan aktual, langkah praktis keamanan akun (2FA, password management, privasi media sosial).

c. Penyusunan Instrumen Evaluasi

Instrumen *pre-test*, *post-test*, dan kuesioner kepuasan disiapkan untuk mengukur efektivitas program.

2. Tahap Pelaksanaan

Pelaksanaan kegiatan dilakukan melalui tiga sesi inti. Pertama, pengenalan *social engineering* dengan membahas konsep dasar, pola serangan, contoh kasus viral, dan diskusi pengalaman peserta. Kedua, pembahasan ancaman AI dalam kejahatan siber yakni menjelaskan bagaimana AI digunakan dalam *deepfake*, *voice cloning*, dan pesan otomatis. Peserta dilatih mengidentifikasi pesan mencurigakan melalui simulasi. Ketiga, praktik keamanan digital berfokus pada praktik langsung yakni aktivasi 2FA, pengaturan privasi whatsapp, facebook, dan akun google, manajemen kata sandi verifikasi identitas digital. Pendampingan dilakukan secara individual untuk memastikan semua peserta berhasil.

3. Tahap Monitoring dan Evaluasi

Kegiatan evaluasi dilaksanakan dengan menggunakan pendekatan kuantitatif dan kualitatif guna mendapatkan pemahaman yang menyeluruh mengenai efektivitas program. Evaluasi kuantitatif dilakukan melalui pemberian pre-test dan post-test kepada seluruh peserta. Alat ukur ini bertujuan untuk menilai peningkatan pengetahuan peserta mengenai rekayasa sosial, ancaman berbasis Kecerdasan Buatan, serta praktik keamanan digital setelah mengikuti rangkaian sesi pelatihan. Perbandingan antara skor pre-test dan post-test memungkinkan tim pelaksana untuk menilai perubahan tingkat pemahaman secara objektif.

Selanjutnya, evaluasi kualitatif dilaksanakan dengan mengumpulkan umpan balik dari peserta melalui diskusi terbuka dan wawancara informal. Dengan pendekatan ini, peserta dapat berbagi pengalaman, tantangan, serta aspek materi yang dianggap paling bermanfaat. Informasi kualitatif tersebut memberikan wawasan yang lebih mendalam mengenai pandangan peserta dan efektivitas metode penyampaian materi.

Selain itu, dokumentasi kegiatan dilakukan secara sistematis, mencakup pengambilan foto, pencatatan daftar hadir, serta pembuatan catatan lapangan. Dokumentasi ini tidak hanya berfungsi sebagai bukti pelaksanaan kegiatan, tetapi juga menjadi sumber pendukung dalam proses penyusunan laporan akhir dan publikasi jurnal ilmiah.

4. Tahap Tindak Lanjut

Tindak lanjut kegiatan dirancang untuk memastikan keberlanjutan dampak program dan memperkuat literasi digital peserta setelah pelatihan selesai. Langkah pertama yang dilakukan adalah memberikan pendampingan lanjutan terkait literasi digital, sehingga peserta tetap memperoleh bimbingan apabila menghadapi kendala dalam menerapkan praktik keamanan digital sehari-hari. Selain itu, tim juga menyediakan modul tambahan berupa panduan anti-hoaks dan materi edukasi digital lainnya yang dapat digunakan secara mandiri oleh peserta maupun pengelola PKBM. Upaya tindak lanjut ini diperkuat dengan membuka potensi kerja sama jangka panjang dengan PKBM Bina Insan Kamil, sehingga program edukasi keamanan digital dapat terus dikembangkan dan diperluas untuk mendukung peningkatan kompetensi masyarakat secara berkelanjutan.

HASIL DAN PEMBAHASAN

Pelaksanaan kegiatan Pengabdian kepada Masyarakat di PKBM Bina Insan Kamil berjalan dengan lancar dan mendapatkan respons positif dari seluruh peserta. Para

peserta, yang merupakan siswa Paket C dengan latar belakang pendidikan yang beragam, mengikuti kegiatan dengan penuh antusias. Hal ini terlihat dari keterlibatan aktif mereka dalam diskusi, tanya jawab, hingga simulasi keamanan digital.

Pada sesi pemaparan materi, peserta diperkenalkan pada berbagai teknik social engineering seperti *phishing*, *impersonation*, *scare tactics*, dan penipuan berbasis media sosial. Contoh-contoh kasus nyata dari *WhatsApp*, *Facebook*, serta *marketplace* memberikan pemahaman konkret mengenai pola serangan yang sering terjadi di sekitar mereka. Selain itu, peserta juga diperkenalkan pada ancaman berbasis *Artificial Intelligence* (AI) seperti *deepfake* dan *voice cloning*, yang memberikan wawasan baru dan meningkatkan kesadaran mereka terhadap risiko manipulasi digital modern.

Pada sesi praktik, peserta dibimbing langsung untuk melakukan langkah-langkah keamanan digital, seperti mengaktifkan *Two-Factor Authentication* (2FA), membuat kata sandi yang kuat, serta mengatur privasi akun media sosial. Pendampingan teknis diberikan secara individual, sehingga peserta dapat menyelesaikan seluruh langkah pengamanan meskipun memiliki tingkat kemampuan digital yang berbeda-beda.

Selain itu dalam tahapan evaluasi pelaksanaan kegiatan yang dilakukan melalui metode pre-test dan post-test untuk mengukur peningkatan pengetahuan peserta setelah mengikuti kegiatan sebagaimana dijelaskan pada Tabel 1.

Tabel 1. Hasil Pengukuran melalui metode Pre-test dan Post-Test

Aspek Penilaian	Pre-test	Post-test	Peningkatan
<i>Social Engineering</i>	45.3	86.7	+41.4
Ancaman AI (<i>deepfake</i> , <i>voice cloning</i>)	38.5	82.1	+43.6
Identifikasi Penipuan	42.7	88.4	+45.7
Keamanan Digital (2FA, <i>password</i> , privasi)	40.9	90.3	+49.4
Rata-rata keseluruhan	41.8	86.9	+45.1

Peningkatan sebesar 45,1 poin secara keseluruhan menunjukkan bahwa kegiatan PKM berhasil meningkatkan pemahaman peserta terhadap ancaman digital dan tindakan pencegahannya. Peningkatan tertinggi terdapat pada kemampuan menerapkan langkah keamanan digital, disusul kemampuan mengidentifikasi pesan penipuan.

Temuan ini konsisten dengan penelitian Allahyari & Zarrabi (2021), Saini (2022), serta Coughlin & Coughlin (2019) yang menekankan bahwa edukasi langsung, simulasi, dan studi kasus merupakan metode yang efektif untuk meningkatkan kesadaran keamanan digital.

Peserta menyatakan bahwa kegiatan ini sangat bermanfaat dan memberikan keterampilan yang dapat langsung diterapkan dalam kehidupan sehari-hari. Peserta memberikan saran yakni agar durasi kegiatan diperpanjang agar materi praktik bisa dijalankan dengan lebih mendalam. Hal ini tercermin dari hasil pengukuran peserta dalam pengalaman dan kepuasan terhadap pelaksanaan kegiatan yang disajikan pada Tabel 2.

Tabel 2. Hasil Kuesioner Kepuasan Peserta

Indikator Penilaian	Skala (1-	Kategori
---------------------	-----------	----------

5)		
Kejelasan penyampaian materi	4.8	Sangat Baik
Relevansi materi	4.9	Sangat Baik
Interaktivitas	4.6	Baik
Manfaat simulasi	4.9	Sangat Baik
Manfaat praktik keamanan digital	5.0	Sangat Baik
Sikap narasumber	4.9	Sangat Baik
Efektivitas waktu	4.5	Baik
Kepuasan keseluruhan	4.8	Sangat Baik

Kegiatan ini terbukti efektif dalam meningkatkan literasi digital peserta, sebagaimana terlihat dari peningkatan nilai tes serta tingginya tingkat kepuasan terhadap seluruh rangkaian pelatihan. Efektivitas ini dapat dilihat dari beberapa aspek penting yang muncul selama pelaksanaan. Pertama, pemanfaatan contoh kasus nyata terbukti sangat membantu peserta dalam memahami pola dan mekanisme serangan digital. Pendekatan berbasis konteks ini membuat peserta mampu mengaitkan materi dengan pengalaman sehari-hari, sehingga sesuai dengan temuan Allahyari dan Zarrabi (2021) serta Saini (2022) yang menyatakan bahwa pembelajaran berbasis kasus nyata meningkatkan kemampuan deteksi dini terhadap ancaman *social engineering*.



Gambar 2 Foto dan Materi Kegiatan Pelaksanaan

Selain itu, penyampaian materi mengenai ancaman berbasis *Artificial Intelligence* (AI), terutama terkait *deepfake* dan *voice cloning*, memberikan wawasan baru bagi peserta. Informasi tersebut membuka pemahaman bahwa ancaman digital kini tidak lagi terbatas pada modus tradisional, tetapi telah berkembang mengikuti kemajuan teknologi. Oleh karena itu, kegiatan ini menunjukkan pentingnya edukasi digital yang berkelanjutan agar masyarakat tetap mampu beradaptasi dengan tantangan keamanan modern.

Aspek lain yang memberikan kontribusi besar terhadap keberhasilan kegiatan adalah pembelajaran berbasis praktik. Melalui sesi praktik keamanan digital, peserta mendapatkan pengalaman langsung dalam menerapkan langkah perlindungan akun, seperti pengaturan privasi dan aktivasi Two-Factor Authentication (2FA). Temuan ini sejalan dengan penelitian Rozali et al. (2024) dan Sunardi dan Rozali (2025) yang menekankan bahwa pembelajaran berbasis praktik memiliki dampak signifikan dalam meningkatkan keterampilan digital masyarakat.

Lebih jauh lagi, kegiatan ini menghasilkan perubahan perilaku digital yang nyata. Peserta menjadi lebih berhati-hati saat menerima pesan dari pihak yang tidak dikenal, tidak lagi membagikan kode OTP, mampu mengenali tanda-tanda penipuan digital, dan lebih sadar dalam menjaga privasi akun media sosial mereka. Perubahan perilaku ini menunjukkan bahwa kombinasi penyuluhan, diskusi, simulasi, dan praktik langsung merupakan metode yang efektif dalam meningkatkan kesadaran sekaligus kemampuan peserta dalam menjaga keamanan digital.

KESIMPULAN

Kegiatan Pengabdian kepada Masyarakat yang dilaksanakan di PKBM Bina Insan Kamil berhasil mencapai tujuan utamanya, yaitu meningkatkan literasi digital peserta terkait ancaman social engineering dan praktik keamanan digital. Melalui penyuluhan, simulasi, dan praktik langsung, peserta memperoleh pemahaman yang lebih mendalam mengenai bentuk-bentuk penipuan digital yang umum terjadi serta cara mengantisipasinya. Peningkatan signifikan pada nilai post-test dibandingkan pre-test menunjukkan adanya perkembangan pengetahuan yang kuat, sementara hasil kuesioner kepuasan peserta menegaskan bahwa metode pelatihan yang digunakan efektif, aplikatif, dan relevan dengan kebutuhan mereka.

Selain peningkatan pengetahuan, kegiatan ini juga menghasilkan perubahan perilaku digital yang positif. Peserta menjadi lebih berhati-hati dalam menerima pesan dari nomor tidak dikenal, tidak membagikan kode OTP, serta lebih mampu mengenali ciri-ciri pesan dan tautan mencurigakan. Penerapan langkah-langkah keamanan digital seperti *Two-Factor Authentication* (2FA), pengaturan privasi akun, dan penggunaan kata sandi yang kuat menunjukkan bahwa peserta tidak hanya memahami konsep, tetapi juga mampu mengimplementasikannya dalam kehidupan sehari-hari.

Secara keseluruhan, kegiatan PKM ini memberikan dampak nyata dalam meningkatkan kesadaran dan kemampuan peserta dalam menjaga keamanan digital mereka. Keberhasilan ini menunjukkan bahwa pendekatan edukasi berbasis kasus nyata, diskusi interaktif, dan praktik langsung mampu memperkuat pemahaman sekaligus membentuk kebiasaan digital yang lebih aman. Untuk keberlanjutan

program, pendampingan lanjutan dan penyediaan modul tambahan sangat dianjurkan sebagai upaya memperkuat literasi digital peserta secara berkelanjutan.

Acknowledge

Pelaksanaan kegiatan ini dibiayai oleh Lembaga Penelitian dan Pengabdian kepada Masyarakat Universitas Pamulang Tahun 2025.

REFERENSI

- Allahyari, H., & Zarrabi, M. (2021). *The impact of social engineering on cybersecurity: A systematic review*. Journal of Cybersecurity and Information Management, 1–15.
- Anas, I., & Zakir, S. (2024). *Artificial intelligence: Solusi pembelajaran era digital 5.0*. Jurnal Sains Komputer & Informatika (J-SAKTI), 35–46.
- APJII. (2023). *Laporan survei pengguna internet Indonesia 2023*. Asosiasi Penyelenggara Jasa Internet Indonesia.
- Coughlin, T., & Coughlin, D. (2019). *The evolving threat of social engineering: Tactics, techniques, and countermeasures*. Cybersecurity Journal, 55–68.
- Kementerian Pendidikan dan Kebudayaan. (2003). *Undang-Undang Republik Indonesia Nomor 20 Tahun 2003 tentang Sistem Pendidikan Nasional*. https://jdih.kemdikbud.go.id/sjdih/siperpu/dokumen/salinan/UU_tahun2003_nomor020.pdf
- O'Boyle, M. J. (2020). *Understanding the threat of AI-driven social engineering*. SANS Institute Information Security Reading Room.
- Rozali, C., Supriyatna, S., Karimah, M., Chaniago, M. A., Gulo, E., Putra, R., ... Waruwu, S. (2024). *Workshop UI/UX desain aplikasi berbasis web menggunakan software Figma pada SMK IT Bina Adzkia*. APPA: Jurnal Pengabdian kepada Masyarakat, 178–183.
- Saini, R. S. (2022). *A review on social engineering attacks and their prevention techniques*. International Journal of Computer Science and Engineering, 20–25.
- Sunardi, D., & Rozali, C. (2025). *Pelatihan visualisasi data kependudukan menggunakan Looker Studio pada Kelurahan Duren Seribu*. JIPM: Jurnal Inovasi Pengabdian Masyarakat, 59–63.