

Artikel Pengabdian kepada Masyarakat

Peningkatan Kapasitas UMKM Kabupaten Cilacap Melalui Kecerdasan Buatan dan Keamanan Transaksi Digital

Bella Adinda Putri*, Linda Perdana Wanti, Satriawan Desmana, Krisna Nuresa Qodri, Ratih, Abdul Rohman Supriyono, Muhammad Nur Faiz, Oman Somantri, Ratih HafSarah Maharrani

Program Studi Rekayasa Keamanan Siber, Politeknik Negeri Cilacap, Cilacap, Indonesia

INFORMASI ARTIKEL

Diterima Redaksi: 02 Juni 2026
Revisi Akhir: 01 Juli 2026
Diterbitkan Online: 02 Juli 2026

KATA KUNCI

Keamanan Siber
Keamanan Transaksi Digital
Kecerdasan Buatan
Literasi Digital
UMKM

KORESPONDENSI (*)

E-mail: belladinda@pnc.ac.id

A B S T R A K

UMKM di era digital menghadapi tantangan karena kurangnya pemahaman tentang literasi digital dan kesadaran akan ancaman siber. Kegiatan ini bertujuan untuk meningkatkan pemahaman pelaku UMKM—yang didukung oleh BAZNAS Kabupaten Cilacap—dalam memanfaatkan teknologi AI dan aplikasi keamanan digital. Metode pelaksanaannya menggunakan pelatihan praktik langsung, diskusi interaktif, dan pendampingan langsung melalui dua tahap: (1) pengenalan konsep AI untuk keamanan transaksi digital; dan (2) pelatihan tentang aplikasi pendukung keamanan digital (GetContact, Kredibel, dan VirusTotal). Kegiatan ini melibatkan 100 pelaku UMKM dari berbagai sektor usaha. Evaluasi yang dilakukan melalui pre-test dan post-test menggunakan 10 pertanyaan terkait materi pelatihan menunjukkan peningkatan yang signifikan dengan rata-rata skor peserta meningkat dari 78,09 (pre-test) menjadi 97,50 (post-test), yang menggambarkan peningkatan sebesar 19,41 poin atau 28,98%. Hal ini menunjukkan bahwa pelatihan tersebut efektif meningkatkan literasi keamanan digital dan memberdayakan pelaku UMKM untuk melindungi bisnis mereka dari ancaman kejahatan siber dan penipuan online.

PENDAHULUAN

Revolusi Industri 4.0 yang ditandai oleh kemajuan teknologi digital seperti kecerdasan buatan (*Artificial Intelligence/AI*), *Internet of Things (IoT)*, *big data*, dan otomatisasi telah membawa dampak signifikan pada sektor ekonomi khususnya Usaha Mikro, Kecil, dan Menengah (UMKM). Pelaku UMKM dihadapkan pada peluang besar untuk mengembangkan usaha melalui digitalisasi, namun juga menghadapi tantangan berupa rendahnya literasi teknologi dan keamanan transaksi (Schwab, 2016).

Transformasi digital UMKM telah menjadi fokus penelitian dalam dekade terakhir. Mikalef dkk. (Mikalef dkk., 2021) dalam penelitiannya menegaskan bahwa AI telah berkembang menjadi enabler penting dalam bisnis B2B, memungkinkan pemasaran berbasis data, analisis perilaku konsumen, hingga deteksi penipuan dalam transaksi keuangan. Rahayu dan Day (Rahayu & Day, 2022)(Lestari, 2021) menunjukkan bahwa UMKM yang mengadopsi teknologi digital, termasuk AI, mampu meningkatkan efisiensi operasional hingga 25% dan lebih siap menghadapi tantangan ekonomi. Studi tersebut menekankan pentingnya inovasi teknologi dan keunggulan kompetitif dalam strategi transformasi digital UMKM. Namun, transformasi digital tidak terlepas dari tantangan serius dalam aspek keamanan transaksi online. Arora dkk. (Arora dkk., 2021) mengembangkan kerangka keamanan siber berbasis AI untuk UKM dan mengidentifikasi bahwa pemanfaatan AI dalam keamanan memiliki empat kelebihan utama: (1) mampu mendeteksi anomali transaksi dengan cepat; (2) mengurangi potensi kerugian akibat penipuan online; (3) meningkatkan kepercayaan konsumen; dan (4) memperluas peluang usaha melalui strategi digital yang aman.

Hasil penelitian Utami dan Wibowo (Utami & Wibowo, 2021) menunjukkan bahwa sebagian besar UMKM di Indonesia masih memiliki tingkat literasi digital yang rendah dan belum memahami pentingnya perlindungan data serta keamanan siber. Kondisi ini mengakibatkan tingginya risiko penipuan daring, pencurian data pribadi, hingga kerugian finansial akibat lemahnya sistem keamanan digital. Nugroho dan Pramudiana (Nugroho & Pramudiana, 2020)(Mahardika dkk., 2025) juga menegaskan bahwa rendahnya kesadaran terhadap keamanan transaksi menjadi salah satu penyebab utama menurunnya kepercayaan konsumen dalam bertransaksi secara online. Penelitian terbaru Musytari (Musytari, 2025)(Nugroho dkk., 2025) memperkuat temuan tersebut dengan menyebutkan bahwa ketahanan digital UMKM tidak hanya bergantung pada teknologi yang digunakan, tetapi juga pada literasi keamanan siber, manajemen keuangan digital, serta kemampuan mendeteksi ancaman menggunakan teknologi cerdas seperti AI. Dwivedi dkk. (Dwivedi dkk., 2023)(Jayusman & Mahardika, 2024) dalam kajiannya tentang Generative AI menegaskan bahwa platform seperti ChatGPT dapat membantu pelaku UMKM tidak hanya dalam pembuatan konten pemasaran digital, tetapi juga dalam analisis data keamanan dan deteksi pola transaksi mencurigakan.

Dalam konteks pemberdayaan ekonomi umat, Huda dkk. (Huda dkk., 2020)(Ripai dkk., 2025) menekankan bahwa integrasi zakat produktif dan teknologi digital dapat memperkuat ketahanan ekonomi masyarakat kecil sekaligus memperluas akses mereka terhadap ekosistem bisnis yang lebih modern dan aman. Studi Kurniawan dan Lestari (Kurniawan & Lestari, 2022) menunjukkan bahwa pelatihan berbasis praktik langsung (*hands-on training*) yang dibarengi dengan pendampingan memberikan dampak signifikan dibandingkan pelatihan satu arah atau hanya teoritis, terutama dalam konteks adopsi teknologi digital oleh UMKM.

Kabupaten Cilacap merupakan kabupaten terluas di Provinsi Jawa Tengah dengan luas wilayah 225.360 ha yang terbagi menjadi 24 kecamatan dan 269 desa/kelurahan. Secara geografis, Cilacap memiliki posisi strategis di pesisir selatan Jawa dengan akses maritim yang memadai, yang mendukung aktivitas ekonomi dan perdagangan. Untuk potensi fisik, Cilacap memiliki infrastruktur yang relatif memadai dengan keberadaan pelabuhan, jalur transportasi darat yang menghubungkan kota-kota besar di Jawa, serta akses telekomunikasi dan internet yang semakin baik. Keberadaan Politeknik Negeri Cilacap sebagai institusi pendidikan vokasi memberikan dukungan dalam pengembangan sumber daya manusia, khususnya dalam bidang teknologi informasi dan keamanan siber. Sedangkan, untuk potensi sosial, masyarakat Cilacap dikenal memiliki jiwa kewirausahaan yang kuat, dengan banyaknya pelaku UMKM di berbagai sektor. Keberadaan BAZNAS Kabupaten Cilacap sebagai lembaga pengelola zakat berperan penting dalam pemberdayaan ekonomi masyarakat melalui program pendampingan dan pembiayaan UMKM binaan. Program pembinaan BAZNAS mencakup berbagai sektor usaha seperti kuliner, fashion, kerajinan, dan jasa, yang sebagian besar merupakan mustahik yang diberdayakan menjadi pelaku usaha mandiri. Dalam segi potensi ekonomi, UMKM di Kabupaten Cilacap berkontribusi signifikan terhadap pertumbuhan ekonomi daerah. Dengan semakin berkembangnya ekosistem digital, banyak pelaku UMKM mulai memanfaatkan platform *e-commerce* dan media sosial untuk memasarkan produk. Namun, peningkatan transaksi digital juga membawa risiko keamanan yang perlu diantisipasi. Potensi pasar lokal yang luas, produk unggulan daerah (hasil laut, batik, makanan olahan), serta dukungan dari berbagai lembaga menjadi modal kuat untuk pengembangan UMKM yang berbasis teknologi dan aman secara digital.

Berdasarkan hasil survei dan diskusi dengan BAZNAS Kabupaten Cilacap serta perwakilan UMKM binaan pada September 2024, teridentifikasi beberapa permasalahan konkrit yang dihadapi pelaku UMKM: (1) Kurangnya pemahaman mengenai konsep dasar AI dalam keamanan transaksi digital: Sebagian besar pelaku UMKM binaan BAZNAS (sekitar 85%) belum memahami konsep kecerdasan artifisial (AI), baik dari sisi definisi, manfaat, maupun penerapannya untuk mendukung keamanan transaksi. Mereka belum mengetahui bagaimana AI dapat membantu menganalisis risiko penipuan online, *phishing*, atau tautan mencurigakan yang berpotensi merugikan usaha; (2) Belum optimalnya pemanfaatan platform AI untuk mendeteksi ancaman digital: Pelaku UMKM masih terbatas dalam keterampilan menggunakan platform berbasis AI untuk membaca dan memahami hasil analisis keamanan. Padahal, penggunaan Generative AI (seperti ChatGPT, Gemini, atau DeepSeek) dapat membantu menjelaskan informasi teknis dari platform analisis keamanan digital agar lebih mudah dipahami dan diterapkan dalam praktik usaha sehari-hari; (3) Rendahnya literasi penggunaan aplikasi pendukung keamanan transaksi digital: Sebagian besar UMKM binaan BAZNAS (lebih dari 90%) belum familiar dengan aplikasi pendukung yang dapat membantu melindungi transaksi digital, seperti GetContact untuk memverifikasi nomor telepon, Kredibel untuk mengecek nomor rekening, maupun VirusTotal untuk mendeteksi potensi bahaya dari URL atau file. Minimnya literasi ini berdampak pada lemahnya strategi perlindungan transaksi digital dan berisiko menurunkan kepercayaan konsumen dalam bertransaksi secara daring.

Berdasarkan permasalahan yang telah diidentifikasi, kegiatan pengabdian kepada masyarakat ini memiliki tujuan sebagai berikut: (1) Memberikan pengenalan konsep dasar AI yang relevan dengan keamanan transaksi digital bagi pelaku UMKM binaan BAZNAS Kabupaten Cilacap, sehingga mereka memahami peran dan manfaat AI dalam melindungi usaha dari ancaman siber; (2) Melatih pelaku UMKM dalam memanfaatkan teknologi AI, khususnya platform Generative AI (ChatGPT, Gemini, DeepSeek), untuk mendeteksi, mencegah, dan meminimalkan risiko ancaman kejahatan siber pada transaksi digital melalui analisis pesan, tautan, dan pola komunikasi mencurigakan; (3) Memberikan pelatihan keterampilan teknis penggunaan aplikasi pendukung keamanan digital seperti GetContact (verifikasi nomor telepon), Kredibel (pengecekan rekening), dan VirusTotal (deteksi file/URL berbahaya) untuk melindungi usaha dari penipuan online serta meningkatkan kepercayaan konsumen dalam bertransaksi.

ANALISIS SITUASI

Permasalahan literasi digital masih menjadi tantangan utama bagi sebagian besar UMKM di Indonesia. Penelitian Utami dan Wibowo (2021) menunjukkan bahwa pelaku UMKM umumnya masih berfokus pada aspek produksi dan pemasaran, sementara pemahaman mengenai keamanan data, perlindungan identitas digital, dan mitigasi risiko transaksi online masih relatif rendah. Kondisi tersebut menyebabkan UMKM menjadi kelompok yang rentan terhadap berbagai modus penipuan digital. Temuan Nugroho dan Pramudiana (2020) juga menunjukkan bahwa lemahnya pemahaman keamanan transaksi digital berkontribusi terhadap meningkatnya risiko kerugian finansial dan menurunnya tingkat kepercayaan konsumen terhadap transaksi daring yang dilakukan oleh UMKM. Kabupaten Cilacap merupakan salah satu daerah dengan aktivitas UMKM yang cukup tinggi di Provinsi Jawa Tengah. Sebagai kabupaten terluas di Jawa Tengah dengan karakteristik wilayah yang beragam, UMKM di Kabupaten Cilacap berkembang pada berbagai sektor, antara lain kuliner, perdagangan, kerajinan, fashion, jasa, serta pengolahan hasil perikanan dan pertanian. Perkembangan infrastruktur telekomunikasi dan meningkatnya penggunaan internet telah mendorong pelaku UMKM untuk mulai memanfaatkan media sosial, marketplace, dan sistem pembayaran digital dalam menjalankan usaha. Kondisi ini menunjukkan bahwa transformasi digital pada sektor UMKM di Kabupaten Cilacap telah berlangsung secara bertahap dan menjadi kebutuhan dalam mendukung keberlanjutan usaha.

Dalam upaya meningkatkan kesejahteraan ekonomi masyarakat, BAZNAS Kabupaten Cilacap telah melaksanakan berbagai program pemberdayaan ekonomi produktif melalui pembinaan dan pendampingan UMKM binaan. Program tersebut ditujukan untuk meningkatkan kemandirian ekonomi mustahik sehingga mampu berkembang menjadi pelaku usaha yang produktif dan berkelanjutan. Namun demikian, hasil observasi awal, survei kebutuhan, dan diskusi kelompok terarah (Focus Group Discussion/FGD) yang dilakukan bersama pengurus BAZNAS Kabupaten Cilacap dan pelaku UMKM binaan pada bulan September 2024 menunjukkan bahwa sebagian besar program pembinaan masih berfokus pada aspek penguatan modal usaha, pemasaran produk, dan pengelolaan usaha, sementara aspek pemanfaatan AI dan keamanan transaksi digital belum mendapatkan perhatian yang memadai.

Hasil identifikasi kebutuhan menunjukkan beberapa permasalahan utama yang dihadapi UMKM binaan BAZNAS Kabupaten Cilacap. Pertama, rendahnya pemahaman mengenai konsep dan pemanfaatan kecerdasan buatan dalam kegiatan usaha. Sebanyak 85% peserta menyatakan belum memahami fungsi AI dalam mendukung aktivitas bisnis maupun keamanan transaksi digital. Sebagian besar peserta hanya mengenal AI sebagai teknologi yang digunakan untuk menghasilkan teks atau gambar, tanpa memahami potensinya dalam membantu analisis risiko, verifikasi informasi, maupun pengambilan keputusan usaha. Kedua, rendahnya keterampilan pemanfaatan platform Generative AI sebagai alat bantu produktivitas dan keamanan digital. Sebagian besar UMKM binaan belum pernah menggunakan platform seperti ChatGPT, Gemini, atau DeepSeek untuk mendukung kegiatan usaha. Padahal, platform tersebut dapat dimanfaatkan untuk menganalisis pesan yang dicurigai sebagai phishing, memeriksa indikasi penipuan dalam komunikasi digital, menyusun edukasi keamanan pelanggan, hingga membantu interpretasi hasil analisis dari berbagai platform keamanan digital. Keterbatasan ini menyebabkan pelaku UMKM belum mampu memanfaatkan teknologi AI secara optimal dalam aktivitas usaha sehari-hari. Ketiga, rendahnya literasi penggunaan aplikasi pendukung keamanan transaksi digital. Berdasarkan hasil survei, lebih dari 90% peserta belum pernah menggunakan aplikasi verifikasi identitas digital seperti GetContact, layanan pengecekan rekening seperti Kredibel, maupun platform analisis keamanan file dan tautan seperti VirusTotal. Kondisi ini menunjukkan bahwa sebagian besar pelaku UMKM belum memiliki keterampilan dasar untuk melakukan verifikasi terhadap pihak yang bertransaksi, mengecek kredibilitas rekening tujuan, maupun mengidentifikasi potensi ancaman siber sebelum melakukan transaksi digital. Keempat, belum tersedianya model pelatihan yang mengintegrasikan kecerdasan buatan dengan praktik keamanan transaksi digital yang aplikatif bagi UMKM. Selama ini

pelatihan yang diterima peserta cenderung berfokus pada pemasaran digital dan pengembangan usaha, sementara pelatihan mengenai pemanfaatan AI untuk mendukung keamanan transaksi digital masih sangat terbatas. Padahal, perkembangan teknologi dan meningkatnya risiko kejahatan siber menuntut pelaku UMKM untuk memiliki kompetensi digital yang lebih komprehensif.

METODE PELAKSANA

Kegiatan pengabdian kepada masyarakat dilaksanakan selama dua hari pada tanggal 20-21 September 2024 di Laboratorium Keamanan Siber Politeknik Negeri Cilacap (PNC). Peserta kegiatan berjumlah 100 orang pelaku UMKM binaan BAZNAS Kabupaten Cilacap dari berbagai sektor usaha, seperti kuliner, fashion, dan jasa.

Kegiatan dilaksanakan melalui beberapa tahapan sistematis, yang pertama adalah survei dan analisis kebutuhan mitra. Survei dilaksanakan pada awal bulan September 2024 melalui kunjungan langsung ke beberapa UMKM binaan BAZNAS Kabupaten Cilacap. Kegiatan survei bertujuan mengidentifikasi kondisi eksisting terkait pemahaman pelaku UMKM terhadap konsep AI serta tingkat kesadaran mengenai keamanan transaksi digital. Lalu yang kedua adalah diskusi dan koordinasi dengan mitra. Tim PkM melakukan diskusi dengan pengurus BAZNAS Cilacap dan perwakilan UMKM binaan dari berbagai sektor usaha. Pembahasan difokuskan pada kondisi aktual terkait rendahnya pemahaman UMKM mengenai konsep dasar AI, keterbatasan pemanfaatan AI untuk keamanan transaksi digital, serta tantangan dalam menggunakan aplikasi pendukung. Hasil diskusi menjadi masukan penting dalam menentukan materi pelatihan dan pendekatan yang relevan. Yang ketiga adalah pelatihan pengenalan konsep AI untuk keamanan transaksi digital. Pelatihan tahap pertama dilaksanakan pada hari Sabtu, 20 September 2024. Materi pelatihan meliputi pemahaman dasar tentang konsep AI dan perannya dalam mendeteksi ancaman siber; pemanfaatan platform Generative AI (ChatGPT, Gemini, dan DeepSeek) untuk menganalisis potensi ancaman transaksi online, menilai keaslian situs web atau tautan pembayaran, menganalisis pola komunikasi mencurigakan menggunakan model bahasa AI; serta materi mengenai konsep dasar keamanan siber (enkripsi data, autentikasi dua faktor, perlindungan privasi digital).

Metode pelatihan menggunakan pendekatan *hands-on training* melalui praktik langsung menggunakan perangkat peserta. Pelatihan ini dilaksanakan pada hari Minggu, 21 September 2024. Materi pelatihan meliputi GetContact untuk memverifikasi identitas nomor telepon yang berhubungan dengan transaksi digital, Kredibel untuk mengecek reputasi pihak ketiga (supplier, konsumen, atau mitra bisnis), dan VirusTotal untuk memindai file atau tautan mencurigakan sebelum digunakan dalam aktivitas usaha online. Peserta dibimbing untuk menghubungkan pemanfaatan aplikasi tersebut dengan konsep AI yang bekerja di baliknya, sehingga tidak hanya mampu menggunakan aplikasi tetapi juga memahami logika dasar bagaimana AI membantu mendeteksi potensi ancaman digital.

sevaluasi dilakukan melalui pre-test dan post-test untuk mengukur peningkatan pemahaman peserta. Pre-test diberikan sebelum pelatihan dimulai untuk mengukur tingkat pemahaman awal peserta mengenai AI dan keamanan transaksi. Post-test diberikan setelah seluruh rangkaian pelatihan selesai untuk mengukur peningkatan pemahaman dan keterampilan peserta. Instrumen evaluasi berupa 10 pertanyaan terkait materi pelatihan yang telah diberikan.

Data hasil pre-test dan post-test dianalisis secara deskriptif kuantitatif dengan menghitung nilai rata-rata, jumlah kenaikan, dan persentase kenaikan menggunakan formula:

$$\text{Persentase Kenaikan} = (\text{Jumlah Kenaikan} / \text{Nilai Pre-test}) \times 100\%$$

HASIL DAN PEMBAHASAN

Hasil Survei dan Koordinasi dengan Mitra

Berdasarkan hasil survei dan diskusi dengan BAZNAS Cilacap serta perwakilan UMKM, teridentifikasi bahwa sebagian besar pelaku UMKM binaan BAZNAS belum memahami konsep AI dan belum memanfaatkan aplikasi pendukung keamanan digital seperti GetContact, Kredibel, dan VirusTotal. Kendala utama yang dihadapi adalah keterbatasan pemahaman teknis, minimnya pelatihan, serta kurangnya pengalaman praktis dalam penggunaan teknologi keamanan

digital. Temuan ini sejalan dengan penelitian Utami dan Wibowo (2021) yang menyatakan bahwa literasi digital UMKM di Indonesia masih rendah, terutama dalam aspek keamanan siber.

Pelaksanaan Pelatihan Pengenalan Konsep AI

Pelatihan hari pertama pada 20 September 2024 diikuti oleh sekitar 100 peserta UMKM binaan BAZNAS. Peserta menunjukkan antusiasme tinggi dalam memahami konsep dasar AI, khususnya bagaimana teknologi ini dapat membantu mengidentifikasi ancaman digital. Melalui pendekatan *hands-on training*, peserta mempraktikkan langsung penggunaan platform Generative AI (ChatGPT, Gemini, DeepSeek) untuk menganalisis pesan atau tautan mencurigakan. Peserta dilatih untuk menggunakan AI sebagai asisten digital dalam menilai keaslian situs web, menganalisis pola komunikasi mencurigakan, dan memahami konsep keamanan siber dasar. Hasil observasi menunjukkan bahwa peserta yang sebelumnya tidak familiar dengan AI mampu menggunakannya untuk keperluan praktis dalam waktu singkat. Hal ini mengindikasikan bahwa pendekatan pembelajaran praktis lebih efektif dibandingkan pembelajaran teoritis, sebagaimana dinyatakan oleh Kurniawan dan Lestari (2022).

Pelaksanaan Pelatihan Aplikasi Pendukung Keamanan Digital

Pelatihan hari kedua pada 21 September 2024 berfokus pada praktik penggunaan aplikasi pendukung keamanan digital. Peserta dilatih menggunakan GetContact untuk memverifikasi identitas kontak, Kredibel untuk memeriksa reputasi mitra bisnis atau nomor rekening, dan VirusTotal untuk mendeteksi file atau tautan berisiko.

Peserta menunjukkan kemampuan yang baik dalam mengoperasikan ketiga aplikasi tersebut. Mereka mampu mempraktikkan secara mandiri cara verifikasi nomor telepon yang mencurigakan, pengecekan kredibilitas rekening sebelum transfer, dan pemindaian tautan atau file sebelum dibuka. Pelatihan ini memberikan keterampilan praktis yang dapat langsung diimplementasikan dalam aktivitas usaha sehari-hari.



Gambar 1. Pelaksanaan Pelatihan



Gambar 2. Pelaksanaan FGD

Integrasi antara pemahaman konsep AI dan penggunaan aplikasi praktis membuat peserta tidak hanya mampu menggunakan teknologi, tetapi juga memahami logika kerja sistem keamanan digital. Hal ini penting untuk membangun kesadaran jangka panjang terhadap ancaman siber, sebagaimana ditekankan oleh Arora dkk. (2021) bahwa literasi keamanan siber yang komprehensif lebih efektif dalam melindungi UMKM.

Hasil Evaluasi Pre-test dan Post-test

Evaluasi dilakukan terhadap 100 peserta menggunakan 10 soal terkait materi pelatihan. Hasil pre-test menunjukkan rata-rata nilai peserta sebesar 78,09. Nilai awal ini tergolong relatif tinggi apabila dikaitkan dengan kondisi literasi digital peserta yang pada tahap identifikasi kebutuhan masih tergolong rendah.

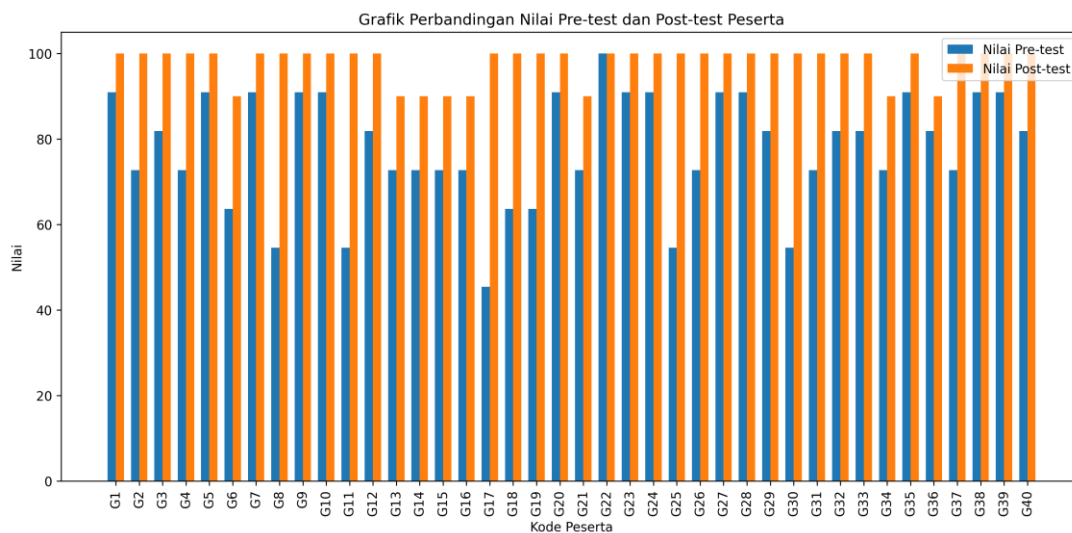
Tingginya nilai pre-test tersebut perlu dimaknai secara proporsional dan disebabkan oleh dua faktor utama. Pertama, kesepuluh soal evaluasi disusun pada tingkat kesulitan dasar yang menekankan konsep umum dan pengenalan istilah, sehingga sebagian pertanyaan masih dapat dijawab peserta berdasarkan pengetahuan umum sehari-hari, bukan berdasarkan pemahaman teknis yang mendalam. Kedua, sebagian materi dasar—seperti istilah kecerdasan buatan dan kewaspadaan umum terhadap penipuan daring—telah dikenal peserta melalui paparan media sosial dan pemberitaan, meskipun mereka belum memahaminya secara praktis dalam pengamanan transaksi digital. Dengan demikian, nilai pre-test yang tinggi lebih mencerminkan pengetahuan permukaan (*surface knowledge*), sementara kesenjangan yang menjadi urgensi kegiatan ini justru terletak pada aspek keterampilan teknis dan penerapannya. Hal ini ditegaskan oleh rendahnya kemampuan awal peserta dalam menggunakan aplikasi pendukung keamanan digital, di mana lebih dari 90% peserta belum pernah menggunakan aplikasi seperti GetContact, Kredibel, maupun VirusTotal sebelum pelatihan. Tabel 1 menunjukkan hasil penilaian pre-test dan post-test peserta selama pelatihan.

Tabel 1. Hasil Penilaian Pre-test dan Post-test Peserta Selama Pelatihan

No	Kode Peserta	Nilai Pre-test	Nilai Post-test	Jumlah Naik	Kenaikan (%)
1	G1	90,91	100	9,09	10
2	G2	72,73	100	27,27	37,5
3	G3	81,82	100	18,18	22,22
4	G4	72,73	100	27,27	37,5
5	G5	90,91	100	9,09	10
6	G6	63,64	90	26,36	41,43
7	G7	90,91	100	9,09	10
8	G8	54,55	100	45,45	83,33
9	G9	90,91	100	9,09	10
10	G10	90,91	100	9,09	10
95	G95	54,55	100	45,45	83,33
96	G96	90,91	100	9,09	10
97	G97	81,82	100	18,18	22,22
98	G98	54,55	100	45,45	83,33
99	G99	90,91	100	9,09	10
100	G100	81,82	100	18,18	22,22
Rata-rata		78,09	97,5	19,41	28,98

Keterangan: Tabel 1 hanya menampilkan sebagian (sampel) data dari keseluruhan 100 peserta kegiatan; data selengkapnya dirangkum pada nilai rata-rata di baris terakhir tabel.

Pada Tabel 1 di atas, terdapat 2 peserta (G22 dan G49) yang telah memiliki nilai sempurna (100) pada pre-test, sementara nilai terendah adalah 36,36 (G82). Setelah mengikuti pelatihan selama dua hari, hasil post-test menunjukkan peningkatan signifikan dengan rata-rata nilai mencapai 97,50. Sebanyak 75 peserta (75%) memperoleh nilai sempurna (100), sedangkan nilai terendah post-test adalah 70,00 (G79), yang tetap menunjukkan peningkatan dari nilai pre-test sebesar 45,45. Rata-rata kenaikan nilai absolut adalah 19,41 poin, dengan persentase kenaikan rata-rata sebesar 28,98%. Kenaikan tertinggi dicapai oleh peserta G82 dengan peningkatan 63,64 poin (175%), yang menunjukkan efektivitas pelatihan bagi peserta dengan pemahaman awal yang sangat terbatas.



Gambar 3. Perbandingan Nilai Pre-test dan Post-test Peserta

Data lengkap hasil evaluasi menunjukkan bahwa seluruh peserta mengalami peningkatan pemahaman, kecuali 2 peserta yang sudah memiliki nilai sempurna sejak pre-test. Hasil ini menunjukkan bahwa metode *hands-on training* dengan pendampingan langsung efektif meningkatkan pemahaman dan keterampilan pelaku UMKM dalam memanfaatkan AI dan aplikasi pendukung keamanan digital. Peningkatan yang signifikan ini sejalan dengan temuan Kurniawan dan Lestari (2022) bahwa pelatihan praktik langsung memberikan dampak lebih besar dibandingkan pelatihan teoritis.

Implikasi Praktis

Peningkatan pemahaman dan keterampilan peserta memiliki implikasi praktis yang penting bagi keberlanjutan usaha UMKM. Dengan kemampuan menggunakan AI dan aplikasi keamanan digital, pelaku UMKM diharapkan dapat:

1. Mengurangi risiko kerugian finansial akibat penipuan online dan serangan siber
2. Meningkatkan kepercayaan konsumen dalam bertransaksi secara digital
3. Memperluas jangkauan pasar melalui platform digital yang aman
4. Meningkatkan daya saing usaha di era ekonomi digital

Keberhasilan program ini juga menunjukkan pentingnya kolaborasi antara perguruan tinggi (Politeknik Negeri Cilacap), lembaga sosial (BAZNAS), dan pelaku usaha dalam memperkuat ekosistem digital yang aman dan berkelanjutan, sebagaimana ditekankan oleh Huda dkk (Huda dkk., 2020).

Keterbatasan Kegiatan

Meskipun menunjukkan hasil yang positif, kegiatan ini memiliki beberapa keterbatasan. Pertama, waktu pelatihan yang terbatas (dua hari) belum cukup untuk memastikan internalisasi pengetahuan jangka panjang. Kedua, kegiatan ini belum mengukur dampak jangka panjang terhadap perubahan perilaku pelaku UMKM dalam mengamankan transaksi digital. Ketiga, belum ada mekanisme pendampingan berkelanjutan pasca-pelatihan untuk memastikan implementasi berkelanjutan.

KESIMPULAN DAN SARAN

Kegiatan pengabdian kepada masyarakat berupa pelatihan AI dan keamanan transaksi digital bagi UMKM binaan BAZNAS Kabupaten Cilacap telah terlaksana dengan baik dan mencapai tujuan yang ditetapkan. Terdapat peningkatan signifikan dalam pemahaman peserta terhadap konsep dasar keamanan transaksi digital dan peran AI dalam mendeteksi ancaman siber, yang ditunjukkan dengan kenaikan rata-rata nilai dari 78,09 (pre-test) menjadi 97,50 (post-test), dengan peningkatan sebesar 19,41 poin atau 28,98%.

Peserta mampu memanfaatkan platform AI (ChatGPT, Gemini, DeepSeek) untuk menganalisis ancaman digital dan menggunakan aplikasi pendukung keamanan (GetContact, Kredibel, VirusTotal) untuk melindungi transaksi usaha. Keberhasilan program ini menunjukkan efektivitas pendekatan *hands-on training* dengan pendampingan langsung dalam meningkatkan literasi keamanan digital pelaku UMKM.

DAFTAR PUSTAKA

- Arora, A., Sharma, P., & Sharma, S. (2021). AI-Based Cybersecurity Framework for SMEs: A Comprehensive Review. *Journal of Cybersecurity and Privacy*, 1(3), 487–510.
- Dwivedi, Y. K., Kshetri, N., Hughes, L., Slade, E. L., Jeyaraj, A., Kar, A. K., & Wright, R. (2023). {`So What If ChatGPT Wrote It?`} Multidisciplinary Perspectives on Opportunities, Challenges and Implications of Generative Conversational AI for Research, Practice and Policy. *International Journal of Information Management*, 71, 102642.
- Huda, N., Rini, N., Mardoni, Y., & Putra, P. (2020). Zakat Produktif untuk Pemberdayaan Ekonomi Umat: Model Pengembangan BAZNAS. *Jurnal Ekonomi Islam*, 11(2), 151–168.
- Jayusman, H., & Mahardika, F. (2024). Mobile-Based Event Decoration Ordering System Using UAT Method with PIECES Framework. *Journal of Innovation Information Technology and Application (JINITA)*, 7, 1623–172.
- Kurniawan, D., & Lestari, P. (2022). Efektivitas Pelatihan Berbasis Praktik dalam Meningkatkan Kompetensi Digital UMKM. *Jurnal Pengabdian Masyarakat*, 5(1), 78–89.
- Lestari, I. (2021). Strategi Pemasaran Dalam Meningkatkan Penjualan Motor Bekas Di Doyok Motor Kecamatan Kebonsari Kabupaten Madiun. *Frontiers in Neuroscience*, 14(1), 1–13.
- Mahardika, F., Amin, M. Al, Suseno, A. T., Informatika, P. T., & Cilacap, P. N. (2025). *PENDAMPINGAN DAN PELATIHAN PENGELOLAAN WEBSITE SMA PGRI 4 GANDRUNGMANGU CILACAP*. 143–152.
- Mikalef, P., Conboy, K., & Krogstie, J. (2021). Artificial Intelligence as an Enabler of B2B Marketing: A Dynamic Capabilities Micro-Foundations Approach. *Industrial Marketing Management*, 98, 80–92.
- Musytari. (2025). Ketahanan UMKM Berbasis Digital: Studi pada UMKM di Sektor E-Commerce. *Musytari: Jurnal Manajemen, Akuntansi, Dan Ekonomi*, 20(7), 111–120.
- Nugroho, A., & Pramudiana, I. (2020). Keamanan Transaksi Digital pada UMKM: Studi Kasus E-Commerce di Indonesia. *Jurnal Teknologi Informasi Dan Komputer*, 6(1), 45–54.
- Nugroho, A., Purwanto, J., Muin, M. A., & Mahardika, F. (2025). UI/UX design of a web-based student organizations system using the design thinking method approach. *E-Journals.Dinamika.Ac.Id*, 7(1). <https://doi.org/10.37802/joti.v7i1.983>
- Rahayu, R., & Day, J. (2022). Digital Transformation of SMEs: The Role of Competitive Advantage and Innovation Capability. *Journal of Small Business Strategy*, 32(2), 15–28.
- Ripai, R., Pari, R. A., Sidik, F., Shandy, S. V., & Mahardika, F. (2025). Implementasi Layanan Cloudflare sebagai Mitigasi terhadap Ancaman Pemindaian dan Eksploitasi Siber Menggunakan Nmap dan Metasploit. *Sudo Jurnal Teknik Informatika*, 4(1), 40–49. <https://doi.org/10.56211/sudo.v4i1.902>
- Schwab, K. (2016). *The Fourth Industrial Revolution*. World Economic Forum.
- Utami, S., & Wibowo, A. (2021). Digitalisasi UMKM: Tantangan dan Strategi dalam Era Industri 4.0. *Jurnal Ekonomi Dan Bisnis*, 24(2), 115–128.