

Model Kerangka Kerja Kesadaran Siber UMKM untuk Meningkatkan Literasi Keamanan Digital dan Pencegahan Rekayasa Sosial

Diana Novita¹, Hanifah², Roy Budiharjo³, Yuliati¹,
Agus Aerwanto¹, Asrarul Rahman³

¹Universitas Esa Unggul

²Sekolah Tinggi Ilmu Ekonomi Bisnis Indonesia

³Universitas Telkom

Penulis korespondensi : diana.novita@esaunggul.ac.id

Dikirim : 14 Mei 2026

Direvisi : 28 Juni 2026

Diterima : 29 Juni 2026

Abstrak: Transformasi digital telah mendorong pelaku Usaha Mikro Kecil dan Menengah (UMKM) untuk mengadopsi berbagai teknologi digital dalam aktivitas bisnis, seperti pemanfaatan media sosial, marketplace, dan sistem pembayaran elektronik. Digitalisasi tersebut memberikan peluang peningkatan daya saing dan efisiensi operasional, namun belum diimbangi dengan tingkat literasi keamanan digital yang memadai. Rendahnya pemahaman terhadap risiko keamanan informasi menjadikan UMKM sebagai kelompok yang sangat rentan terhadap serangan siber, khususnya social engineering yang memanfaatkan manipulasi psikologis pengguna untuk memperoleh informasi sensitif. Kegiatan pengabdian kepada masyarakat ini bertujuan mengimplementasikan sekaligus mengevaluasi UMKM Cyber Awareness Framework sebagai model peningkatan literasi keamanan digital berbasis edukasi partisipatif dan praktik langsung. Metode yang digunakan adalah Participatory Action Research dengan pendekatan kuantitatif melalui desain pre-test dan post-test terhadap 38 pelaku UMKM digital. Tahapan kegiatan meliputi analisis kebutuhan, pelatihan keamanan digital, simulasi kasus social engineering, implementasi praktik keamanan akun, serta evaluasi hasil pelatihan. Analisis data dilakukan menggunakan uji validitas instrumen, pengujian reliabilitas Cronbach Alpha, serta paired sample t-test untuk mengukur efektivitas program. Hasil evaluasi menunjukkan adanya peningkatan signifikan literasi keamanan digital peserta, dengan skor rata-rata meningkat dari 53,2 sebelum pelatihan menjadi 87,4 setelah kegiatan ($p < 0,001$). Nilai reliabilitas sebesar $\alpha = 0,89$ menunjukkan konsistensi instrumen yang sangat baik. Program pengabdian ini terbukti mampu meningkatkan kesadaran keamanan digital, kemampuan identifikasi phishing, serta praktik perlindungan data pelanggan. Framework yang dihasilkan memberikan kontribusi praktis sebagai model edukasi keamanan digital yang adaptif dan berpotensi direplikasi secara luas pada komunitas UMKM di tingkat nasional.

Kata kunci: kesadaran siber, literasi keamanan digital, pelayanan masyarakat, rekayasa sosial, UMKM

Abstract: Digital transformation has encouraged Micro, Small, and Medium Enterprises (MSMEs) to adopt various digital technologies in their business activities, such as the use of social media, marketplaces, and electronic payment systems. This digitalization provides opportunities to increase competitiveness and operational efficiency, but has not been matched

by an adequate level of digital security literacy. Low understanding of information security risks makes MSMEs a group that is highly vulnerable to cyber attacks, particularly social engineering that exploits user psychological manipulation to obtain sensitive information. This community service activity aims to implement and evaluate the MSME Cyber Awareness Framework as a model for increasing digital security literacy based on participatory education and direct practice. The method used is Participatory Action Research with a quantitative approach through a pre-test and post-test design on 38 digital MSMEs. The activity stages include needs analysis, digital security training, social engineering case simulations, implementation of account security practices, and evaluation of training results. Data analysis was carried out using instrument validity testing, Cronbach Alpha reliability testing, and paired sample t-tests to measure program effectiveness. The evaluation results showed a significant increase in participants' digital security literacy, with the average score increasing from 53.2 before the training to 87.4 after the activity ($p < 0.001$). A reliability value of $\alpha = 0.89$ indicates excellent instrument consistency. This community service program has been proven to be able to increase digital security awareness, phishing identification skills, and customer data protection practices. The resulting framework provides a practical contribution as an adaptive digital security education model and has the potential for widespread replication in MSME communities at the national level.

Keywords: *community service, cyber awareness, digital security literacy, MSMEs, social engineering*

1. Pendahuluan

Digitalisasi ekonomi telah mendorong pelaku Usaha Mikro Kecil dan Menengah (UMKM) untuk mengadopsi berbagai teknologi digital dalam menjalankan aktivitas bisnis (Mutiarani dkk., 2025; Angraini dkk., 2024; Fizzanty, 2024; Meilariza *et al.*, 2024). Pemanfaatan *marketplace*, media sosial, serta sistem pembayaran elektronik memungkinkan UMKM memperluas jangkauan pemasaran, meningkatkan efisiensi operasional, serta membangun hubungan yang lebih interaktif dengan pelanggan. Transformasi digital ini memberikan peluang besar bagi UMKM untuk meningkatkan daya saing dan mempercepat pertumbuhan usaha di tengah perkembangan ekonomi berbasis teknologi (Ayu *et al.*, 2026; Morisson dkk., 2025). Melalui platform digital, pelaku UMKM tidak lagi terbatas oleh ruang dan waktu, sehingga mampu menjangkau konsumen lintas daerah bahkan pasar global dengan biaya operasional yang relatif lebih rendah. Namun, di balik berbagai manfaat tersebut, peningkatan konektivitas digital juga membawa konsekuensi berupa meningkatnya risiko keamanan siber yang semakin kompleks dan dinamis (Abrardi *et al.*, 2026; Admass *et al.*, 2024; Agustin, 2024). Aktivitas bisnis yang sebelumnya dilakukan secara konvensional kini berpindah ke ruang digital yang rentan terhadap berbagai bentuk serangan siber. Banyak pelaku UMKM yang fokus pada aspek pemasaran dan penjualan digital, tetapi belum memiliki kesadaran yang memadai terhadap perlindungan data, keamanan akun bisnis, maupun

manajemen risiko digital. Kondisi ini menciptakan celah keamanan yang dapat dimanfaatkan oleh pelaku kejahatan siber untuk melakukan eksploitasi.

Ancaman keamanan siber modern tidak lagi hanya menargetkan kelemahan teknis sistem atau perangkat lunak, tetapi lebih banyak mengeksploitasi faktor manusia sebagai titik lemah utama keamanan informasi (Colabianchi *et al.*, 2025; Khadka & Ullah, 2025; Masmoudi, 2025). Pendekatan ini dikenal sebagai *social engineering*, yaitu teknik serangan yang memanfaatkan manipulasi psikologis untuk mempengaruhi korban agar secara sukarela memberikan informasi sensitif. Informasi yang menjadi target antara lain kata sandi akun, kode autentikasi, data transaksi, hingga informasi pelanggan. Menurut Hadnagy (2018), keberhasilan *social engineering* bergantung pada kemampuan penyerang memahami perilaku manusia, rasa percaya, serta kurangnya kewaspadaan pengguna terhadap ancaman digital. Pelaku UMKM menjadi salah satu kelompok yang paling rentan terhadap serangan *social engineering* (Anggita dkk., 2025). Hal ini disebabkan oleh beberapa faktor, antara lain rendahnya literasi keamanan digital, keterbatasan sumber daya teknologi, serta minimnya pelatihan keamanan informasi yang terstruktur dan berkelanjutan. Banyak pelaku UMKM menggunakan perangkat pribadi untuk aktivitas bisnis tanpa pengamanan yang memadai, seperti penggunaan kata sandi yang sama pada berbagai platform, tidak mengaktifkan autentikasi dua faktor, serta kurang memahami tanda-tanda penipuan digital. Situasi tersebut memperbesar risiko kebocoran data, pengambilalihan akun bisnis, hingga kerugian finansial yang signifikan.

Laporan keamanan global menunjukkan bahwa lebih dari 70% insiden pelanggaran data diawali oleh kesalahan manusia, seperti mengklik tautan phishing, membuka lampiran berbahaya, atau membocorkan kredensial akun bisnis secara tidak sadar (Verizon, 2023). Fakta ini menegaskan bahwa investasi teknologi keamanan saja tidak cukup untuk melindungi organisasi maupun pelaku usaha dari ancaman siber. Keamanan digital membutuhkan pendekatan yang berpusat pada manusia (*human-centered cybersecurity*), di mana peningkatan literasi, kesadaran, dan perilaku pengguna menjadi lapisan pertahanan utama dalam sistem keamanan informasi. Dalam konteks tersebut, perguruan tinggi memiliki peran strategis sebagai agen perubahan sosial melalui kegiatan pengabdian kepada masyarakat. Institusi pendidikan tinggi tidak hanya berfungsi sebagai pusat pengembangan ilmu pengetahuan, tetapi juga sebagai fasilitator peningkatan kapasitas masyarakat dalam menghadapi tantangan transformasi digital. Melalui program pengabdian masyarakat, dosen dan akademisi dapat

mentransfer pengetahuan praktis mengenai keamanan digital kepada komunitas UMKM sehingga mereka mampu menjalankan bisnis digital secara aman dan berkelanjutan.

Kegiatan pengabdian ini menawarkan kebaruan melalui pengembangan UMKM *Cyber Awareness Framework*, yaitu model literasi keamanan digital yang dirancang secara sistematis dengan mengintegrasikan edukasi konseptual, simulasi serangan nyata, serta pembentukan perubahan perilaku keamanan digital. *Framework* ini tidak hanya berfokus pada penyampaian materi teoritis, tetapi juga menekankan pengalaman belajar berbasis praktik dan refleksi peserta. Pendekatan tersebut diharapkan mampu meningkatkan pemahaman sekaligus membangun kebiasaan keamanan digital yang berkelanjutan dalam aktivitas bisnis UMKM. Kontribusi utama kegiatan ini meliputi beberapa aspek penting. Pertama, menghasilkan model pengabdian masyarakat berbasis *cybersecurity awareness* yang sistematis, aplikatif, dan mudah direplikasi pada berbagai komunitas UMKM. Kedua, kegiatan ini mengukur dampak pelatihan secara kuantitatif melalui pendekatan ilmiah sehingga efektivitas program dapat dibuktikan secara empiris. Ketiga, kegiatan menghasilkan luaran implementatif berupa peningkatan kemampuan praktis pelaku UMKM dalam mengamankan akun bisnis, melindungi data pelanggan, serta menjaga keamanan transaksi digital. Dengan adanya model UMKM *Cyber Awareness Framework*, diharapkan pelaku UMKM tidak hanya mampu memanfaatkan teknologi digital untuk pertumbuhan bisnis, tetapi juga memiliki ketahanan siber yang kuat dalam menghadapi ancaman keamanan informasi. Model ini berpotensi menjadi referensi strategis dalam pengembangan program literasi keamanan digital nasional, sekaligus mendukung terciptanya ekosistem ekonomi digital yang aman, inklusif, dan berkelanjutan di era transformasi digital.

2. Metode

Metode pelaksanaan kegiatan pengabdian kepada masyarakat ini menggunakan pendekatan *Participatory Action Research* (PAR) yang menekankan keterlibatan aktif peserta dalam seluruh tahapan kegiatan. Pendekatan ini dipilih karena mampu mengintegrasikan proses pembelajaran, praktik langsung, serta evaluasi berkelanjutan guna menghasilkan perubahan perilaku yang nyata. Model PAR dilaksanakan melalui siklus kegiatan yang meliputi perencanaan, aksi, observasi, dan refleksi sebagaimana dikemukakan oleh Kemmis & McTaggart (2014).

Pada tahap perencanaan, tim pengabdian melakukan identifikasi kebutuhan mitra UMKM

melalui survei awal dan diskusi kelompok untuk mengetahui tingkat literasi keamanan digital serta permasalahan yang sering dihadapi peserta. Hasil analisis kebutuhan digunakan sebagai dasar penyusunan materi pelatihan, modul edukasi, serta skenario simulasi social engineering yang relevan dengan aktivitas bisnis UMKM.

Tahap aksi dilakukan melalui metode presentasi interaktif yang menyampaikan materi literasi keamanan digital, jenis-jenis serangan *social engineering*, serta strategi perlindungan akun bisnis dan data pelanggan. Penyampaian materi dilakukan secara komunikatif menggunakan media visual, studi kasus nyata, dan demonstrasi praktik keamanan digital agar peserta lebih mudah memahami konsep yang diberikan.

Selanjutnya, tahap observasi dilakukan selama kegiatan berlangsung dengan memantau partisipasi peserta, tingkat pemahaman materi, serta kemampuan peserta dalam mengikuti simulasi keamanan digital. Tim pelaksana mencatat respons, kendala, dan perkembangan peserta sebagai bahan evaluasi program.

Tahap terakhir yaitu refleksi, dilaksanakan melalui sesi tanya jawab dan diskusi terbuka antara narasumber dan peserta. Pada sesi ini peserta dapat menyampaikan pengalaman, permasalahan nyata, serta solusi yang dapat diterapkan secara langsung dalam bisnis mereka. Proses refleksi ini bertujuan memperkuat pemahaman peserta sekaligus memastikan keberlanjutan praktik keamanan digital setelah kegiatan pengabdian selesai.

Evaluasi program pengabdian dilakukan untuk mengukur efektivitas implementasi UMKM *Cyber Awareness Framework* dalam meningkatkan literasi keamanan digital serta kemampuan peserta dalam mencegah serangan *social engineering*. Evaluasi menggunakan pendekatan *before-after* dengan desain *pre-test* dan *post-test* yang dilaksanakan sebelum dan setelah pelatihan. Pengukuran difokuskan pada tiga aspek utama, yaitu peningkatan pengetahuan (*knowledge*), kesadaran terhadap keamanan digital (*security awareness*), dan perubahan perilaku dalam menerapkan praktik keamanan digital (*security practice*). Hasil evaluasi digunakan untuk menganalisis perubahan kemampuan peserta sebagai indikator keberhasilan pelaksanaan program pengabdian.

Indikator evaluasi program disusun untuk mengukur tingkat keberhasilan pelaksanaan pelatihan literasi keamanan digital pada pelaku UMKM. Evaluasi mencakup lima aspek utama, yaitu literasi keamanan digital, *social engineering awareness*, keamanan akun, perlindungan data, dan perubahan perilaku peserta setelah mengikuti kegiatan. Pada aspek literasi keamanan digital, evaluasi difokuskan pada kemampuan peserta dalam memahami konsep dasar

keamanan serta mengenali berbagai risiko yang dapat mengancam aktivitas bisnis digital. Aspek *social engineering awareness* bertujuan mengukur kemampuan peserta dalam mengidentifikasi berbagai bentuk serangan phishing dan modus penipuan digital yang umum terjadi. Selanjutnya, aspek keamanan akun menilai penerapan praktik pengelolaan kata sandi yang aman, termasuk penggunaan autentikasi dua faktor (*Two-Factor Authentication*) sebagai upaya meningkatkan keamanan akun bisnis. Aspek perlindungan data mengevaluasi kemampuan peserta dalam mengelola dan menyimpan data pelanggan secara aman sesuai dengan prinsip keamanan informasi. Sementara itu, aspek perubahan perilaku digunakan untuk mengukur sejauh mana peserta mampu mengimplementasikan praktik-praktik keamanan digital yang telah diperoleh selama pelatihan ke dalam aktivitas bisnis sehari-hari. Kelima aspek tersebut diharapkan dapat memberikan gambaran yang komprehensif mengenai perubahan pengetahuan, kesadaran, dan perilaku peserta sebagai indikator keberhasilan program pengabdian kepada masyarakat. Indikator evaluasi direkapitulasi dalam Tabel 1.

Tabel 1. Indikator evaluasi

Aspek	Indikator	Deskripsi
Literasi Keamanan Digital	Pemahaman konsep keamanan	Memahami risiko digital
<i>Social Engineering Awareness</i>	Identifikasi <i>phishing</i>	Mengenali modus penipuan
Keamanan Akun	Pengelolaan <i>password</i>	Penggunaan autentikasi ganda
Perlindungan Data	Manajemen data pelanggan	Praktik penyimpanan aman
Perubahan Perilaku	Implementasi praktik	Penerapan setelah pelatihan

Evaluasi program menggunakan instrumen berupa kuesioner dengan skala Likert lima tingkat, yaitu 1 = sangat tidak setuju, 2 = tidak setuju, 3 = netral, 4 = setuju, dan 5 = sangat setuju. Kuesioner terdiri atas 20 butir pertanyaan yang dirancang untuk mengukur tingkat pengetahuan, kesadaran, dan perilaku peserta dalam menerapkan keamanan digital. Beberapa indikator yang diukur meliputi pemahaman terhadap ciri-ciri pesan *phishing*, penggunaan kata sandi yang berbeda pada setiap akun bisnis, penerapan *Two-Factor Authentication* (2FA), serta pemahaman mengenai pentingnya perlindungan data pelanggan. Data penelitian dikumpulkan melalui pelaksanaan *pre-test* sebelum pelatihan dan *post-test* setelah pelatihan, yang didukung dengan observasi selama kegiatan berlangsung, dokumentasi praktik keamanan digital yang dilakukan peserta, serta diskusi reflektif dan sesi tanya jawab untuk memperoleh informasi yang lebih komprehensif mengenai perubahan pengetahuan dan perilaku peserta. Sebelum digunakan, instrumen evaluasi diuji validitasnya menggunakan uji *Pearson Product Moment* dan reliabilitasnya menggunakan koefisien Cronbach's Alpha untuk memastikan bahwa setiap

butir pertanyaan mampu mengukur aspek yang dimaksud secara konsisten. Selanjutnya, data dianalisis menggunakan statistik deskriptif untuk menggambarkan rata-rata peningkatan skor literasi keamanan digital peserta, sedangkan pengujian perbedaan hasil *pre-test* dan *post-test* dilakukan menggunakan *paired sample t-test*. Program dinyatakan memberikan pengaruh yang signifikan apabila hasil pengujian menunjukkan nilai signifikansi (p-value) kurang dari 0,05.

3. Hasil dan Diskusi

3.1 Profil Peserta dan Kondisi Awal Literasi Keamanan Digital UMKM

Kegiatan pengabdian kepada masyarakat dengan tema Literasi Keamanan Digital dan Pencegahan *Social Engineering* pada UMKM dilaksanakan dengan melibatkan pelaku UMKM yang aktif menggunakan platform digital dalam operasional bisnisnya. Peserta berjumlah 32 pelaku UMKM yang bergerak pada sektor kuliner, *fashion*, kesehatan herbal, jasa kreatif, dan perdagangan online. Mayoritas peserta menggunakan media sosial seperti Instagram, WhatsApp Business, serta *marketplace* sebagai sarana utama transaksi bisnis.

Hasil identifikasi awal melalui kuesioner pre-test menunjukkan bahwa tingkat literasi keamanan digital peserta masih berada pada kategori rendah hingga menengah. Sebanyak 68% peserta belum memahami konsep autentikasi dua faktor (*Two Factor Authentication*), 72% peserta menggunakan kata sandi yang sama pada beberapa akun bisnis, dan 60% peserta pernah menerima pesan mencurigakan namun tidak mengetahui cara melakukan verifikasi keamanan.

Temuan ini sejalan dengan penelitian Hadnagy (2018) yang menyatakan bahwa kelemahan utama keamanan siber bukan berada pada teknologi, melainkan pada perilaku pengguna. Pelaku UMKM cenderung fokus pada aktivitas pemasaran dan penjualan tanpa mempertimbangkan risiko keamanan digital yang menyertainya. Kondisi tersebut memperlihatkan bahwa peningkatan literasi keamanan menjadi kebutuhan mendesak dalam ekosistem ekonomi digital.

Selain itu, wawancara awal menunjukkan bahwa sebagian besar peserta menganggap serangan siber hanya terjadi pada perusahaan besar. Persepsi keliru ini menyebabkan rendahnya kesiapan UMKM dalam menghadapi ancaman *phishing*, penipuan digital, maupun pengambilalihan akun bisnis.

3.2 Implementasi UMKM *Cyber Awareness Framework*

Pelaksanaan kegiatan pengabdian kepada masyarakat menggunakan pendekatan *Participatory Action Research* (PAR), yang menempatkan peserta sebagai subjek aktif dalam seluruh proses pembelajaran dan penerapan praktik keamanan digital. Melalui pendekatan ini, peserta tidak hanya menerima materi secara teoretis, tetapi juga terlibat secara langsung dalam proses identifikasi masalah, praktik, refleksi, dan evaluasi. Program dirancang berdasarkan *UMKM Cyber Awareness Framework*, yang dikembangkan dalam empat tahapan utama, yaitu edukasi konseptual mengenai keamanan digital, simulasi berbagai bentuk serangan *social engineering*, praktik implementasi pengamanan akun bisnis, serta refleksi dan evaluasi terhadap perubahan pengetahuan, kesadaran, dan perilaku peserta dalam menerapkan keamanan digital. Keempat tahapan tersebut disusun secara sistematis untuk membangun kompetensi peserta secara bertahap, mulai dari peningkatan pemahaman konseptual hingga kemampuan mengimplementasikan praktik keamanan digital dalam aktivitas bisnis sehari-hari.

3.2.1 Edukasi Konseptual

Pada tahap awal, peserta diberikan pemahaman mengenai konsep dasar keamanan informasi, jenis ancaman siber pada UMKM, karakteristik serangan *social engineering*, dan pentingnya perlindungan data pelanggan. Materi disampaikan melalui metode presentasi interaktif menggunakan studi kasus nyata penipuan marketplace dan pembajakan akun bisnis. Pendekatan ini terbukti meningkatkan keterlibatan peserta karena materi dikaitkan langsung dengan pengalaman bisnis mereka. Diskusi kelompok menunjukkan bahwa peserta mulai memahami bahwa keamanan digital merupakan bagian dari strategi bisnis, bukan hanya aspek teknis teknologi.

3.2.2 Simulasi Serangan *Social Engineering*

Tahap simulasi menjadi bagian paling penting dalam kegiatan pengabdian. Tim pelaksana melakukan simulasi berupa pesan *phishing* tiruan, *e-mail* penawaran palsu, permintaan kode OTP fiktif, dan rekayasa komunikasi melalui WhatsApp. Hasil observasi menunjukkan bahwa pada simulasi pertama, 56% peserta masih memberikan respons terhadap pesan *phishing*. Setelah sesi edukasi lanjutan dan refleksi bersama, tingkat keberhasilan peserta dalam mengenali serangan meningkat secara signifikan. Simulasi terbukti efektif karena memberikan pengalaman belajar berbasis praktik (*experiential learning*). Peserta tidak hanya memahami teori, tetapi juga mengalami langsung mekanisme manipulasi psikologis yang digunakan pelaku kejahatan siber.

3.2.3 Praktik Implementasi Keamanan Digital

Pada tahap aksi, peserta melakukan praktik langsung pengamanan akun bisnis, meliputi aktivasi autentikasi dua faktor, pembuatan *password* kuat, pengaturan privasi media sosial, *backup* data pelanggan, dan pengenalan aplikasi keamanan dasar. Pendampingan dilakukan secara langsung agar setiap peserta mampu menerapkan langkah keamanan secara mandiri. Sebanyak 90% peserta berhasil mengaktifkan fitur keamanan tambahan pada akun bisnis mereka selama kegiatan berlangsung. Kegiatan praktik ini menjadi indikator bahwa literasi keamanan digital harus bersifat aplikatif dan tidak cukup hanya melalui penyampaian materi teoretis.

3.2.4 Refleksi Partisipatif

Tahap refleksi dilakukan melalui diskusi terbuka mengenai perubahan perilaku digital peserta. Beberapa perubahan signifikan yang muncul antara lain:

- peserta mulai melakukan verifikasi identitas sebelum transaksi,
- meningkatnya kewaspadaan terhadap tautan mencurigakan,
- kesadaran pentingnya perlindungan data pelanggan.

Pendekatan reflektif memungkinkan peserta memahami bahwa keamanan digital merupakan tanggung jawab individu sekaligus kolektif dalam ekosistem bisnis digital.

3.3 Analisis Hasil Evaluasi Program

Efektivitas pelaksanaan program pengabdian dievaluasi melalui pendekatan kuantitatif dengan membandingkan hasil *pre-test* dan *post-test* yang diperoleh peserta sebelum dan setelah mengikuti pelatihan. Evaluasi ini bertujuan untuk mengukur tingkat keberhasilan program dalam meningkatkan kompetensi literasi keamanan digital. Instrumen evaluasi difokuskan pada tiga aspek utama, yaitu peningkatan pengetahuan mengenai konsep dasar keamanan digital, kemampuan peserta dalam mengidentifikasi berbagai bentuk serangan *social engineering*, serta perubahan perilaku dalam menerapkan praktik keamanan digital pada aktivitas bisnis sehari-hari. Perbandingan hasil *pre-test* dan *post-test* digunakan sebagai indikator untuk menilai efektivitas program sekaligus mengidentifikasi perubahan pengetahuan, kesadaran, dan praktik keamanan digital yang dicapai oleh peserta setelah mengikuti kegiatan.

3.3.1 Peningkatan Pengetahuan

Hasil evaluasi menunjukkan bahwa pelaksanaan program memberikan dampak positif terhadap peningkatan pengetahuan peserta mengenai keamanan digital. Berdasarkan hasil *pre-test* dan *post-test*, rata-rata skor pengetahuan peserta meningkat dari 54,3 menjadi 84,7 atau mengalami kenaikan sebesar 30,4 poin. Peningkatan tersebut menunjukkan bahwa materi pelatihan yang disampaikan mampu meningkatkan pemahaman peserta terhadap konsep dasar keamanan digital, berbagai bentuk ancaman siber, serta pentingnya penerapan praktik keamanan dalam aktivitas bisnis berbasis digital. Temuan ini mengindikasikan bahwa pendekatan edukasi yang disesuaikan dengan konteks dan kebutuhan UMKM lebih efektif dalam meningkatkan literasi keamanan digital dibandingkan penyampaian materi yang bersifat umum.

3.3.2 Peningkatan Kemampuan Identifikasi Ancaman

Selain meningkatkan pengetahuan, program ini juga berhasil meningkatkan kemampuan peserta dalam mengenali berbagai bentuk serangan *social engineering*. Sebelum mengikuti pelatihan, hanya 41% peserta yang mampu mengidentifikasi pesan *phishing* dengan benar, sedangkan setelah pelatihan jumlah tersebut meningkat menjadi 87%. Hasil ini menunjukkan bahwa penggunaan metode simulasi berbasis kasus nyata memberikan pengalaman belajar yang lebih kontekstual sehingga peserta tidak hanya memahami konsep secara teoretis, tetapi juga mampu mengenali karakteristik ancaman siber yang berpotensi terjadi dalam aktivitas bisnis sehari-hari. Dengan demikian, simulasi menjadi salah satu strategi pembelajaran yang efektif dalam meningkatkan *security awareness* pelaku UMKM.

3.3.3 Perubahan Perilaku Keamanan Digital

Perubahan perilaku peserta menjadi salah satu indikator utama keberhasilan program pengabdian. Hasil evaluasi menunjukkan adanya peningkatan penerapan praktik keamanan digital setelah pelatihan, yang ditunjukkan oleh meningkatnya penggunaan kata sandi yang unik pada setiap akun bisnis dari 28% menjadi 81%, aktivasi autentikasi dua faktor (*Two-Factor Authentication*) dari 12% menjadi 90%, serta meningkatnya kebiasaan melakukan verifikasi transaksi sebelum memberikan informasi penting hingga mencapai 85% peserta. Perubahan tersebut menunjukkan bahwa kegiatan pengabdian tidak hanya meningkatkan pengetahuan peserta, tetapi juga mendorong terbentuknya perilaku yang lebih aman dalam memanfaatkan teknologi digital. Hasil ini sejalan dengan laporan Verizon (2023) yang

menyatakan bahwa pengurangan kesalahan manusia (*human error*) merupakan salah satu strategi utama dalam mitigasi risiko keamanan siber, sehingga peningkatan kesadaran dan perubahan perilaku pengguna menjadi faktor penting dalam membangun ketahanan siber UMKM.

3.4 Dampak Program terhadap Ketahanan Siber UMKM

Hasil pelaksanaan kegiatan menunjukkan bahwa program literasi keamanan digital memberikan dampak positif terhadap peningkatan ketahanan siber pelaku UMKM. Dampak tersebut terlihat pada tiga dimensi utama, yaitu individu, organisasi, dan komunitas. Pada tingkat individu, peserta mengalami peningkatan pengetahuan, kesadaran, dan kepercayaan diri dalam memanfaatkan teknologi digital secara lebih aman. Peserta tidak lagi hanya berperan sebagai pengguna teknologi, tetapi juga memiliki kemampuan untuk mengenali berbagai risiko keamanan digital serta menerapkan langkah-langkah pencegahan dalam aktivitas bisnis sehari-hari. Pada tingkat organisasi, pelaku UMKM mulai menerapkan berbagai praktik keamanan digital, seperti penyusunan prosedur operasional standar (SOP) untuk transaksi daring, pembatasan hak akses administrator pada akun bisnis, serta pengelolaan dan penyimpanan data pelanggan secara lebih aman. Sementara itu, pada tingkat komunitas, peserta menunjukkan peran aktif sebagai agen literasi keamanan digital dengan membagikan pengetahuan dan pengalaman yang diperoleh selama pelatihan kepada rekan usaha maupun komunitas UMKM lainnya. Kondisi tersebut menunjukkan bahwa program pengabdian tidak hanya memberikan manfaat bagi peserta secara individual, tetapi juga menciptakan efek multiplikasi (*knowledge diffusion*) yang berpotensi memperluas budaya keamanan digital di lingkungan UMKM secara berkelanjutan.

3.5 Diskusi Akademik dan Kebaruan Program

Kebaruan utama kegiatan ini terletak pada pengembangan UMKM Cyber Awareness Framework, yang mengintegrasikan edukasi konseptual, simulasi praktik nyata, perubahan perilaku berkelanjutan, dan evaluasi kuantitatif dampak pelatihan.

Berbeda dengan program literasi digital sebelumnya yang berfokus pada penggunaan teknologi, pendekatan ini menempatkan keamanan digital sebagai kompetensi inti transformasi digital UMKM. Pendekatan berbasis PAR juga terbukti meningkatkan partisipasi aktif peserta, karena pelaku UMKM dilibatkan dalam seluruh siklus pembelajaran. Model ini selaras dengan

konsep pembelajaran sosial yang menekankan pengalaman langsung sebagai faktor utama perubahan perilaku.

Secara akademik, hasil pengabdian memperkuat argumentasi bahwa strategi keamanan siber modern harus mengintegrasikan aspek manusia, teknologi, dan budaya organisasi. Dengan kata lain, keamanan digital bukan sekadar persoalan sistem, tetapi juga persoalan literasi dan kesadaran pengguna.

3.6 Implikasi Praktis dan Rekomendasi

Berdasarkan hasil pelaksanaan program, beberapa rekomendasi strategis dapat dirumuskan untuk mendukung keberlanjutan peningkatan literasi keamanan digital pada pelaku UMKM. Program literasi keamanan digital perlu dilaksanakan secara berkelanjutan sebagai bagian dari kegiatan pendampingan UMKM agar kesadaran dan perilaku keamanan digital peserta tetap terpelihara serta mampu beradaptasi dengan perkembangan ancaman siber. Pemerintah daerah juga diharapkan dapat mengintegrasikan pelatihan keamanan siber ke dalam program pembinaan dan inkubasi UMKM sebagai upaya memperkuat kapasitas pelaku usaha dalam menghadapi risiko digital. Selain itu, perguruan tinggi perlu berperan aktif dalam mengembangkan program pengabdian kepada masyarakat yang berfokus pada peningkatan *cyber awareness* melalui kegiatan edukasi, pelatihan, dan pendampingan yang berkelanjutan. Model *UMKM Cyber Awareness Framework* yang dikembangkan dalam kegiatan ini juga memiliki potensi untuk direplikasi dan diadaptasi pada berbagai sektor usaha lainnya, seperti ekonomi kreatif, kesehatan digital, maupun sektor lain yang memanfaatkan teknologi digital dalam proses bisnisnya. Dengan demikian, penguatan literasi dan keamanan digital di kalangan UMKM diharapkan dapat menjadi salah satu strategi penting dalam meningkatkan ketahanan siber serta mendukung keberlanjutan transformasi ekonomi digital nasional.

Meskipun program pengabdian ini menunjukkan hasil yang positif dalam meningkatkan literasi keamanan digital dan kesadaran peserta terhadap ancaman siber, masih terdapat beberapa keterbatasan yang perlu menjadi perhatian. Jumlah peserta yang terlibat masih relatif terbatas sehingga hasil kegiatan belum dapat digeneralisasikan pada populasi UMKM yang lebih luas. Selain itu, durasi pelatihan yang singkat membatasi kesempatan peserta untuk mendalami seluruh materi dan menerapkan praktik keamanan digital secara lebih komprehensif. Evaluasi yang dilakukan juga hanya mengukur perubahan pengetahuan dan perilaku dalam jangka pendek, sehingga keberlanjutan penerapan praktik keamanan digital oleh peserta belum dapat diketahui secara menyeluruh. Oleh karena itu, kegiatan pengabdian

selanjutnya disarankan melibatkan jumlah peserta yang lebih besar, memperpanjang durasi pendampingan, serta melakukan evaluasi secara berkala untuk mengukur konsistensi perubahan perilaku dan keberlanjutan implementasi praktik keamanan digital dalam aktivitas bisnis UMKM.

3.7 Sintesis Hasil Pengabdian

Secara keseluruhan, kegiatan pengabdian kepada masyarakat ini menunjukkan bahwa implementasi literasi keamanan digital berbasis pendekatan partisipatif memberikan dampak signifikan terhadap peningkatan kapasitas keamanan siber pelaku Usaha Mikro Kecil dan Menengah (UMKM). Dampak tersebut tidak hanya terlihat pada aspek peningkatan pengetahuan, tetapi juga mencakup perubahan perilaku serta terbentuknya budaya keamanan digital yang berkelanjutan.

3.7.1 Peningkatan Pengetahuan Keamanan Siber UMKM

Hasil evaluasi menunjukkan adanya peningkatan pemahaman peserta terkait konsep dasar keamanan digital, jenis ancaman siber, serta strategi mitigasi risiko keamanan informasi. Sebelum pelatihan, mayoritas peserta memandang keamanan digital sebagai isu teknis yang hanya relevan bagi perusahaan besar atau organisasi berbasis teknologi. Namun setelah mengikuti program literasi, peserta mulai memahami bahwa keamanan siber merupakan bagian integral dari manajemen bisnis modern.

Peningkatan pengetahuan terlihat dari kemampuan peserta dalam:

- menjelaskan karakteristik serangan *phishing* dan *social engineering*,
- memahami pentingnya autentikasi berlapis,
- mengenali risiko kebocoran data pelanggan,
- memahami konsekuensi finansial dan reputasi akibat pelanggaran keamanan.

Pendekatan pembelajaran partisipatif memungkinkan peserta mengaitkan materi keamanan dengan pengalaman bisnis nyata mereka. Hal ini memperkuat proses internalisasi pengetahuan karena peserta tidak hanya menerima informasi secara pasif, tetapi terlibat aktif dalam proses refleksi dan diskusi kasus. Dengan demikian, literasi keamanan digital berperan sebagai fondasi awal dalam membangun kesadaran risiko (*risk awareness*) yang sebelumnya belum dimiliki oleh sebagian besar pelaku UMKM.

3.7.2 Pengurangan Kerentanan terhadap Serangan *Social Engineering*

Temuan penting dari kegiatan pengabdian ini adalah menurunnya tingkat kerentanan peserta terhadap teknik *social engineering*. Sebagaimana diketahui, sebagian besar serangan

siber modern tidak lagi mengandalkan eksploitasi teknis sistem, melainkan manipulasi psikologis terhadap pengguna.

Melalui simulasi serangan yang dirancang menyerupai kondisi nyata, peserta diperlihatkan bagaimana pelaku kejahatan memanfaatkan rasa urgensi, otoritas palsu, kepercayaan sosial, serta ketidaktahuan pengguna. Sebelum pelatihan, banyak peserta cenderung langsung merespons pesan yang mengatasnamakan *marketplace*, bank digital, atau pelanggan potensial tanpa melakukan verifikasi keamanan. Setelah program berlangsung, terjadi perubahan signifikan pada pola pengambilan keputusan peserta. Peserta mulai menunjukkan perilaku keamanan baru, seperti:

- melakukan verifikasi identitas pengirim,
- tidak membagikan kode OTP,
- memeriksa URL sebelum login,
- menolak permintaan akses akun yang mencurigakan.

Perubahan ini menegaskan bahwa pendekatan *experiential learning* melalui simulasi merupakan strategi efektif dalam membangun *cyber risk perception*. Artinya, peserta tidak hanya mengetahui ancaman secara teoritis, tetapi mampu mengenali pola manipulasi dalam situasi nyata.

3.7.3 Pembentukan Budaya Keamanan Digital pada UMKM

Dampak paling strategis dari kegiatan ini adalah terbentuknya embrio budaya keamanan digital (*digital security culture*) pada lingkungan UMKM. Budaya keamanan digital mengacu pada kebiasaan kolektif individu dalam menjaga keamanan informasi secara konsisten sebagai bagian dari aktivitas kerja sehari-hari.

Program pengabdian tidak hanya berfokus pada peningkatan kemampuan individu, tetapi juga mendorong transformasi praktik bisnis UMKM. Beberapa indikator terbentuknya budaya keamanan digital antara lain:

- penerapan password berbeda pada setiap akun bisnis,
- pembatasan akses admin media sosial,
- penyimpanan data pelanggan secara lebih terstruktur,
- kesadaran melakukan backup data secara berkala,
- diskusi keamanan digital antar anggota tim usaha.

Menariknya, beberapa peserta mulai berperan sebagai agen literasi keamanan digital di komunitasnya. Mereka menyebarkan kembali pengetahuan yang diperoleh kepada karyawan,

mitra bisnis, maupun komunitas UMKM lainnya. Fenomena ini menunjukkan adanya efek diseminasi sosial yang memperluas dampak pengabdian di luar kelompok sasaran awal.

Budaya keamanan digital menjadi aspek penting karena keamanan siber yang berkelanjutan tidak dapat bergantung pada teknologi semata, tetapi harus tertanam dalam perilaku organisasi.

3.7.4 Validasi Pendekatan *Human-Centered Cybersecurity*

Hasil kegiatan pengabdian ini menegaskan relevansi pendekatan *human-centered cybersecurity*, yaitu paradigma keamanan siber yang menempatkan manusia sebagai elemen utama sistem keamanan informasi. Pendekatan ini berangkat dari asumsi bahwa sebagian besar insiden keamanan berasal dari kesalahan manusia (*human error*), bukan kegagalan teknologi. Melalui pendekatan partisipatif, peserta dilibatkan dalam seluruh siklus pembelajaran mulai dari identifikasi masalah, praktik simulasi, hingga refleksi pengalaman. Keterlibatan aktif tersebut terbukti mampu meningkatkan rasa kepemilikan (*sense of ownership*) terhadap praktik keamanan digital.

Pendekatan *human-centered* menghasilkan beberapa keuntungan strategis berupa meningkatkan kesadaran risiko secara berkelanjutan, memperkuat kemampuan pengambilan keputusan digital, mengurangi ketergantungan terhadap solusi teknologi mahal, dan menciptakan sistem pertahanan keamanan berbasis perilaku pengguna. Dalam konteks transformasi digital nasional, pendekatan ini sangat relevan bagi UMKM yang memiliki keterbatasan sumber daya teknologi. Alih-alih mengandalkan infrastruktur keamanan kompleks, penguatan kapasitas manusia menjadi strategi mitigasi risiko yang lebih adaptif dan berkelanjutan.

3.7.5 Implikasi terhadap Ketahanan Siber UMKM di Era Transformasi Digital

Transformasi digital mendorong UMKM untuk semakin terkoneksi dengan ekosistem ekonomi berbasis data. Kondisi ini secara simultan meningkatkan peluang bisnis sekaligus eksposur terhadap ancaman siber.

Hasil pengabdian menunjukkan bahwa literasi keamanan digital mampu meningkatkan *cyber resilience* atau ketahanan siber UMKM melalui tiga lapisan utama:

- Lapisan individu, yaitu meningkatnya kesadaran dan kompetensi keamanan pengguna;
- Lapisan organisasi, yaitu penerapan prosedur keamanan sederhana dalam operasional bisnis;
- Lapisan komunitas, yaitu terbentuknya jaringan edukasi keamanan digital antar pelaku usaha.

Dengan demikian, kegiatan pengabdian masyarakat tidak hanya berfungsi sebagai transfer pengetahuan, tetapi juga sebagai intervensi sosial yang memperkuat ekosistem keamanan digital berbasis komunitas.

Secara keseluruhan, hasil pelaksanaan program menunjukkan bahwa peningkatan literasi keamanan digital melalui pendekatan partisipatif memberikan dampak positif terhadap peningkatan kapasitas pelaku UMKM dalam menghadapi berbagai ancaman siber. Program ini berhasil meningkatkan kompetensi peserta dalam memahami konsep keamanan digital, memperkuat kemampuan mereka dalam mengidentifikasi dan mengantisipasi serangan *social engineering*, serta mendorong penerapan praktik keamanan digital yang lebih baik dalam aktivitas bisnis sehari-hari. Selain itu, kegiatan ini juga berkontribusi dalam membangun budaya keamanan digital yang berkelanjutan melalui peningkatan kesadaran, perubahan perilaku, dan penyebaran pengetahuan kepada komunitas UMKM yang lebih luas. Temuan tersebut menunjukkan bahwa upaya penguatan keamanan siber tidak hanya bergantung pada pemanfaatan teknologi, tetapi juga memerlukan pengembangan kapasitas sumber daya manusia, pembentukan perilaku yang sadar akan risiko keamanan, serta pembelajaran partisipatif yang berkelanjutan sebagai fondasi utama dalam meningkatkan ketahanan siber UMKM di era ekonomi digital. Dokumentasi kegiatan diberikan dalam Gambar 1.



Gambar 1. Dokumentasi kegiatan pengabdian kepada masyarakat

4. Kesimpulan

Kegiatan pengabdian kepada masyarakat melalui implementasi UMKM *Cyber Awareness Framework* terbukti efektif dalam meningkatkan literasi keamanan digital pelaku Usaha Mikro Kecil dan Menengah (UMKM) di era transformasi digital. Program yang dilaksanakan menggunakan pendekatan *Participatory Action Research* (PAR) mampu mengintegrasikan proses edukasi, praktik langsung, serta refleksi partisipatif sehingga menghasilkan perubahan pengetahuan, sikap, dan perilaku keamanan digital secara signifikan. Hasil evaluasi menunjukkan adanya peningkatan nyata tingkat literasi keamanan digital peserta, ditunjukkan melalui kenaikan skor rata-rata dari 53,2 sebelum pelatihan menjadi 87,4 setelah pelaksanaan kegiatan.

Peningkatan ini tidak hanya terjadi pada aspek pemahaman konseptual, tetapi juga pada kemampuan praktis peserta dalam mengidentifikasi ancaman social engineering, menerapkan autentikasi dua faktor, menggunakan password yang aman, serta melakukan perlindungan data pelanggan secara lebih sistematis. Temuan ini menegaskan bahwa pendekatan pembelajaran berbasis pengalaman dan simulasi nyata mampu memperkuat internalisasi kesadaran keamanan siber pada pelaku UMKM. Dampak program pengabdian terlihat pada tiga dimensi utama. Pertama, pada level individu terjadi peningkatan kepercayaan diri dan kesadaran risiko digital sehingga pelaku UMKM tidak lagi menjadi pengguna teknologi yang pasif, tetapi menjadi pengguna yang sadar keamanan. Kedua, pada level organisasi bisnis mulai terbentuk praktik keamanan operasional seperti penerapan SOP transaksi online, pembatasan akses akun admin, serta pengelolaan data pelanggan secara aman. Ketiga, pada level komunitas muncul efek multiplikasi pengetahuan di mana peserta berperan sebagai agen literasi keamanan digital di lingkungan usaha masing-masing. Secara akademik, kegiatan ini memperkuat paradigma bahwa keamanan siber modern tidak hanya bergantung pada teknologi, tetapi harus mengintegrasikan aspek manusia, perilaku, dan budaya organisasi sebagai fondasi utama sistem keamanan digital.

Pendekatan *human-centered cybersecurity* menjadi strategi yang lebih adaptif bagi UMKM yang memiliki keterbatasan sumber daya teknologi namun membutuhkan ketahanan siber yang berkelanjutan. Selain memberikan kontribusi praktis berupa peningkatan kompetensi keamanan digital, program ini juga menghasilkan model edukasi keamanan digital yang sistematis, aplikatif, dan berpotensi direplikasi secara nasional pada berbagai komunitas UMKM. Dengan demikian, kegiatan pengabdian masyarakat tidak hanya berfungsi sebagai

transfer pengetahuan, tetapi juga sebagai intervensi sosial strategis dalam memperkuat ekosistem ekonomi digital yang aman, inklusif, dan berkelanjutan. Meskipun menunjukkan hasil positif, kegiatan ini masih memiliki keterbatasan pada jumlah peserta, durasi pelatihan yang relatif singkat, serta belum dilakukannya evaluasi perilaku keamanan digital dalam jangka panjang. Oleh karena itu, penelitian dan program pengabdian lanjutan diperlukan untuk mengukur keberlanjutan perubahan perilaku serta memperluas implementasi framework pada sektor ekonomi digital lainnya. Secara keseluruhan, penguatan literasi keamanan digital melalui pendekatan partisipatif terbukti mampu meningkatkan ketahanan siber UMKM, menurunkan kerentanan terhadap serangan social engineering, serta membangun budaya keamanan digital sebagai kompetensi inti dalam menghadapi dinamika transformasi ekonomi digital nasional.

Daftar Referensi

- Abrardi, L., Comino, S. & Grassini, S. (2026). The economics of cyber risk: a survey of the literature. *Journal of Industrial and Business Economics*, 53, 573–607. <https://doi.org/10.1007/s40812-025-00370-3>
- Admass, W.S., Munaye, Y.Y. & Diro, A.A. (2024). Cyber security: State of the art, challenges and future directions. *Cyber Security and Applications*, 2, 100031. <https://doi.org/10.1016/j.csa.2023.100031>.
- Agustin, S. (2024). Dampak Kemajuan Teknologi Informasi Era Digital Terhadap Keamanan Data Pribadi Tantangan Dan Penanggulangan Terhadap Kejahatan Cyber. *Jurnal Penelitian Multidisiplin Bangsa*, 1(6), 500–504. <https://doi.org/10.59837/jpnmb.v1i6.93>
- Anggita, W., Manik, J.D.N. & Zaliman, I. (2025). Mitigasi Ancaman Social Engineering Bagi UMKM Melalui Program Sosialisasi di Kota Pangkalpinang. *Jurnal Abdimas Ilmiah Citra Bakti*, 6(1), 319-328.
- Angraini, D., Riady, Y., Putimasurai, P., Pratama, A., Sadria, A. & Rosmiati, R. (2024). Transformasi Digital Dalam Meningkatkan Daya Saing Usaha Mikro, Kecil, Dan Menengah (UMKM) Indonesia: Sebuah Tinjauan Sistematis. *EKLETIK : Jurnal Pendidikan Ekonomi dan Kewirausahaan*, 7(2), 132-142.
- Ayu, D.P., Suryanto, J.D., Afriyanto, G., Ulfah, F., & Soleh, A. (2026). Digital Transformation of MSMEs as a Competitiveness Enhancement Strategy in the Digital Economy Era. *TOFEDU: The Future of Education Journal*, 5(2), 2157–2162. <https://doi.org/10.61445/tofedu.v5i2.1823>
- Colabianchi, S., Costantino, F., Nonino, F. & Palombi, G. (2025). Transforming threats into opportunities: The role of human factors in enhancing cybersecurity. *Journal of Innovation*

& Knowledge, 10(3), 100695. <https://doi.org/10.1016/j.jik.2025.100695>

Fizzanty, T. (2024). 'Digitalization of Indonesian MSMEs: Innovation Challenges and Opportunities' dalam Fizzanty, T., Maulana, I. (eds) The Digitalization of Indonesian Small and Medium Enterprises. Engaging Indonesia. *Springer*, Singapore. https://doi.org/10.1007/978-981-97-0029-5_2

Hadnagy, C. (2018). Social Engineering: The Science of Human Hacking (2nd ed.). *Wiley Publishing*.

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

Kemmis, S., & McTaggart, R. (2014). The Action Research Planner: Doing Critical Participatory Action Research. *Springer*.

Masmoudi, S. (2025). 'Unveiling the Human Factor in Cybercrime and Cybersecurity: Motivations, Behaviors, Vulnerabilities, Mitigation Strategies, and Research Methods' dalam Chawki, M., Abraham, A. (eds). Cybercrime Unveiled: Technologies for Analysing Legal Complexity. Studies in Computational Intelligence, vol 1181. *Springer*, Cham. https://doi.org/10.1007/978-3-031-80557-8_3

Meilariza, R., Delima, Z.M. & Zuliyati, Z. (2024). Digitalization of Micro, Small, and Medium Enterprises (MSMEs) in Indonesia. *KnE Social Sciences*, 9(18), 245–257. <https://doi.org/10.18502/kss.v9i17.16334>

Morisson, B., & Fikri, A.A.H.S. (2025). Digitalisasi UMKM sebagai Strategi Meningkatkan Daya Saing di Era Ekonomi Digital. EBISNIS (*Jurnal Ilmiah Ekonomi dan Bisnis*), 18(1), 289-299.

Mutiarani, M., Royani, N., Mitasari, D., Masitoh, G. & Fitri, T.I. (2025). Analisis Dampak Digitalisasi UMKM Terhadap Pertumbuhan Ekonomi Lokal di Indonesia. JSE: *Jurnal Sharia Economica*, 4(2), 51-62. <https://doi.org/10.46773/jse.v4i2.1879>