



## **Manajemen Krisis dan Prosedur Pelaporan: Langkah Tanggap bagi Korban Penipuan Digital untuk Meminimalkan Kerugian**

### ***Crisis Management and Reporting Procedures: Responsive Steps for Digital Fraud Victims to Minimize Losses***

**Dwinanda Marsya Tealova<sup>1</sup>, Ceyzha Putri Tarita<sup>2</sup>, Destia Riyanti<sup>3</sup>, Jamaludin<sup>4</sup>**

Fakultas Ekonomi dan Bisnis, Universitas Pamulang

Email : tealovaaa@gmail.com<sup>1</sup>, dosen01020@unpam.ac.id

#### **Article Info**

##### **Article history:**

Received : 02-07-2026

Revised : 04-07-2026

Accepted : 06-07-2026

Published : 08-07-2026

#### **Abstract**

*The rapid development of artificial intelligence (AI) technology has had a dual impact on society. While facilitating daily activities, it has also opened up opportunities for criminals to launch increasingly sophisticated and difficult-to-detect digital fraud schemes. The female members of the Majelis Ta'lim Auladina on Jl. Masjid Daruttaqwa, Gg. Perin, Depok, are among the vulnerable groups. Although accustomed to using digital financial services in their daily lives, most lack adequate knowledge on how to recognize AI-based digital fraud schemes, take appropriate emergency response steps, or learn official reporting procedures to the authorities. This Community Service (PKM) activity aimed to provide counseling and practical training to the Majelis Ta'lim Auladina members on crisis management and reporting procedures for victims of digital fraud. The methods used included interactive counseling, real-life case simulations, and communicative and easy-to-understand question-and-answer sessions. The results of this activity demonstrated an increased understanding of the participants regarding various AI-based digital fraud schemes, their readiness to take emergency action when facing indications of fraud, and their understanding of accessible official reporting channels. By increasing the participants' digital financial literacy, it is hoped that family economic stability can be better protected from the increasingly rampant threat of cybercrime.*

**Keywords:** *digital fraud, artificial intelligence, crisis management*

#### **Abstrak**

Perkembangan teknologi kecerdasan buatan (AI) yang begitu pesat telah membawa dampak ganda bagi masyarakat. Di satu sisi memudahkan aktivitas sehari-hari, namun di sisi lain membuka celah bagi pelaku kejahatan untuk melancarkan aksi penipuan digital yang semakin canggih dan sulit dideteksi. Ibu-ibu anggota Majelis Ta'lim Auladina di Jl. Masjid Daruttaqwa, Gg. Perin, Depok merupakan salah satu kelompok masyarakat yang rentan terhadap ancaman ini. Meski sudah terbiasa menggunakan layanan keuangan digital dalam keseharian mereka, sebagian besar belum memiliki pengetahuan yang memadai tentang cara mengenali modus penipuan digital berbasis AI, mengambil langkah tanggap darurat yang tepat, maupun prosedur pelaporan resmi kepada pihak berwenang. Kegiatan Pengabdian Kepada Masyarakat (PKM) ini dilaksanakan dengan tujuan memberikan penyuluhan dan pelatihan praktis kepada ibu-ibu Majelis Ta'lim Auladina terkait manajemen krisis dan prosedur pelaporan bagi korban penipuan digital. Metode yang digunakan meliputi penyuluhan interaktif, simulasi kasus nyata, serta sesi tanya jawab yang komunikatif dan mudah dipahami. Hasil dari kegiatan ini menunjukkan adanya peningkatan pemahaman peserta terhadap berbagai modus penipuan digital berbasis AI, kesiapan dalam mengambil tindakan darurat ketika menghadapi indikasi penipuan, serta pemahaman tentang jalur pelaporan resmi yang dapat diakses. Dengan meningkatnya literasi keuangan digital para peserta, diharapkan stabilitas ekonomi keluarga dapat lebih terlindungi dari ancaman kejahatan siber yang semakin marak.

**Kata Kunci:** *penipuan digital, kecerdasan buatan, manajemen krisis*



## **PENDAHULUAN**

Memasuki era digital yang terus berkembang, teknologi kecerdasan buatan atau Artificial Intelligence (AI) sudah menjadi bagian dari kehidupan masyarakat sehari-hari, termasuk dalam pengelolaan keuangan keluarga. Namun seiring dengan kemudahan yang ditawarkan, ancaman kejahatan digital berbasis AI pun semakin nyata dan sulit dikenali. Pelaku penipuan kini mampu menciptakan suara palsu yang menyerupai suara orang-orang terdekat korban menggunakan teknologi deepfake audio, memanipulasi video lewat kecerdasan buatan, hingga menyebarkan pesan phishing yang dibuat tampak sangat meyakinkan. Kondisi ini menjadi ancaman serius, terutama bagi kelompok masyarakat yang tingkat literasi digitalnya masih terbatas.

Ibu-ibu anggota Majelis Ta'lim Auladina yang berlokasi di Jl. Masjid Daruttaqwa, Gg. Perin, Depok merupakan salah satu komunitas yang aktif dan memiliki jaringan sosial luas di lingkungannya. Komunitas ini sudah berdiri sejak tahun 2012 dan memiliki kegiatan rutin berupa pengajian berkala yang mempererat hubungan antar anggota. Dalam keseharian, para anggota sudah cukup familiar menggunakan layanan keuangan digital seperti mobile banking, dompet digital, hingga platform belanja online. Akan tetapi, berdasarkan observasi awal yang dilakukan tim pelaksana, ditemukan bahwa pemahaman mereka tentang cara mengenali, menghadapi, dan melaporkan kasus penipuan digital masih sangat minim.

Banyak anggota yang belum mengetahui bagaimana cara kerja teknologi AI yang kini dimanfaatkan oleh para pelaku penipuan. Di sisi lain, ketika menghadapi dugaan penipuan atau kebocoran data keuangan, mereka tidak memiliki gambaran langkah apa yang harus segera diambil. Persoalan ini semakin diperparah oleh rendahnya pemahaman terhadap jalur pelaporan resmi yang tersedia, sehingga banyak kasus penipuan yang akhirnya tidak pernah ditangani secara hukum dan korban pun terus menanggung kerugian sendiri.

## **TINJAUAN PUSTAKA**

### **Penipuan Digital Berbasis Kecerdasan Buatan (AI)**

Penipuan digital berbasis kecerdasan buatan merupakan tindak kejahatan siber yang memanfaatkan teknologi AI untuk menipu korban dengan cara yang semakin canggih dan sulit dideteksi. Menurut Kementerian Komunikasi dan Informatika (2023), kejahatan siber berbasis AI terus meningkat seiring dengan semakin mudahnya akses terhadap berbagai perangkat teknologi canggih oleh masyarakat umum. Salah satu bentuk yang paling meresahkan adalah teknologi deepfake, yaitu manipulasi suara atau video yang dibuat sedemikian rupa sehingga tampak nyata dan meyakinkan.

Selain deepfake, modus lain yang banyak digunakan adalah pesan phishing yang dirancang dengan bantuan AI sehingga tampilannya sangat profesional dan tampak berasal dari lembaga keuangan resmi. Para pelaku juga memanfaatkan AI untuk menciptakan robot percakapan (chatbot) yang mampu berkomunikasi layaknya manusia nyata guna mengelabui calon korban. Tingkat kecanggihan ini membuat kelompok masyarakat yang literasi digitalnya masih rendah menjadi sasaran yang sangat mudah dijangkau oleh para pelaku kejahatan.

Prasetyo (2023) menjelaskan bahwa perkembangan teknologi deepfake tidak hanya mengancam individu secara finansial, tetapi juga membahayakan reputasi dan kepercayaan publik secara lebih luas. Manipulasi konten digital yang semakin mudah dilakukan membuat verifikasi



kebenaran informasi menjadi tantangan tersendiri bagi masyarakat. Oleh karena itu, pemahaman tentang jenis-jenis ancaman ini menjadi langkah pertama yang sangat krusial dalam upaya perlindungan diri dari kejahatan digital.

Dalam konteks Indonesia, laporan BSSN (2023) mencatat peningkatan signifikan dalam jumlah insiden siber yang dilaporkan, dengan penipuan digital menjadi salah satu kategori yang paling banyak terjadi. Hal ini menunjukkan urgensi edukasi dan literasi digital yang harus diberikan kepada seluruh lapisan masyarakat, tidak terkecuali kelompok ibu rumah tangga yang semakin aktif bertransaksi secara digital.

### **Manajemen Krisis dalam Konteks Penipuan Digital**

Manajemen krisis merupakan serangkaian tindakan yang direncanakan dan dilaksanakan secara sistematis untuk menghadapi situasi darurat dengan tujuan meminimalkan kerugian dan memulihkan kondisi sesegera mungkin. Dalam konteks penipuan digital, manajemen krisis mencakup kemampuan seseorang untuk tetap tenang, berpikir jernih, dan mengambil langkah-langkah yang tepat dalam waktu singkat ketika menyadari dirinya menjadi target atau korban penipuan.

Hariyanto (2022) menyatakan bahwa respons cepat dalam situasi penipuan digital sangat menentukan seberapa besar kerugian yang akan diderita korban. Semakin cepat seseorang menyadari adanya penipuan dan mengambil tindakan pencegahan seperti memblokir rekening, mengganti kata sandi, atau menghubungi pihak bank, maka semakin kecil peluang pelaku untuk menguras aset korban lebih jauh. Oleh karena itu, pembekalan tentang manajemen krisis menjadi sangat penting agar masyarakat tidak panik dan tahu harus berbuat apa saat menghadapi situasi tersebut.

Tahapan manajemen krisis yang efektif dalam penipuan digital meliputi tiga fase utama, yaitu fase pencegahan (prevention), fase respons (response), dan fase pemulihan (recovery). Pada fase pencegahan, individu dibekali dengan kemampuan untuk mengenali tanda-tanda penipuan sebelum kerugian terjadi. Fase respons melibatkan tindakan-tindakan darurat yang harus dilakukan segera setelah penipuan terdeteksi. Sementara itu, fase pemulihan mencakup langkah-langkah untuk memulihkan kondisi keuangan dan psikologis korban setelah peristiwa terjadi.

Widiyanti (2022) menekankan bahwa edukasi tentang manajemen krisis digital harus disampaikan dengan cara yang praktis dan mudah dipahami oleh berbagai kalangan masyarakat. Pendekatan berbasis komunitas terbukti efektif dalam menyebarkan pengetahuan ini karena memanfaatkan jaringan kepercayaan yang sudah ada di antara anggota komunitas. Dengan demikian, pemahaman tentang manajemen krisis tidak hanya berhenti pada individu yang hadir dalam pelatihan, tetapi juga dapat tersebar lebih luas melalui jaringan komunitas tersebut.

### **Prosedur Pelaporan Penipuan Digital**

Setelah mengambil langkah tanggap darurat, korban penipuan digital perlu segera melaporkan kejadian yang dialaminya kepada pihak-pihak berwenang agar kasus dapat diproses secara hukum dan pelaku dapat ditindak. Di Indonesia, terdapat beberapa saluran pelaporan resmi yang dapat digunakan oleh korban penipuan digital, antara lain: Otoritas Jasa Keuangan (OJK) melalui hotline 157, Bareskrim Polri melalui platform patrolisiber.id, pihak bank terkait untuk



pemblokiran rekening dan penelusuran transaksi, serta BSSN (Badan Siber dan Sandi Negara) untuk kasus yang berkaitan dengan keamanan siber.

Nugroho (2023) menekankan bahwa banyak korban penipuan digital yang akhirnya tidak melapor karena tidak mengetahui kemana harus mengadu dan menganggap laporannya tidak akan ditindaklanjuti. Padahal, semakin banyak laporan yang masuk, semakin mudah bagi aparat untuk memetakan pola kejahatan dan menangkap pelaku. Pengetahuan tentang prosedur pelaporan yang benar dan efektif karenanya menjadi salah satu komponen terpenting dalam upaya melindungi masyarakat dari kerugian akibat penipuan digital.

Dasar hukum pelaporan kejahatan siber di Indonesia diatur dalam Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016. Undang-undang ini memberikan landasan yang kuat bagi korban untuk melaporkan tindak kejahatan digital dan bagi aparat untuk menindak para pelaku. Pemahaman tentang kerangka hukum ini penting agar korban tidak merasa sendirian dalam menghadapi permasalahan yang dialaminya.

### **Literasi Keuangan Digital**

Literasi keuangan digital dapat diartikan sebagai kemampuan seseorang untuk memahami, mengelola, dan memanfaatkan layanan keuangan digital secara aman dan bijaksana. Otoritas Jasa Keuangan (OJK, 2022) mendefinisikan literasi keuangan sebagai pengetahuan, keterampilan, dan keyakinan yang memengaruhi sikap serta perilaku seseorang dalam meningkatkan kualitas pengambilan keputusan keuangan.

Dalam konteks era digital saat ini, literasi keuangan tidak hanya mencakup pemahaman tentang produk dan layanan keuangan konvensional, tetapi juga kemampuan untuk mengenali potensi ancaman dan risiko yang muncul dalam transaksi digital. Masyarakat yang memiliki tingkat literasi keuangan digital yang baik cenderung lebih waspada terhadap tawaran-tawaran mencurigakan, lebih mampu menjaga kerahasiaan data pribadi, serta lebih sigap dalam mengambil tindakan ketika menemui indikasi penipuan.

Santoso (2022) dalam penelitiannya tentang literasi keuangan digital pada ibu rumah tangga di perkotaan menemukan bahwa kelompok ini memiliki kerentanan yang lebih tinggi terhadap penipuan digital dibandingkan kelompok usia muda, terutama karena kurangnya pengalaman dalam mengenali modus-modus penipuan yang terus berkembang. Penelitian ini juga menunjukkan bahwa intervensi edukasi yang dilakukan dalam format kelompok kecil terbukti lebih efektif dibandingkan penyebaran informasi melalui media massa.

Oleh sebab itu, penguatan literasi keuangan digital menjadi fondasi utama dalam upaya melindungi masyarakat dari kejahatan siber yang semakin marak. Program PKM ini hadir sebagai salah satu bentuk kontribusi nyata dalam meningkatkan literasi keuangan digital di tingkat komunitas, dengan harapan dampaknya dapat dirasakan tidak hanya oleh peserta langsung, tetapi juga oleh keluarga dan lingkungan sekitar mereka

### **METODE PENELITIAN**

Materi yang disampaikan dalam kegiatan penyuluhan ini mencakup tiga topik utama yang saling berkaitan dan dirancang untuk memberikan pemahaman komprehensif kepada peserta:



### 1. Mengenal Modus Penipuan Digital Berbasis AI

Bagian pertama materi membahas tentang berbagai jenis kejahatan digital yang saat ini marak memanfaatkan teknologi kecerdasan buatan. Peserta diajak untuk mengenal cara kerja deepfake audio dan video yang bisa digunakan untuk memalsukan identitas seseorang, mengenali ciri-ciri pesan phishing yang tampak meyakinkan namun sebenarnya merupakan jebakan, serta memahami modus investasi bodong yang dikemas secara profesional menggunakan AI. Materi ini juga menyertakan contoh-contoh kasus nyata yang terjadi di masyarakat agar lebih mudah dipahami dan direlasikan dengan pengalaman sehari-hari peserta.

Sub-materi yang dibahas dalam sesi ini meliputi:

- a. pengertian dan cara kerja teknologi deepfake audio dan video
- b. ciri-ciri pesan phishing dan cara mengenalinya
- c. modus penipuan melalui aplikasi chatbot berbasis AI
- d. penipuan investasi digital yang menggunakan teknologi AI dalam presentasinya
- e. tips dan trik praktis untuk memverifikasi keaslian informasi dan identitas pengirim pesan.

### 2. Langkah Tanggap Darurat bagi Korban Penipuan Digital

Materi kedua berfokus pada tindakan-tindakan yang harus segera dilakukan ketika seseorang menyadari dirinya menjadi korban atau target penipuan digital. Langkah-langkah yang diajarkan antara lain: segera menghubungi bank untuk memblokir rekening dan kartu yang berpotensi disalahgunakan, mengganti kata sandi akun-akun digital penting, mengamankan dan mendokumentasikan bukti-bukti transaksi atau komunikasi yang mencurigakan, serta tidak memberikan informasi pribadi lebih lanjut kepada pihak yang tidak dikenal. Materi ini disampaikan dalam format yang praktis dan mudah diingat agar peserta dapat langsung menerapkannya dalam situasi nyata.

Urutan langkah tanggap darurat yang diajarkan adalah:

- a. Tetap tenang dan jangan terburu-buru mengambil Keputusan.
- b. Segera putuskan komunikasi dengan pelaku.
- c. Hubungi bank melalui nomor resmi untuk melakukan pemblokiran.
- d. Ganti semua kata sandi akun digital yang berpotensi diketahui pelaku.
- e. Kumpulkan dan simpan semua bukti komunikasi dan transaksi.
- f. Laporkan kepada pihak berwenang.
- g. Informasikan kepada keluarga dan orang-orang terdekat untuk mencegah korban tambahan.

### 3. Prosedur Pelaporan Resmi

Materi ketiga menjelaskan secara rinci tentang saluran-saluran pelaporan resmi yang dapat diakses oleh korban penipuan digital. Peserta diberikan informasi tentang cara menghubungi OJK melalui hotline 157, cara melaporkan kejahatan siber melalui platform patrolisiber.id milik Bareskrim Polri, prosedur pengaduan kepada pihak bank, serta informasi kontak lembaga-lembaga terkait lainnya. Panduan ini juga dikemas dalam bentuk modul yang bisa dibawa pulang oleh peserta untuk dipelajari kembali di rumah.

Tabel panduan pelaporan yang diberikan kepada peserta mencakup informasi lengkap tentang: nama lembaga, nomor kontak/hotline, platform digital yang tersedia, dokumen yang



perlu disiapkan, serta estimasi waktu penanganan. Informasi ini disederhanakan sedemikian rupa agar mudah dipahami dan diingat oleh peserta dengan berbagai latar belakang pendidikan.

### **Khalayak Sasaran**

Sasaran kegiatan PKM ini adalah ibu-ibu anggota Majelis Ta'lim Auladina di Jl. Masjid Daruttaqwa, Gg. Perin, Depok. Komunitas ini dipilih berdasarkan beberapa pertimbangan yang matang. Pertama, para anggotanya sudah aktif menggunakan layanan keuangan digital namun belum memiliki pemahaman yang cukup tentang keamanan digital. Kedua, komunitas ini memiliki jaringan sosial yang luas sehingga pemahaman yang diperoleh dapat tersebar lebih jauh ke masyarakat sekitar. Ketiga, adanya kepercayaan yang kuat di antara sesama anggota menjadikan forum ini tempat yang ideal untuk kegiatan edukasi berbasis komunitas.

Peserta yang hadir dalam kegiatan ini berjumlah sekitar 15 orang ibu-ibu yang merupakan anggota aktif Majelis Ta'lim Auladina. Mereka berasal dari berbagai latar belakang pekerjaan dan tingkat pendidikan yang beragam, sehingga penyampaian materi dirancang untuk dapat dipahami oleh semua kalangan tanpa memandang latar belakang pendidikan formal mereka

## **HASIL DAN PEMBAHASAN**

### **Hasil Kegiatan**

Kegiatan penyuluhan literasi keuangan digital dengan tema manajemen krisis dan prosedur pelaporan bagi korban penipuan digital telah berhasil dilaksanakan dengan baik dan lancar di lingkungan Majelis Ta'lim Auladina, Depok. Secara keseluruhan, kegiatan ini memberikan hasil yang positif, yang dapat dirangkum dalam beberapa poin berikut:

#### **1. Peningkatan Pemahaman tentang Modus Penipuan Digital**

Sebelum kegiatan dilaksanakan, sebagian besar peserta mengaku belum pernah mendengar istilah deepfake dan belum memahami bagaimana teknologi AI bisa dimanfaatkan untuk melancarkan aksi penipuan. Setelah sesi penyuluhan selesai, peserta terlihat antusias mendiskusikan contoh-contoh kasus yang dipaparkan dan mulai menyadari bahwa beberapa situasi yang pernah mereka alami atau dengar sebenarnya merupakan indikasi penipuan digital. Meningkatnya partisipasi aktif peserta dalam sesi diskusi dan tanya jawab menjadi salah satu indikator nyata adanya peningkatan pemahaman tersebut.

#### **2. Kesiapan Tindakan Tanggap Darurat**

Setelah pemaparan materi tentang langkah-langkah tanggap darurat, peserta mendapatkan gambaran yang lebih jelas tentang apa yang harus mereka lakukan ketika menghadapi situasi darurat akibat penipuan digital. Simulasi kasus yang dilakukan selama sesi berlangsung membantu peserta untuk mempraktikkan langkah-langkah tersebut secara langsung, mulai dari cara memblokir rekening melalui aplikasi mobile banking hingga cara mengumpulkan bukti transaksi yang mencurigakan. Hal ini penting agar ketika situasi serupa benar-benar terjadi, peserta tidak panik dan tahu harus berbuat apa.

#### **3. Pengetahuan tentang Jalur Pelaporan Resmi**

Salah satu temuan penting dalam kegiatan ini adalah betapa rendahnya pengetahuan peserta tentang jalur pelaporan resmi yang tersedia. Banyak di antara mereka yang tidak mengetahui



bahwa OJK memiliki hotline 157 khusus untuk pengaduan keuangan, atau bahwa ada platform patrolisiber.id yang bisa digunakan untuk melaporkan kejahatan siber. Setelah penjelasan dan pembagian modul panduan, peserta menyatakan lebih siap dan percaya diri untuk melaporkan jika sewaktu-waktu mengalami penipuan digital.

## **Pembahasan**

### **1. Sesi I ( Penyampaian Materi Modus Penipuan Digital Berbasis AI )**

Pemateri : Dwinanda Marsya Tealova

Materi sesi pertama difokuskan pada pengenalan berbagai jenis penipuan digital yang memanfaatkan teknologi AI. Pemateri menyampaikan materi dengan cara yang sederhana dan menggunakan banyak contoh konkret agar mudah dipahami. Peserta terlihat sangat tertarik ketika diperlihatkan contoh-contoh bagaimana deepfake audio dapat menirukan suara seseorang dengan sangat meyakinkan. Beberapa peserta bahkan mengaku pernah menerima pesan yang kini mereka sadari merupakan percobaan phishing. Diskusi yang berlangsung pada sesi ini sangat hidup dan menunjukkan bahwa peserta mulai terhubung dengan realitas ancaman yang selama ini belum mereka sadari.

### **2. Sesi II ( Penyampaian Materi Tanggap Darurat dan Prosedur Pelaporan )**

Pemateri : Ceyzha Putri Tarita

Destia Riyanti

Sesi kedua berjalan lebih interaktif dengan adanya simulasi kasus yang melibatkan peserta secara langsung. Pemateri mengajak peserta untuk membayangkan situasi di mana mereka tiba-tiba menerima transfer uang yang tidak dikenal atau mendapat telepon dari pihak yang mengaku sebagai petugas bank. Melalui role-play sederhana ini, peserta berlatih untuk merespons situasi tersebut dengan tepat. Antusiasme peserta sangat tinggi pada sesi ini, terutama ketika mereka dikenalkan dengan platform patrolisiber.id dan cara menggunakannya untuk melapor. Modul panduan yang dibagikan kepada setiap peserta juga mendapat respons yang positif karena dianggap praktis dan mudah dimengerti.

### **3. Secara keseluruhan, hasil dari kedua sesi materi menunjukkan bahwa pendekatan yang digunakan dalam kegiatan PKM ini sangat efektif dalam meningkatkan pemahaman dan kesiapan peserta. Kombinasi antara penyampaian materi secara presentasi, simulasi kasus nyata, dan sesi tanya jawab terbuka terbukti mampu mengakomodasi berbagai gaya belajar yang dimiliki peserta. Respons positif yang diterima dari seluruh peserta dan pengurus Majelis Ta'lim Auladina menjadi bukti nyata keberhasilan kegiatan PKM ini**

## **KESIMPULAN**

Berdasarkan keseluruhan rangkaian kegiatan Pengabdian Kepada Masyarakat yang telah dilaksanakan, dapat ditarik beberapa kesimpulan sebagai berikut:

1. Kegiatan penyuluhan ini berhasil meningkatkan kesadaran dan pemahaman ibu-ibu Majelis Ta'lim Auladina tentang berbagai modus penipuan digital berbasis AI yang saat ini marak terjadi di masyarakat. Peserta yang awalnya kurang mengenal istilah seperti deepfake dan phishing menjadi lebih paham dan waspada setelah kegiatan berlangsung.



2. Pelatihan langkah-langkah tanggap darurat yang dilakukan melalui simulasi kasus terbukti efektif dalam membekali peserta dengan keterampilan praktis yang dapat langsung diterapkan ketika menghadapi situasi penipuan digital di kehidupan nyata.
3. Pemberian panduan prosedur pelaporan resmi dalam bentuk modul yang mudah dipahami berhasil menutup celah ketidaktahuan peserta tentang ke mana dan bagaimana cara melaporkan kasus penipuan digital. Hal ini diharapkan dapat mendorong lebih banyak korban untuk berani melapor sehingga kasus-kasus penipuan dapat ditangani secara hukum.
4. Secara umum, kegiatan PKM ini menunjukkan bahwa kolaborasi antara mahasiswa, dosen pembimbing, dan komunitas masyarakat merupakan cara yang efektif untuk meningkatkan literasi keuangan digital di tingkat akar rumput, sehingga keamanan ekonomi keluarga dapat lebih terlindungi dari ancaman kejahatan siber.

#### **DAFTAR PUSTAKA**

- Badan Siber dan Sandi Negara (BSSN). (2023). Laporan Tahunan Keamanan Siber Indonesia 2023. Jakarta: BSSN.
- Hariyanto, B. (2022). Manajemen Krisis Digital: Panduan Praktis Menghadapi Kejahatan Siber. Yogyakarta: Gadjah Mada University Press.
- Kementerian Komunikasi dan Informatika Republik Indonesia. (2023). Panduan Keamanan Bertransaksi Digital untuk Masyarakat. Jakarta: Kominfo.
- Nugroho, A. (2023). Kejahatan Siber di Indonesia: Tantangan dan Strategi Penanggulangannya. Jakarta: Rajawali Press.
- Otoritas Jasa Keuangan (OJK). (2022). Survei Nasional Literasi dan Inklusi Keuangan 2022. Jakarta: OJK.
- Prasetyo, W. (2023). Deepfake dan Ancaman Keamanan Digital: Perspektif Hukum dan Teknologi. *Jurnal Hukum dan Teknologi*, 5(2), 112–125.
- Santoso, R. (2022). Literasi Keuangan Digital pada Ibu Rumah Tangga di Perkotaan. *Jurnal Manajemen dan Keuangan*, 11(1), 45–58.
- Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016.
- Widiyanti, M. (2022). Pemberdayaan Masyarakat melalui Edukasi Keamanan Transaksi Digital. *Jurnal Pengabdian Kepada Masyarakat*, 8(3), 201–214.
- Zunaidi, A. (2023). Ancaman Phishing Berbasis AI dan Upaya Pencegahannya di Kalangan Masyarakat Awam. *Jurnal Ilmu Komputer dan Keamanan Siber*, 3(1), 22–35.