

Optimalisasi Literasi Keuangan Digital Masyarakat Untuk Meminimalisir Risiko Penipuan *Link Phising*

Optimization of Community Digital Financial Literacy to Minimize the Risk of Phishing Link Fraud

Putu Ayu Titha Paramita Pika*, Anak Agung Gede Agung Keysan Arjuna Putra

Program Studi Manajemen, Fakultas Ekonomi dan Bisnis, Universitas Pendidikan Nasional,
Denpasar

*Email: paramitatitha@undiknas.ac.id

(Diterima 05-03-2026; Disetujui 24-06-2026)

ABSTRAK

Transformasi ekonomi digital di Indonesia telah menjangkau kawasan pedesaan, membawa kemudahan akses layanan keuangan bagi masyarakat dan pelaku Usaha Mikro, Kecil, dan Menengah (UMKM). Namun, transisi ini diiringi oleh lonjakan ancaman kejahatan siber, khususnya penipuan berbasis tautan *phishing* yang memanfaatkan rekayasa sosial dan kerentanan psikologis pengguna. Kegiatan pengabdian kepada masyarakat ini bertujuan untuk mengoptimalkan literasi keuangan digital masyarakat di Desa Gemuh guna meminimalisir risiko penipuan *phishing*. Metode pelaksanaan menggunakan *Participatory Action Research* (PAR) yang terbagi dalam tiga tahapan utama: observasi awal (prates), edukasi multidisipliner (mencakup aspek teknologi, ekonomi, dan hukum), serta simulasi identifikasi ancaman digital yang diakhiri dengan evaluasi (pascates). Kegiatan ini dilaksanakan pada awal tahun 2026 dengan melibatkan 50 peserta yang terdiri atas pelaku UMKM, ibu rumah tangga, dan anggota Karang Taruna. Hasil pengabdian menunjukkan adanya kesenjangan yang signifikan antara tingkat adopsi teknologi keuangan dan pemahaman keamanan siber pada kondisi awal. Pasca-intervensi, terjadi peningkatan persentase pemahaman peserta dalam mengidentifikasi tautan *phishing* dari 22% menjadi 88%, serta peningkatan kesadaran akan prosedur pelaporan hukum perlindungan data pribadi. Kesimpulan dari kegiatan ini menegaskan bahwa pendekatan edukasi yang menggabungkan mitigasi kejahatan siber, pemahaman ekonomi digital, dan literasi regulasi secara efektif dapat membangun resiliensi masyarakat pedesaan terhadap kejahatan finansial digital.

Kata kunci: Literasi Keuangan Digital; *Phishing*; Keamanan Siber; Pemberdayaan Masyarakat; Perlindungan Konsumen

ABSTRACT

The digital economic transformation in Indonesia has reached rural areas, bringing ease of access to financial services for the community and Micro, Small, and Medium Enterprises (MSMEs). However, this transition is accompanied by a surge in cybercrime threats, particularly phishing link fraud that exploits social engineering and users' psychological vulnerabilities. This community service activity aims to optimize the digital financial literacy of the community in Gemuh Village to minimize the risk of phishing fraud. The implementation method uses Participatory Action Research (PAR) which is divided into three main stages: initial observation (pre-test), multidisciplinary education (covering technological, economic, and legal aspects), and simulation of digital threat identification ending with an evaluation (post-test). This activity was carried out in early 2026 involving 50 participants consisting of MSME actors, housewives, and youth organizations (Karang Taruna). The results of the community service showed a significant gap between the rate of financial technology adoption and cybersecurity understanding in the initial conditions. Post-intervention, there was an increase in the percentage of participants' understanding in identifying phishing links from 22% to 88%, as well as increased awareness of legal reporting procedures for personal data protection. The conclusion of this activity confirms that an educational approach combining cybercrime mitigation, digital economy understanding, and regulatory literacy can effectively build rural community resilience against digital financial crimes.

Keywords: Digital Financial Literacy; *Phishing*; Cybersecurity; Community Empowerment; Consumer Protection

PENDAHULUAN

Infrastruktur dan adopsi teknologi digital di Indonesia mengalami percepatan yang sangat masif, yang tidak lagi hanya terpusat di wilayah perkotaan (urban), melainkan telah berintegrasi ke dalam sendi-sendi kehidupan masyarakat pedesaan dan semi-urban. Perkembangan ini ditandai dengan semakin maraknya penggunaan dompet digital (*e-wallet*), aplikasi perbankan seluler (*mobile banking*), dan *platform e-commerce* oleh berbagai lapisan masyarakat, termasuk para pelaku Usaha Mikro, Kecil, dan Menengah (UMKM) yang kini mulai mendigitalisasi arus kas dan pemasarannya. Transformasi ini pada dasarnya memberikan dampak positif yang terukur terhadap stabilitas keuangan dan inklusi ekonomi di tingkat akar rumput (Risman et al., 2021; 1980). Kemudahan bertransaksi tanpa uang tunai memberikan efisiensi waktu dan transparansi yang sangat dibutuhkan untuk memacu roda perputaran ekonomi lokal. Kendati demikian, digitalisasi yang berlangsung secara eksponensial ini ternyata menyimpan residu permasalahan yang serius apabila tidak diimbangi dengan kesiapan kognitif penggunanya. Tingkat penetrasi gawai dan internet yang tinggi seringkali tidak berjalan linier dengan tingkat literasi digital dan keuangan masyarakat. Ketimpangan inilah yang kemudian menciptakan celah kerentanan baru yang dieksploitasi oleh para pelaku kejahatan siber (*cybercrime*).

Salah satu manifestasi kejahatan siber yang paling merugikan dan mengalami lonjakan kasus paling tajam dalam ekosistem keuangan digital modern adalah *phishing* (Hafid et al., 2023; 2202). *Phishing* merupakan metode penipuan yang dilakukan oleh oknum tidak bertanggung jawab dengan cara menyamar sebagai entitas yang sah atau institusi resmi—seperti bank, lembaga pemerintah, atau perusahaan logistik—dengan tujuan memanipulasi korban agar menyerahkan data sensitif mereka. Data sensitif ini meliputi kredensial *login*, nomor identitas pribadi (PIN), *One-Time Password* (OTP), hingga nomor kartu kredit. Modus operandi kejahatan ini terus berevolusi; jika dahulu hanya mengandalkan surel (email) palsu, kini para peretas memanfaatkan aplikasi pesan singkat seperti WhatsApp, SMS, dan media sosial untuk menyebarkan tautan (*link*) berbahaya maupun dokumen berformat APK (*Android Package Kit*) yang disamarkan sebagai undangan pernikahan digital, surat tilang elektronik, atau pemberitahuan resi paket (Adisa & Nugroho, 2024; 245). Data dari *Indonesia Anti-Phishing Data Exchange* (IDADX) mencatat lonjakan tajam laporan serangan *phishing* di Indonesia, di mana pada kuartal pertama tahun 2023 saja terdapat 26.675 kasus, yang merepresentasikan ancaman nyata bagi keamanan aset masyarakat (Lokapala et al., 2024; 24).

Keberhasilan teknik penipuan *phishing* ini sejatinya sangat erat kaitannya dengan eksploitasi psikologis yang memanfaatkan mekanisme *Attention Economy* (Ekonomi Perhatian) di era digital. Dalam lanskap digital yang dibanjiri oleh arus informasi yang tanpa henti, para pelaku kejahatan merancang pesan-pesan penipuan yang secara spesifik menargetkan emosi reaktif manusia — seperti kepanikan, ketakutan, atau antusiasme yang berlebihan. Pesan yang berisi ancaman pemblokiran rekening secara tiba-tiba, atau sebaliknya, janji pemberian bantuan sosial yang menggiurkan, dirancang untuk membajak sistem logika pengguna agar mereka mengklik tautan tanpa melakukan verifikasi terlebih dahulu. Saat korban menekan tautan manipulatif tersebut, mereka diarahkan pada situs *web* replika yang sangat menyerupai situs aslinya, di mana segala informasi yang diketikkan oleh korban akan terekam secara *real-time* ke dalam basis data peretas. Fenomena ini membuktikan bahwa literasi digital yang dibutuhkan saat ini bukan sekadar keterampilan teknis dalam mengoperasikan ponsel pintar, melainkan juga kecakapan kritis untuk mengidentifikasi distorsi informasi dan memitigasi risiko di dunia maya (Sila & Taufik, 2023; 105).

Fenomena penipuan digital ini menimbulkan kerugian finansial yang destruktif, khususnya bagi masyarakat pedesaan dan pelaku UMKM yang seringkali memiliki ketahanan modal yang terbatas (Safitri et al., 2022; 1205). Ketika modal usaha atau tabungan keluarga terkuras akibat *phishing*, dampaknya secara langsung mengancam keberlanjutan usaha dan kesejahteraan rumah tangga. Secara hukum, Indonesia sebenarnya telah memiliki instrumen regulasi yang komprehensif untuk merespons kejahatan ini, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Pelindungan Data Pribadi (UU PDP), serta Peraturan Otoritas Jasa Keuangan (POJK) Nomor 22 Tahun 2023 tentang Pelindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan (Kartiko et al., 2024; 350). Namun, penegakan hukum dari perspektif keadilan restoratif (*restorative justice*) bagi korban penipuan digital masih menghadapi berbagai kendala, terutama karena kompleksitas dalam melacak jejak digital pelaku yang seringkali beroperasi secara anonim melintasi yurisdiksi, serta kurangnya pemahaman masyarakat mengenai prosedur pelaporan yang benar. Nasabah yang menjadi korban seringkali menyalahkan pihak perbankan atas hilangnya

dana, padahal kebocoran data acapkali bersumber dari kelalaian konsumen itu sendiri (Erdiyanto, 2023; 74). Hal ini menegaskan bahwa perlindungan preventif melalui edukasi dan kesadaran mandiri (*self-awareness*) merupakan benteng pertahanan pertama dan yang paling rasional.

Permasalahan ini sangat relevan dengan dinamika sosial ekonomi yang terjadi di pedesaan, tak terkecuali di wilayah Desa Gemuh. Berdasarkan pengamatan sosiologis dan interaksi empiris di lapangan, masyarakat desa tersebut saat ini tengah berada dalam fase transisi teknologi yang cepat. Peningkatan infrastruktur publik dan kemudahan akses internet telah mendorong masyarakat untuk mengadopsi layanan perbankan digital. Akan tetapi, kultur masyarakat komunal yang cenderung mudah percaya (*high-trust society*) terhadap informasi yang disebarkan melalui grup komunikasi internal (seperti grup WhatsApp keluarga atau RT/RW) menjadikan mereka target yang sangat rentan terhadap penyebaran tautan *phishing* yang berkedok informasi resmi (Anan et al., 2024; 4342). Kelompok rentan seperti ibu rumah tangga dan pemuda (termasuk anggota karang taruna) seringkali terjebak dalam skema penipuan ini karena minimnya paparan edukasi sistematis mengenai ancaman digitalisasi keuangan (Fikri et al., 2022; 108).

Menyikapi urgensi tersebut, diperlukan sebuah intervensi akademis dan praktis yang terstruktur untuk menjembatani kesenjangan antara kemajuan teknologi dan kesiapan masyarakat. Program pengabdian masyarakat ini hadir sebagai respons proaktif untuk merancang dan mengimplementasikan kegiatan edukasi yang komprehensif. Tujuan utama dari kegiatan ini adalah untuk mengoptimalisasi literasi keuangan digital masyarakat guna meminimalisir risiko penipuan tautan *phishing*. Melalui pendekatan multidisipliner yang mengintegrasikan pemahaman teknologi sistem informasi, manajemen risiko bisnis, dan kesadaran hukum perlindungan data, diharapkan masyarakat tidak hanya mampu mengenali dan menghindari jebakan siber, tetapi juga memiliki kepercayaan diri yang kuat dalam memanfaatkan ekosistem ekonomi digital secara aman dan produktif untuk mendukung kesejahteraan mereka.

BAHAN DAN METODE

Kegiatan pengabdian masyarakat ini dirancang dan dilaksanakan dengan mengadopsi metode *Participatory Action Research* (PAR), sebuah kerangka metodologi yang berfokus pada kolaborasi aktif antara akademisi dan elemen masyarakat untuk mengidentifikasi masalah, merumuskan solusi, dan menerapkan tindakan perbaikan secara langsung dalam suatu komunitas. Pemilihan metode PAR didasari oleh kebutuhan untuk tidak sekadar memberikan transfer pengetahuan secara satu arah, melainkan menciptakan kesadaran kritis dan perubahan perilaku yang berkelanjutan di kalangan masyarakat (Andaningsih et al., 2022; 145). Kegiatan ini dipusatkan di Balai Desa Gemuh dan berlangsung pada periode bulan Januari hingga Februari 2026. Fokus geografis dan demografis ini dipilih mengingat karakteristik masyarakat desa tersebut yang sangat representatif menggambarkan fenomena transisi masyarakat semi-urban menuju tatanan ekonomi digital.

Sasaran strategis (*target audience*) dalam kegiatan pengabdian ini berjumlah 50 orang partisipan, yang secara purposif dipilih berdasarkan representasi kelompok masyarakat yang memiliki frekuensi transaksi keuangan digital yang aktif namun rentan terhadap ancaman siber. Komposisi peserta terdiri atas tiga kelompok utama: (1) Pelaku UMKM lokal yang menggunakan *mobile banking* untuk transaksi bisnis sehari-hari; (2) Ibu rumah tangga yang mengelola keuangan keluarga dan rutin menggunakan *e-commerce* serta dompet digital; dan (3) Pemuda atau anggota karang taruna yang sering menjadi pengadopsi awal (*early adopters*) dari berbagai platform teknologi pendanaan baru (Gayatri & Muzdalifah, 2022; 299). Keberagaman profil peserta ini penting untuk memetakan variasi tingkat literasi dan modus penipuan yang paling relevan dengan masing-masing kelompok usia dan profesi.

Pelaksanaan pengabdian masyarakat ini disusun melalui empat tahapan sistematis dan terukur:

1. Tahap Persiapan dan Observasi Diagnostik (Prates)

Tahap awal dimulai dengan koordinasi intensif bersama perangkat desa setempat guna memetakan kondisi demografis dan menetapkan jadwal kegiatan sosialisasi yang tidak mengganggu produktivitas ekonomi warga. Pada tahap ini, instrumen penelitian berupa kuesioner asesmen diagnostik awal (prates) disusun secara cermat. Kuesioner ini dirancang untuk mengukur variabel *baseline* pengetahuan peserta yang mencakup pemahaman tentang definisi informasi

sensitif, pengenalan anatomi tautan (*URL/Uniform Resource Locator*), pengalaman terkait upaya penipuan *online*, serta pemahaman dasar mengenai hukum perlindungan data. Kuesioner dibagikan sesaat sebelum pemaparan materi inti dimulai, guna mendapatkan data empiris mengenai tingkat literasi aktual masyarakat sebelum adanya intervensi.

2. Tahap Sosialisasi dan Edukasi Multidisipliner

Fase ini merupakan inti dari intervensi pengetahuan, di mana materi edukasi disampaikan menggunakan pendekatan multidisipliner yang memadukan perspektif teknologi informasi, manajemen bisnis, dan logika hukum. Metode penyampaian mengutamakan teknik ceramah interaktif dengan meminimalisir jargon akademis yang rumit, menggantinya dengan bahasa keseharian masyarakat yang mudah dicerna (*humanized language*). Materi yang disajikan mencakup:

- Anatomi Ekonomi Digital: Pengenalan ekosistem pembayaran digital (QRIS, *e-wallet*, transfer bank *online*), serta manfaatnya bagi efisiensi bisnis UMKM.
- Anatomi Kejahatan Siber (*Phishing*): Penjelasan mendalam mengenai modus operandi manipulasi psikologis, rekayasa sosial (*social engineering*), dan cara kerja *file* ekstensi APK peretas dalam mengambil alih kontrol peranti (Wahib et al., 2022; 2205).
- Regulasi dan Proteksi Legal: Pengenalan hak-hak dasar nasabah sebagai konsumen jasa keuangan yang diatur dalam UU ITE dan regulasi OJK, serta mitigasi hukum (langkah pemblokiran kartu, pelaporan ke kepolisian, dan pengaduan ke pihak perbankan).

3. Tahap Pendampingan dan Simulasi Praktis

Untuk mengkonkretkan materi teoretis, kegiatan dilanjutkan dengan sesi pendampingan (*Focus Group Discussion*) dan simulasi identifikasi ancaman. Peserta dibagi ke dalam beberapa kelompok kecil (beranggotakan 5-6 orang) untuk menganalisis berbagai tangkapan layar (*screenshot*) yang menampilkan studi kasus nyata berisi pesan WhatsApp mencurigakan, surel palsu, dan desain situs *web* perbankan yang dipalsukan. Dalam sesi ini, peserta diajarkan metode pengecekan keamanan siber secara praktis, seperti memeriksa sertifikat keamanan situs (HTTPS), mengenali taktik *typosquatting* (kesalahan ejaan nama *domain* yang disengaja), serta praktik aktivasi fitur Autentikasi Dua Faktor (*Two-Factor Authentication/2FA*) pada aplikasi masing-masing.

4. Tahap Evaluasi Peningkatan Pemahaman (Pascates)

Tahap pungkasan bertujuan untuk mengukur efikasi dan signifikansi perubahan tingkat literasi digital peserta. Kuesioner evaluasi (*pascates*) dengan instrumen dan indikator yang sejajar dengan *prates* didistribusikan kembali setelah sesi simulasi berakhir. Data kuantitatif yang diperoleh dari selisih skor *prates* dan *pascates* kemudian ditabulasi, divisualisasikan, dan dianalisis secara deskriptif komparatif untuk menjustifikasi keberhasilan program pengabdian. Selain itu, sesi tanya jawab dan *feedback* terbuka juga dilakukan untuk menampung aspirasi masyarakat terkait kebutuhan literasi teknologi lanjutan.

HASIL DAN PEMBAHASAN

Pelaksanaan kegiatan pengabdian masyarakat di Desa Gemuh menghasilkan serangkaian temuan empiris yang komprehensif. Melalui metode pengukuran *prates* dan *pascates*, serta observasi partisipatif selama sesi simulasi dan diskusi, diperoleh data yang merefleksikan dinamika adopsi teknologi serta efektivitas edukasi keamanan siber di ranah masyarakat akar rumput. Pembahasan hasil kegiatan ini diuraikan ke dalam beberapa sub-fokus analitis sebagai berikut:

1. Analisis Kondisi Awal dan Kerentanan Masyarakat (Hasil Prates)

Hasil kuesioner diagnostik awal memperlihatkan potret literasi digital yang cukup mengkhawatirkan meskipun adopsi instrumen keuangan digital telah meluas. Sebanyak 92% peserta telah menggunakan *smartphone* dan memiliki setidaknya satu aplikasi dompet digital atau perbankan seluler. Namun, ironisnya, hanya 22% peserta yang mampu mendefinisikan secara tepat apa yang dimaksud dengan tautan berbahaya atau *phishing*. Lebih lanjut, ketika dihadapkan pada skenario penerimaan pesan WhatsApp yang melampirkan *file* APK berkedok "Undangan Pernikahan.apk" atau "Resi Paket J&T.apk", 68% peserta mengaku bahwa refleksi pertama mereka adalah menekan (*tap*) dan mencoba mengunduh *file* tersebut tanpa rasa curiga.

Ketidaktahuan masyarakat mengenai bahaya di balik *file* APK tidak resmi merupakan salah satu titik buta (*blind spot*) terbesar dalam lanskap keamanan digital lokal. Para pelaku kejahatan

memanipulasi *file* berekstensi *Android Package Kit* ini agar, ketika diinstal, aplikasi tersebut memiliki hak akses tersembunyi (*hidden permissions*) untuk membaca SMS yang masuk (Adisa & Nugroho, 2024; 246). Hal inilah yang memungkinkan peretas untuk mencuri kode OTP (yang biasanya dikirimkan bank via SMS) dan menguras saldo korban tanpa disadari. Rendahnya literasi pada tahap ini juga diperparah oleh absennya budaya pengecekan ganda (*double-checking*) terhadap informasi yang disebar melalui jaringan interpersonal terpercaya, sebuah fenomena sosiologis di mana kepercayaan komunal yang tinggi disalahgunakan oleh peretas yang mengambil alih akun WhatsApp kerabat.

2. Implementasi Edukasi dan Pendekatan Multidisipliner

Proses sosialisasi difokuskan pada dekonstruksi narasi-narasi penipuan. Tim pelaksana menyajikan materi dengan menitikberatkan pada perpotongan antara psikologi ekonomi dan teknologi. Peserta diajak untuk memahami bahwa penipuan digital modern tidak selalu berwujud peretasan sistem yang canggih (*brute force hacking*), melainkan beroperasi melalui rekayasa sosial yang mengeksploitasi kepanikan atau keserakahan manusia. Konsep *Attention Economy* diadopsi secara sederhana untuk menjelaskan bagaimana notifikasi palsu yang berbunyi "*Rekening Anda akan diblokir dalam 24 jam*" dirancang sedemikian rupa untuk menciptakan urgensi psikologis (Wulan et al., 2022; 1205). Ketika otak manusia berada dalam kondisi panik dan mendesak, kemampuan analisis logis menurun drastis, menyebabkan korban secara refleks menekan tautan yang dilampirkan.

Bagi kelompok pelaku UMKM, materi diperdalam dengan mengontekstualisasikan risiko kejahatan siber terhadap manajemen kelangsungan usaha (*business continuity management*). Kasus-kasus nyata dipaparkan untuk mengilustrasikan bahwa keamanan data pelanggan dan aset digital usaha sama vitalnya dengan mengelola inventaris fisik. Sementara itu, untuk peserta dari karang taruna, ditekankan peran mereka sebagai agen perubahan (*change agents*) dan garda depan yang mampu mentransfer literasi digital kepada generasi yang lebih tua (lansia) di keluarga masing-masing, mengingat kelompok usia 19-35 tahun memiliki intuisi navigasi gawai yang jauh lebih adaptif (Sila & Taufik, 2023; 107).

3. Simulasi Identifikasi Tautan Phishing dan Taktik Typosquatting

Puncak antusiasme kegiatan terjadi pada sesi pendampingan praktis dan bedah kasus. Tim pengabdian menampilkan visualisasi struktur *URL* untuk mengajarkan peserta membedakan antara *domain* perbankaan yang sah dan situs imitasi. Salah satu teknik penipuan yang paling banyak dikupas adalah *typosquatting*—praktik mendaftarkan nama *domain* internet yang dieja sangat mirip dengan situs populer, dengan harapan agar pengguna internet salah mengetik atau tidak menyadari perbedaan kecil pada tautan (Kartiko et al., 2024; 352).

Dalam simulasi tersebut, peserta diajak membandingkan secara saksama antara alamat situs asli (misalnya, <https://www.klikbca.com>) dengan variasi palsunya yang beredar di pesan berantai (seperti <http://www.klikbca-promo-id.com> - menggunakan huruf 'l' kapital menggantikan huruf 'i' kecil, atau menambahkan tanda hubung yang tidak standar). Edukasi difokuskan pada tiga langkah taktis, yang disingkat dengan kampanye "Saring Sebelum Sharing dan Klik":

1. Cek Pengirim: Memastikan kredibilitas nomor pengirim. Institusi perbankan resmi tidak pernah menghubungi nasabah menggunakan nomor seluler biasa (pra-bayar).
2. Cek Anatomi Tautan: Mengidentifikasi protokol keamanan koneksi (<https://> dengan ikon gembok, di mana "s" berarti *secure*), serta mencermati kelogisan nama *domain* utama.
3. Hindari Transaksi di Luar Aplikasi Resmi: Mengedukasi peserta agar selalu membuka aplikasi perbankan resmi (*mobile banking app*) yang diunduh dari *Google Play Store* atau *Apple App Store* secara mandiri, ketimbang login melalui *browser* dari tautan tidak dikenal.

4. Literasi Hukum, Pelindungan Konsumen, dan Langkah Mitigasi

Aspek yang tidak kalah penting dalam kegiatan ini adalah penguatan literasi hukum. Berdasarkan dialog interaktif, terungkap bahwa banyak masyarakat yang tidak mengetahui langkah krusial apa yang harus ditempuh pada "Menit Pertama" (*Golden Minute*) setelah menyadari bahwa mereka telah menjadi korban klik tautan *phishing*. Peserta diberikan pemahaman logis dan prosedural terkait mitigasi bencana digital (Erdiyanto, 2023; 75). Langkah pertama yang ditekankan adalah tidak panik, segera memutuskan koneksi internet data seluler atau mengaktifkan "Mode Pesawat" (*Airplane Mode*) untuk memutus transmisi data pelaku. Langkah selanjutnya adalah segera menghubungi *call*

center resmi bank untuk memblokir kartu dan rekening, serta melakukan pencopotan (*uninstall*) aplikasi berbahaya atau memulihkan perangkat ke pengaturan pabrik (*factory reset*).

Selain itu, peserta diedukasi mengenai payung hukum perlindungan konsumen sebagaimana tertuang dalam Peraturan OJK (POJK) No. 22 Tahun 2023 dan peran Otoritas Jasa Keuangan dalam mengawasi industri perbankan (Lokapala et al., 2024; 25). Kendati hukum menuntut bank memiliki sistem manajemen risiko dan mitigasi serangan siber yang tangguh, warga juga diberikan pencerahan bahwa pihak perbankan tidak dapat mengganti kerugian materiil apabila hasil investigasi digital forensik membuktikan bahwa kelalaian berasal dari sisi nasabah—seperti secara sadar menyerahkan kode OTP atau PIN kepada peretas. Penjabaran ini berhasil mematahkan miskonsepsi hukum di masyarakat yang menganggap perbankan menanggung seluruh risiko kebocoran dana otomatis, dan pada gilirannya sukses menumbuhkan rasa tanggung jawab personal (*personal accountability*) warga dalam menjaga privasi keamanan data mereka.

5. Evaluasi Dampak Edukasi (Hasil Pascatest)

Keberhasilan kegiatan pengabdian diukur dari analisis data kuesioner pascates yang dilakukan pada akhir sesi. Terjadi lonjakan pemahaman yang sangat masif dan memuaskan. Tingkat kemampuan mengidentifikasi ciri-ciri tautan *phishing* meningkat drastis dari yang awalnya hanya 22% melonjak menjadi 88%. Pemahaman warga terkait esensi kode OTP sebagai gembok digital yang pantang dibagikan kepada siapapun mencapai 100% retensi. Lebih jauh lagi, lebih dari 75% peserta telah mampu mendeskripsikan secara tepat perbedaan fundamental antara *file* dokumen foto/PDF yang aman dengan *file* instalasi program APK yang sangat berbahaya jika dikirimkan oleh nomor tak dikenal.

Keberhasilan kognitif ini juga memicu perubahan iktikad perilaku teknis (*behavioral intention*). Dalam pantauan pasca-kegiatan, banyak peserta dari kalangan UMKM yang langsung meminta bantuan untuk diajarkan cara mengaktifkan lapisan keamanan ganda (*Two-Factor Authentication*) di akun media sosial bisnis dan dompet digital mereka (Andaningsih et al., 2022; 150). Perubahan paradigma ini mengindikasikan bahwa resistensi masyarakat terhadap ancaman siber tidak membutuhkan perangkat mahal, melainkan berakar kuat pada tersedianya pengetahuan, logika berpikir logis, dan kewaspadaan literasi.

KESIMPULAN DAN SARAN

Kesimpulan

Kegiatan pengabdian kepada masyarakat yang berfokus pada optimalisasi literasi keuangan digital di Desa Gemuh telah terlaksana dengan komprehensif dan menghasilkan diseminasi pengetahuan yang berdampak positif secara empiris. Transformasi digitalisasi perekonomian lokal, di mana masyarakat dan pelaku UMKM semakin masif memanfaatkan platform keuangan digital, ternyata diiringi oleh kesenjangan yang lebar pada tingkat kesadaran keamanan siber (*cybersecurity awareness*). Kerentanan tertinggi ditemukan pada ketidakmampuan warga mengidentifikasi modus manipulasi *file* instalasi palsu (APK) dan rekayasa *URL phishing* yang menyebar melalui aplikasi perpesanan instan. Melalui metode pendekatan edukasi multidisipliner yang memadukan mitigasi teknologi ancaman, psikologi ekonomi (*attention economy*), dan perlindungan legal hukum data, tingkat kecakapan literasi keamanan digital masyarakat terbukti meningkat secara signifikan. Hasil evaluasi mencatat lonjakan rasio kemampuan masyarakat dalam mendeteksi ancaman penipuan tautan berbahaya yang meningkat hampir empat kali lipat (dari 22% menjadi 88%). Hal ini menegaskan bahwa strategi literasi keuangan di era modern tidak dapat lagi sekadar berkutat pada pencatatan akuntansi dan tata kelola arus kas, namun wajib mengintegrasikan protokol mitigasi kejahatan siber demi mengamankan keberlanjutan ekonomi dari kerugian finansial yang destruktif.

Saran

Berdasarkan hasil analisis, simpulan, dan dinamika yang terbangun selama pelaksanaan pengabdian, terdapat beberapa rekomendasi strategis yang diajukan. *Pertama*, kepada jajaran Perangkat Desa Gemuh dan pemerintah daerah terkait, direkomendasikan untuk membentuk gugus tugas atau kader literasi digital tingkat desa (yang dapat dimotori oleh karang taruna) guna memastikan adanya edukasi yang berkesinambungan bagi warga lansia maupun pelaku usaha mikro yang belum terpapar pelatihan. *Kedua*, institusi perbankan lokal dan penyelenggara *Fintech* perlu meningkatkan desain antarmuka aplikasi (*User Interface*) yang lebih proaktif dalam memberikan peringatan keamanan (*security prompts*) berbahasa lokal yang mudah dipahami bagi nasabah area pedesaan. *Ketiga*, untuk

agenda penelitian maupun kegiatan pengabdian masyarakat di masa mendatang, disarankan untuk memperluas instrumen pelatihan hingga mencakup pendampingan digital forensik dasar, pendampingan pelaporan kejahatan siber secara formal ke pihak aparat penegak hukum dan OJK, serta merancang modul kurikulum keamanan digital yang spesifik untuk diintegrasikan dalam program penguatan UMKM nasional.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih atas dukungan administratif dan koordinasi dalam pelaksanaan pengabdian masyarakat ini. Apresiasi juga disampaikan kepada seluruh pihak yang telah membantu penyediaan sumber daya mandiri sehingga program optimalisasi literasi keuangan digital untuk meminimalisir risiko *phishing* ini dapat diselesaikan sesuai target yang direncanakan.

DAFTAR PUSTAKA

- Adisa, A. Z., & Nugroho, A. A. (2024). Perlindungan Hukum Terhadap Korban Phising Terkait Pengiriman File Apk. *Justisi*, 10(1), 242–256. <https://doi.org/10.33506/js.v10i1.2980>
- Anan, M., Rahmah, S. A., & Risuhendri, R. (2024). Edukasi Keamanan Digital untuk Meningkatkan Kewaspadaan Masyarakat Terhadap Link Phising. *Jurnal Pengabdian Sosial*, 2(9), 4341–4346. <https://ejournal.jurnalpengabdiansosial.com/index.php/jps/article/view/875>
- Andaningsih, I. R., Trinandari, T., Novita, N., & Kurnia, K. (2022). Pemberdayaan UMKM Melalui Digitalisasi Keuangan Menggunakan Aplikasi Catatan Keuangan di Pasar Kraggan Wilayah Kecamatan Jati Sampurna Kota Bekasi Jawa Barat. *Jurnal Abdimas BSI: Jurnal Pengabdian Kepada Masyarakat*, 5(1), 143–155. <https://ejournal.bsi.ac.id/ejurnal/index.php/abdimas/article/view/10931>
- Andriani, & Hermantoro, B. (2023). Optimizing Financial Technology Literacy in Minimizing Phishing Threats (Case Study of Indonesian Sharia Bank Customers). *Proceeding of International Conference on Islamic Philanthropy*, 1, 38–52. <https://jurnal.unigal.ac.id/abdimasgaluh/article/view/18206>
- Erdiyanto, R. P. (2023). Penipuan mengatasnamakan bank berbentuk phishing. *Jurnal Inovasi Global*, 1(2), 71–79. <https://baskara.pubmedia.id/index.php/jb/article/download/357/16/430>
- Fikri, M. N., et al. (2022). Edukasi literasi digital kepada masyarakat tentang keamanan siber. *Jurnal Komunikasi Ikatan Sarjana Komunikasi Indonesia*, 8(1), 85–100. <https://www.journal.uinsgd.ac.id/index.php/mashadiruna/article/download/34819/pdf/112269>
- Gayatri, A. M., & Muzdalifah. (2022). Memahami literasi keuangan sebagai upaya pencegahan perilaku konsumtif dari pinjaman online. *Judicious: Journal of Management*, 3(2), 297–306. https://ejurnal.unmuhjember.ac.id/index.php/PENGABDIAN_IPTEKS/article/download/650/159
- Hafid, M., et al. (2023). Literasi Keuangan Digital Sebagai Upaya Pencegahan Penipuan Perbankan dan Mitigasi Kebocoran Data Pribadi. *Jurnal Akuntansi dan Keuangan (JAK)*, 12(2), 2200–2215. <https://ejurnal.uinj.ac.id/index.php/JAK/article/download/3673/2202>
- Kartiko, N. D., et al. (2024). Perlindungan Konsumen Sektor Keuangan: Peran OJK dalam Menghadapi Ancaman Phising dan Skimming. *IURIS STUDIA: Jurnal Kajian Hukum*, 5(2), 347–363. <http://jurnal.bundamedia grup.co.id/index.php/iuris/article/viewFile/616/439>
- Lokapala, Y. H., Nurfauzi, F. J., & Widowaty, Y. (2024). Aspek Yuridis Kejahatan Phishing Dalam Ketentuan Hukum Di Indonesia. *Indonesian Journal of Criminal Law and Criminology (IJCLC)*, 5(1), 22–35. <https://ejournal.fisip.unjani.ac.id/index.php/jurnal-dialektika-hukum/article/download/2881/806>
- Risman, A., Mulyana, B., Silvatika, B. A., & Sulaeman, A. S. (2021). The effect of digital finance on financial stability. *Management Science Letters*, 11(7), 1979–1984. <https://doi.org/10.5267/j.msl.2021.3.004>
- Safitri, N., Permadi, I., & Eva, F. (2022). Literasi Keuangan Digital, Keberlanjutan Usaha Industri Kecil Dan Menengah Serta Dampaknya Terhadap Kesejahteraan Keuangan. *Jurnal Ilmiah*

- MEA (Manajemen, Ekonomi, Dan Akuntansi)*, 6(3), 1203–1214. <https://doi.org/10.31955/mea.v6i3.2201>
- Sila, & Taufik. (2023). Upaya Penguatan Literasi Digital di Masyarakat. *Alahyan Jurnal Pengabdian Masyarakat Multidisiplin*, 1(2), 104–111. <https://www.journal.uinsgd.ac.id/index.php/mashadiruna/article/download/34819/pdf/112269>
- Wahib, et al. (2022). Meningkatkan penggunaan internet yang bijak, dan memperkuat literasi digital. *Jurnal Pengabdian Sosial*, 2(1), 220–235. <https://ejurnal.uij.ac.id/index.php/JAK/article/download/3673/2202>
- Wulan, et al. (2022). Tingkat literasi keuangan digital pada generasi Z dalam pemanfaatan teknologi. *Jurnal Ilmiah Ekonomi Bisnis*, 15(2), 1200–1210. <https://ejurnal.uij.ac.id/index.php/JAK/article/download/3673/2202>