CREATIVE: Jurnal Pengabdian Masyarakat
ISSN 3123-5204 (online)
Vol. 1 No. 4 Hal. 1202-1216
https://ejournal.scmdigi.id/index.php/creative

Edukasi *anti-scam* untuk UMKM: membangun kesadaran dan ketahanan digital terhadap ancaman penipuan online

Alfin Muslikhun[1*], Firmansyah[2], Kharis Raharjo[2], Syahqim Sudarpo[2], Mukhlidin[1], Diandra Alfaresta Cahya[1]
[1]Institut Teknologi Statistika dan Bisnis Muhammadiyah Semarang, Jawa Tengah, Indonesia
[2]Universitas Pandanaran Semarang, Jawa Tengah, Indonesia
*Author korespondensi: alfin.muslikhun@itesa.ac.id
DOI: https://doi.org/10.65881/creative.v1i4.239

INFO ARTIKEL

History:
Submit: 14-10-2026
Revisi: 19-10-2026
Diterima: 20-10-2026
Terbit: 26-10-2026

Kata kunci:
edukasi *anti-scam*;
umkm;
penipuan online;
keamanan digital;
literasi digital.

ABSTRAK

Tujuan: untuk meningkatkan pemahaman dan kesadaran pelaku UMKM mengenai modus penipuan online, khususnya APK palsu, *phishing*, dan pencurian data pribadi, serta mendorong penerapan praktik keamanan digital dalam melindungi akun, data, dan transaksi usaha.
Metode: menggunakan pendekatan edukatif dan partisipatif yang dilaksanakan melalui tiga tahapan, yaitu persiapan, pelaksanaan edukasi melalui penyampaian materi, demonstrasi, diskusi, dan tanya jawab, serta evaluasi melalui kuesioner kepuasan peserta. Kegiatan diikuti oleh 45 peserta di balai kelurahan Wonolopo, kota Semarang. Data peserta dianalisis secara deskriptif.
Hasil: menunjukkan bahwa edukasi *anti-scam* diikuti oleh 45 peserta dan memperoleh respons positif, dengan 93% peserta menyatakan sangat puas terhadap materi yang disampaikan. Kegiatan ini memberikan pemahaman praktis mengenai pencegahan penipuan online, meskipun peningkatan pengetahuan dan perubahan perilaku peserta belum diukur secara langsung.
Kesimpulan: edukasi *anti-scam* menjadi langkah preventif untuk memperkuat literasi dan ketahanan digital UMKM dalam menghadapi ancaman penipuan online.
Kontribusi: memperkuat literasi keamanan digital UMKM melalui edukasi pencegahan penipuan online dan perlindungan data serta transaksi usaha.

Artikel akses terbuka di bawah lisensi CC–BY-SA.

Pendahuluan

Perkembangan teknologi digital telah membuka peluang yang semakin luas bagi usaha mikro, kecil, dan menengah (UMKM) untuk meningkatkan daya saing melalui

perluasan jangkauan pemasaran, efisiensi operasional, serta kemudahan transaksi (Faturrahman et al., 2025). Pemanfaatan media sosial, marketplace, layanan perbankan digital, dan teknologi finansial (*financial technology* atau fintech) menjadi bagian penting dalam mendukung transformasi digital dan keberlanjutan usaha UMKM (Al-Okaily & Al-Okaily, 2026; Kumar & Rani, 2026; Zunairoh & Wijaya, 2024). Meskipun demikian, peningkatan ketergantungan terhadap teknologi digital juga diikuti oleh risiko keamanan siber, terutama penipuan online, pencurian data pribadi, dan penyalahgunaan akun digital yang dapat mengganggu aktivitas usaha serta menimbulkan kerugian finansial (Anan et al., 2024; Muslikhun et al., 2024). Kondisi tersebut menunjukkan bahwa keberhasilan transformasi digital UMKM tidak hanya ditentukan oleh kemampuan memanfaatkan teknologi untuk kegiatan ekonomi, tetapi juga oleh kesiapan pelaku usaha dalam mengenali dan mengantisipasi berbagai ancaman digital. Oleh karena itu, literasi keamanan digital menjadi kompetensi penting yang perlu dikembangkan untuk mendukung pemanfaatan teknologi secara aman, bijak, dan berkelanjutan (Usnur et al., 2026).

Salah satu permasalahan keamanan digital yang perlu mendapat perhatian adalah meningkatnya variasi modus penipuan online yang memanfaatkan aplikasi komunikasi dan interaksi digital sehari-hari. Modus tersebut antara lain penyebaran berkas *android package kit* (APK) berbahaya yang disamarkan sebagai undangan pernikahan, bukti pengiriman barang, dokumen tagihan, atau informasi lain yang mendorong penerima untuk membuka dan memasang aplikasi (Hariyadi et al., 2025; Purnamasari & Putri, 2026; Silmina et al., 2025). Selain itu, pelaku penipuan menggunakan teknik *phishing* melalui tautan, situs web, atau pesan yang menyerupai layanan resmi untuk memperoleh kata sandi, kode autentikasi, informasi rekening, dan data pribadi lainnya (Eriana et al., 2025; Nugroho et al., 2023; Susan et al., 2026). Bagi pelaku UMKM, ancaman tersebut tidak hanya berisiko terhadap keamanan perangkat dan informasi pribadi, tetapi juga dapat menyebabkan pengambilalihan akun usaha, penyalahgunaan identitas, terganggunya komunikasi dengan pelanggan, serta kerugian akibat transaksi palsu. Dampak tersebut berpotensi menurunkan kepercayaan konsumen dan menghambat keberlangsungan usaha (Pembayun et al., 2026; Ramadhan et al., 2026). Dengan demikian, persoalan utama yang perlu diatasi bukan sekadar keterbatasan akses terhadap teknologi, melainkan juga kemungkinan belum memadainya pengetahuan dan keterampilan praktis pelaku UMKM dalam mengidentifikasi pesan mencurigakan, melindungi data, memverifikasi transaksi, dan menentukan tindakan awal ketika menghadapi dugaan penipuan.

Sejumlah penelitian dan kegiatan pengabdian terdahulu telah membahas upaya peningkatan literasi digital dan pencegahan penipuan online melalui edukasi keamanan digital, sosialisasi bahaya *phishing*, perlindungan data pribadi, serta peningkatan kewaspadaan dalam menggunakan aplikasi komunikasi dan layanan perdagangan elektronik (Anan et al., 2024; Eriana et al., 2025; Muslikhun et al., 2024; Nugroho et al., 2023). Kajian lainnya menyoroti pentingnya literasi digital untuk menghadapi penipuan online berbasis e-commerce, penyalahgunaan data pribadi, dan berbagai bentuk kejahatan siber di lingkungan masyarakat (Pembayun et al., 2026; Purnamasari & Putri, 2026; Ramadani, 2026; Rismawati et al., 2026; Silmina et al., 2025; Syaiful & Khoir, 2026). Temuan dan praktik tersebut memberikan landasan bahwa edukasi merupakan salah satu pendekatan preventif yang relevan untuk meningkatkan kewaspadaan masyarakat terhadap ancaman digital. Namun, berdasarkan cakupan literatur yang dirujuk dalam kegiatan ini, masih terdapat ruang untuk memperkuat edukasi yang secara spesifik mengaitkan pengenalan modus

penipuan, khususnya APK berbahaya dan *phishing*, dengan kebutuhan perlindungan akun, data, dan transaksi dalam aktivitas usaha sehari-hari. Selain itu, dokumentasi penerimaan peserta terhadap kegiatan edukasi dapat melengkapi evaluasi pelaksanaan program pengabdian. Kesenjangan tersebut menjadi dasar perlunya kegiatan edukasi *anti-scam* yang kontekstual bagi pelaku UMKM, dengan penekanan pada pemahaman terhadap ancaman digital, penerapan langkah pencegahan, dan penguatan kebiasaan bertransaksi secara aman.

Berdasarkan permasalahan tersebut, kegiatan pengabdian kepada masyarakat ini dilaksanakan di balai kelurahan Wonolopo, kecamatan Mijen, kota Semarang, pada Senin, 21 September 2026. Kegiatan ini diikuti oleh 45 peserta, yang terdiri atas 35 laki-laki dan 10 perempuan, sebagai bagian dari upaya meningkatkan kesadaran masyarakat mengenai pentingnya keamanan digital dalam pemanfaatan teknologi untuk kegiatan ekonomi. Secara khusus, kegiatan ini bertujuan untuk meningkatkan pemahaman peserta mengenai berbagai modus penipuan digital, terutama undangan APK palsu dan *phishing*; memperkuat kesadaran akan pentingnya menjaga kerahasiaan informasi pribadi, keamanan perangkat, dan perlindungan akun digital; serta mendorong penerapan perilaku yang lebih waspada dalam mengakses pesan, membuka tautan, dan melakukan transaksi online. Untuk mendukung evaluasi pelaksanaan kegiatan, survei kepuasan peserta digunakan guna memperoleh gambaran mengenai penerimaan peserta terhadap materi edukasi dan penyelenggaraan program. Dengan demikian, kegiatan ini tidak hanya diarahkan pada penyampaian informasi, tetapi juga pada penguatan pemahaman praktis yang relevan dengan risiko digital dalam aktivitas usaha.

Kegiatan pengabdian ini diharapkan memberikan kontribusi praktis berupa peningkatan kesadaran dan kewaspadaan pelaku UMKM terhadap berbagai bentuk penipuan online, sekaligus mendorong terbentuknya kebiasaan digital yang lebih aman dalam pengelolaan komunikasi, akun, data, dan transaksi usaha. Dari sisi pelaksanaan pengabdian kepada masyarakat, kegiatan ini dapat menjadi salah satu model edukasi preventif yang menghubungkan pemahaman mengenai ancaman siber dengan kebutuhan nyata pelaku usaha dalam ekosistem ekonomi digital. Sementara itu, hasil survei kepuasan peserta diharapkan dapat memberikan informasi awal mengenai penerimaan terhadap materi dan pelaksanaan kegiatan sebagai bahan evaluasi serta perbaikan program edukasi berikutnya. Meskipun kepuasan peserta tidak secara langsung membuktikan peningkatan pengetahuan atau perubahan perilaku, informasi tersebut dapat menjadi salah satu indikator pendukung dalam menilai penerimaan program. Pada akhirnya, edukasi *anti-scam* diharapkan turut mendukung penguatan ketahanan digital UMKM agar pelaku usaha tidak hanya mampu memanfaatkan teknologi untuk memperluas pasar dan meningkatkan efisiensi, tetapi juga lebih siap mengenali, mencegah, dan merespons ancaman penipuan online secara tepat.

Metode

Kegiatan pengabdian kepada masyarakat ini menggunakan pendekatan edukatif dan partisipatif yang bertujuan untuk meningkatkan kesadaran serta pemahaman masyarakat, khususnya pelaku usaha mikro, kecil, dan menengah (UMKM), mengenai keamanan digital dan pencegahan penipuan online. Pendekatan edukatif diterapkan melalui penyampaian materi yang relevan dengan permasalahan keamanan digital dalam aktivitas usaha, sedangkan pendekatan partisipatif diwujudkan melalui demonstrasi, simulasi kasus, diskusi, dan tanya jawab yang melibatkan peserta secara aktif. Pelaksanaan kegiatan

dirancang secara sistematis dengan mengacu pada prinsip pelaksanaan kegiatan dan evaluasi yang dikemukakan dalam literatur metodologi penelitian (Ferdinand, 2021; Sugiyono, 2022).

Kegiatan dilaksanakan di balai kelurahan Wonolopo, kecamatan Mijen, kota Semarang, pada Senin, 21 September 2026. Kegiatan ini diikuti oleh 45 peserta, yang terdiri atas 35 laki-laki dan 10 perempuan. Peserta memperoleh edukasi mengenai berbagai bentuk penipuan digital yang berpotensi mengancam keamanan data dan keberlangsungan aktivitas usaha, terutama penipuan melalui berkas aplikasi *android package kit* (APK) palsu, *phishing*, pencurian data pribadi, serta penyalahgunaan akun dan transaksi digital. Untuk memastikan kegiatan terlaksana secara terarah, pelaksanaan pengabdian dibagi menjadi tiga tahapan utama, yaitu tahap persiapan, tahap pelaksanaan edukasi, dan tahap evaluasi. Alur pelaksanaan kegiatan tersebut disajikan pada Gambar 1.



Gambar 1 tahapan pelaksanaan kegiatan pengabdian kepada masyarakat

Tahap pertama adalah persiapan, yang meliputi analisis kebutuhan mitra, penyusunan materi edukasi, serta persiapan sarana dan koordinasi pelaksanaan kegiatan. Analisis kebutuhan dilakukan untuk mengidentifikasi permasalahan keamanan digital yang relevan dengan aktivitas masyarakat dan pelaku UMKM. Berdasarkan kebutuhan tersebut, materi edukasi disusun dengan menitikberatkan pada pengenalan modus penipuan online, karakteristik pesan dan tautan mencurigakan, perlindungan data pribadi, serta keamanan akun dan transaksi digital. Persiapan selanjutnya mencakup koordinasi dengan pihak kelurahan, pendataan peserta, serta penyediaan tempat, peralatan, dan media pendukung.

Tahap ini menghasilkan kesiapan materi, peserta, dan sarana yang diperlukan untuk mendukung pelaksanaan edukasi.

Tahap kedua adalah pelaksanaan edukasi, yang dilakukan melalui empat rangkaian kegiatan, yaitu pembukaan dan pengenalan, penyampaian materi, demonstrasi dan simulasi kasus, serta diskusi dan tanya jawab. Pada sesi pembukaan, peserta diperkenalkan dengan tujuan kegiatan dan pentingnya kewaspadaan terhadap ancaman penipuan digital. Materi kemudian disampaikan dengan membahas modus undangan APK palsu, ciri-ciri *phishing* dan cara menghindarinya, pencegahan pencurian data pribadi, serta langkah-langkah menjaga keamanan akun dan transaksi digital. Untuk memperkuat pemahaman praktis, penyampaian materi dilengkapi dengan demonstrasi dan simulasi kasus yang menggambarkan situasi penipuan digital. Sesi diskusi dan tanya jawab memberikan kesempatan kepada peserta untuk menyampaikan pertanyaan, mengklarifikasi informasi, serta mendiskusikan tindakan pencegahan yang dapat diterapkan dalam kegiatan usaha sehari-hari.

Tahap ketiga adalah evaluasi, yang dilakukan melalui pengumpulan umpan balik peserta, analisis hasil survei kepuasan, dan penyusunan laporan kegiatan. Umpan balik dikumpulkan menggunakan kuesioner untuk memperoleh gambaran mengenai tanggapan peserta terhadap materi edukasi dan pelaksanaan kegiatan. Data karakteristik peserta dianalisis secara deskriptif berdasarkan jumlah dan jenis kelamin, sedangkan hasil survei kepuasan diolah dalam bentuk persentase sesuai dengan data jawaban yang diperoleh. Analisis deskriptif digunakan untuk menyajikan karakteristik peserta dan respons mereka secara sistematis tanpa melakukan generalisasi di luar cakupan data yang tersedia (Sugiyono, 2020). Hasil evaluasi selanjutnya digunakan sebagai bahan penyusunan laporan dan perumusan rekomendasi bagi kegiatan edukasi berikutnya.

Hasil dan pembahasan

Tahap persiapan

Tahap persiapan merupakan langkah awal untuk memastikan bahwa kegiatan pengabdian kepada masyarakat sesuai dengan kebutuhan peserta dan dapat dilaksanakan secara terarah. Kegiatan dilaksanakan di balai kelurahan Wonolopo, kecamatan Mijen, kota Semarang, pada Senin, 21 September 2026. Persiapan kegiatan mencakup penyusunan materi edukasi, koordinasi pelaksanaan dengan pihak kelurahan, pendataan peserta, serta penyiapan tempat dan media pendukung. Materi dirancang untuk membahas ancaman digital yang relevan dengan aktivitas masyarakat dan pelaku UMKM, terutama penipuan melalui undangan aplikasi *android package kit* (APK) palsu, phishing, pencurian data pribadi, serta penyalahgunaan akun dan transaksi digital.

Penyusunan materi tersebut diarahkan agar peserta tidak hanya memperoleh informasi mengenai bentuk-bentuk penipuan, tetapi juga memahami langkah pencegahan yang dapat diterapkan dalam penggunaan perangkat dan layanan digital. Dengan demikian, tahap persiapan menjadi landasan bagi penyampaian edukasi yang kontekstual, praktis, dan berkaitan dengan kebutuhan perlindungan aktivitas usaha. Rangkaian persiapan juga menghasilkan kesiapan pelaksanaan kegiatan, baik dari segi materi, koordinasi, maupun sarana pendukung.

Tahap pelaksanaan edukasi

Pelaksanaan edukasi diikuti oleh 45 peserta, yang terdiri atas 35 laki-laki (77,78%) dan 10 perempuan (22,22%). Komposisi tersebut menunjukkan bahwa peserta laki-laki merupakan kelompok mayoritas dalam kegiatan ini. Meskipun demikian, data jenis kelamin hanya menggambarkan karakteristik demografis peserta dan tidak dapat digunakan untuk menyimpulkan perbedaan tingkat literasi digital atau kebutuhan keamanan digital antara laki-laki dan perempuan. Dokumentasi penyampaian materi oleh narasumber ditampilkan pada Gambar 2 dan Gambar 3.



Gambar 2 penyampaian materi edukasi *anti-scam* oleh narasumber



Gambar 3 pemaparan materi keamanan digital kepada peserta

Materi edukasi difokuskan pada tiga bentuk ancaman digital yang berpotensi mengganggu keamanan individu maupun aktivitas usaha. Pertama, peserta diberikan penjelasan mengenai modus undangan APK palsu, yaitu penyebaran berkas aplikasi yang disamarkan sebagai undangan, dokumen pengiriman barang, atau informasi lain untuk mendorong penerima memasang aplikasi dari sumber yang tidak tepercaya. Peserta diarahkan agar tidak langsung membuka atau memasang berkas aplikasi yang diterima melalui pesan, melainkan memeriksa konteks pesan, mengonfirmasi identitas pengirim melalui saluran yang dapat dipercaya, dan menghindari pemasangan aplikasi yang tidak jelas asal-usulnya.

Kedua, materi *phishing* menekankan pengenalan pesan dan tautan yang dirancang menyerupai komunikasi resmi. Peserta diberikan pemahaman mengenai pentingnya memeriksa alamat situs, identitas pengirim, serta isi pesan yang meminta informasi sensitif atau mendesak penerima untuk segera bertindak. Pesan yang mengandung ancaman pemblokiran akun, permintaan verifikasi yang tidak wajar, atau penawaran keuntungan yang tidak masuk akal perlu diperiksa secara kritis sebelum ditindaklanjuti. Ketiga, materi perlindungan data pribadi membahas risiko penyalahgunaan kata sandi, PIN, kode *one-time password* (OTP), informasi rekening, dan data lain yang dapat digunakan untuk mengambil alih akun atau melakukan penipuan atas nama korban.

Penyampaian materi dilengkapi dengan arahan praktis untuk memperkuat keamanan akun dan transaksi digital. Peserta diingatkan agar menggunakan kata sandi yang kuat dan berbeda untuk akun penting, mengaktifkan autentikasi dua faktor apabila tersedia, memeriksa izin akses aplikasi, serta memperbarui perangkat dan aplikasi secara berkala. Dalam konteks transaksi UMKM, peserta juga diarahkan untuk memverifikasi pembayaran melalui aplikasi perbankan atau penyedia layanan pembayaran resmi, bukan hanya mengandalkan tangkapan layar bukti transfer. Langkah-langkah tersebut ditujukan untuk membantu peserta mengenali risiko dan menerapkan kebiasaan yang lebih aman dalam berkomunikasi dengan pelanggan, mengelola akun bisnis, serta melakukan transaksi digital.

Selain penyampaian materi, kegiatan dilengkapi dengan sesi diskusi dan tanya jawab sebagai ruang bagi peserta untuk mengklarifikasi informasi dan membahas persoalan yang berkaitan dengan penipuan online. Beberapa peserta mengajukan pertanyaan mengenai cara mengantisipasi pesan mencurigakan dan tindakan yang perlu dilakukan apabila terindikasi menjadi korban penipuan. Narasumber menjelaskan pentingnya menghentikan interaksi yang mencurigakan, memverifikasi informasi melalui saluran resmi, mengamankan akun, dan menghubungi bank atau penyedia layanan pembayaran apabila terdapat risiko terhadap rekening. Peserta juga diingatkan untuk menyimpan bukti percakapan dan transaksi guna mendukung proses pelaporan. Dokumentasi interaksi tersebut disajikan pada Gambar 4 dan Gambar 5.



Gambar 4 sesi tanya jawab peserta dengan narasumber

Sesi interaktif tersebut melengkapi penyampaian materi dengan memberikan kesempatan kepada peserta untuk menghubungkan informasi yang diperoleh dengan persoalan keamanan digital yang mereka temui. Namun, pertanyaan dan partisipasi dalam

diskusi merupakan indikator keterlibatan selama kegiatan, bukan bukti langsung bahwa seluruh peserta telah menguasai atau menerapkan langkah-langkah pencegahan yang dijelaskan.



Gambar 5 diskusi mengenai pencegahan dan penanganan penipuan online

Tahap evaluasi

Tahap evaluasi dilakukan melalui pengumpulan umpan balik peserta menggunakan kuesioner untuk memperoleh gambaran mengenai penerimaan terhadap materi edukasi. Ringkasan pelaksanaan kegiatan yang ditampilkan pada Gambar 6 memuat tiga informasi utama, yaitu jumlah peserta, komposisi peserta berdasarkan jenis kelamin, dan tingkat kepuasan terhadap materi. Berdasarkan infografik tersebut, jumlah peserta tercatat sebanyak 45 orang, terdiri atas 35 laki-laki atau 77,78% dan 10 perempuan atau 22,22%. Dari aspek kepuasan, sebanyak 93% peserta dinyatakan sangat puas terhadap materi yang disampaikan.



Gambar 6 ringkasan pelaksanaan kegiatan pengabdian kepada masyarakat

Persentase kepuasan sebesar 93% menunjukkan bahwa materi edukasi memperoleh respons positif dari peserta berdasarkan hasil evaluasi yang tersedia. Angka tersebut

memberikan gambaran awal bahwa topik keamanan digital yang disampaikan diterima dengan baik oleh peserta kegiatan. Meskipun demikian, interpretasi hasil perlu memperhatikan keterbatasan informasi pada infografik. Jumlah peserta kegiatan tercatat sebanyak 45 orang, tetapi jumlah responden yang benar-benar mengisi kuesioner, jumlah butir pertanyaan, dan distribusi jawaban untuk kategori kepuasan lainnya belum dijelaskan secara terperinci. Oleh karena itu, persentase 93% dilaporkan sesuai dengan ringkasan evaluasi yang tersedia dan tidak langsung dikonversi menjadi jumlah peserta tertentu.

Evaluasi ini juga belum mencakup pengukuran pengetahuan sebelum dan sesudah edukasi maupun pengamatan terhadap penerapan perilaku keamanan digital setelah kegiatan. Dengan demikian, hasil survei digunakan untuk menggambarkan penerimaan peserta terhadap materi, bukan untuk menyatakan bahwa pengetahuan meningkat sebesar 93% atau bahwa risiko penipuan telah menurun. Data evaluasi tersebut selanjutnya dapat dimanfaatkan sebagai bahan penyusunan laporan kegiatan dan pertimbangan untuk perbaikan program edukasi berikutnya.

Edukasi keamanan digital sebagai bagian dari penguatan kapasitas UMKM

Kegiatan edukasi *anti-scam* menempatkan keamanan digital sebagai bagian yang tidak terpisahkan dari pemanfaatan teknologi dalam aktivitas ekonomi. Digitalisasi memberikan peluang bagi UMKM untuk memperluas pemasaran, mempermudah komunikasi dengan pelanggan, dan meningkatkan efisiensi transaksi. Akan tetapi, manfaat tersebut dapat disertai risiko ketika pelaku usaha belum memiliki kebiasaan yang memadai dalam memeriksa keaslian pesan, menjaga kerahasiaan data, dan mengamankan akun yang digunakan untuk menjalankan usaha. Oleh karena itu, literasi digital perlu mencakup tidak hanya kemampuan menggunakan aplikasi, tetapi juga kemampuan menilai risiko dan mengambil keputusan secara aman ketika berinteraksi di ruang digital.

Pandangan tersebut sejalan dengan Anan et al. (2024), yang membahas peningkatan kesadaran digital untuk pencegahan penipuan online pada kelompok UMKM, serta Muslikhun et al. (2024), yang mengangkat upaya mengurangi risiko penipuan jual beli online melalui pelatihan bagi pelaku UMKM. Kedua rujukan tersebut menunjukkan relevansi edukasi keamanan digital dalam konteks kegiatan ekonomi masyarakat. Kontribusi kegiatan di Wonolopo terletak pada penggabungan pengenalan modus penipuan, perlindungan informasi pribadi, keamanan akun, dan verifikasi transaksi ke dalam satu rangkaian edukasi. Penggabungan tersebut penting karena risiko digital yang dihadapi pelaku UMKM tidak berdiri sendiri: satu pesan mencurigakan dapat menjadi pintu masuk bagi pencurian data, pengambilalihan akun, atau penipuan transaksi.

Dari perspektif pengabdian kepada masyarakat, pendekatan edukatif dan partisipatif memungkinkan materi keamanan digital disampaikan dalam konteks yang dekat dengan pengalaman peserta. Meskipun demikian, pelaksanaan satu kali kegiatan belum cukup untuk membuktikan terbentuknya ketahanan digital dalam jangka panjang. Ketahanan digital memerlukan kemampuan mengenali ancaman, menerapkan langkah pencegahan, merespons insiden, dan memulihkan keamanan setelah terjadi gangguan. Dengan demikian, kegiatan ini lebih tepat diposisikan sebagai upaya awal untuk memperkuat kesadaran dan memberikan dasar keterampilan pencegahan, yang selanjutnya perlu didukung oleh praktik berulang dan pendampingan.

Relevansi materi APK palsu dan phishing terhadap risiko penipuan online

Penekanan pada modus APK palsu dan *phishing* relevan karena kedua bentuk ancaman tersebut memanfaatkan interaksi digital yang tampak wajar untuk mendorong pengguna melakukan tindakan berisiko. Pada modus APK palsu, penerima dapat diarahkan untuk memasang aplikasi yang tidak tepercaya melalui pesan yang menyerupai dokumen atau informasi sehari-hari. Sementara itu, *phishing* memanfaatkan pesan atau situs yang menyerupai layanan resmi untuk memperoleh informasi sensitif. Dalam kedua situasi tersebut, keputusan pengguna untuk langsung mempercayai pesan tanpa memverifikasi sumber dapat meningkatkan risiko keamanan.

Eriana et al. (2025) membahas sosialisasi keamanan digital untuk mengatasi *phishing* dan APK berbahaya, sedangkan Nugroho et al. (2023) menekankan edukasi keamanan digital untuk meningkatkan kewaspadaan terhadap tautan *phishing*. Hariyadi et al. (2025) juga mengangkat peningkatan kewaspadaan terhadap kejahatan siber melalui aplikasi WhatsApp. Literatur tersebut memiliki keterkaitan langsung dengan fokus materi kegiatan di Wonolopo, yaitu membangun kebiasaan memeriksa pengirim, menghindari pemasangan aplikasi dari sumber yang tidak tepercaya, dan tidak memberikan informasi sensitif melalui tautan yang belum terverifikasi.

Implikasi penting dari materi tersebut adalah bahwa pencegahan tidak cukup hanya dilakukan dengan menghafal jenis-jenis penipuan. Peserta perlu memahami pola manipulasi yang digunakan pelaku, seperti menciptakan rasa takut, mendesak penerima bertindak cepat, atau menawarkan keuntungan yang tidak masuk akal. Pemahaman terhadap pola tersebut dapat menjadi dasar pengambilan keputusan yang lebih hati-hati. Namun, karena kegiatan ini belum menggunakan pengukuran sebelum dan sesudah edukasi, belum dapat dipastikan sejauh mana kemampuan peserta dalam mengidentifikasi modus tersebut berubah setelah mengikuti kegiatan. Untuk pengembangan selanjutnya, demonstrasi dapat dilengkapi dengan latihan klasifikasi pesan, yaitu meminta peserta membedakan pesan yang relatif aman, pesan mencurigakan, dan pesan yang perlu diverifikasi melalui saluran resmi.

Perlindungan data pribadi dan keamanan transaksi sebagai pengelolaan risiko usaha

Perlindungan data pribadi memiliki implikasi yang lebih luas daripada sekadar menjaga kerahasiaan informasi individu. Dalam kegiatan UMKM, akun media sosial, akun marketplace, nomor telepon, alamat surat elektronik, dan akses layanan pembayaran dapat menjadi bagian dari infrastruktur operasional usaha. Jika akun tersebut diambil alih atau disalahgunakan, pelaku usaha berpotensi kehilangan akses komunikasi dengan pelanggan, menghadapi penyamaran identitas, dan mengalami gangguan transaksi. Risiko tersebut dapat memengaruhi kepercayaan konsumen, terutama ketika pelaku penipuan menggunakan identitas bisnis yang telah dikenal oleh pelanggan.

Silmina et al. (2025) membahas perlindungan data pribadi dan pencegahan penipuan online dalam kegiatan literasi digital, sedangkan Ramadhan et al. (2026) mengangkat aspek tanggung jawab perdata dalam konteks penipuan online berbasis *phishing*. Susan et al. (2026) juga membahas risiko penyalahgunaan data pribadi pada media sosial. Rujukan tersebut memperkuat pentingnya menghubungkan keamanan data, keamanan akun, dan kewaspadaan transaksi dengan aktivitas digital sehari-hari. Dalam konteks UMKM, penggunaan kata sandi yang kuat, aktivasi autentikasi dua faktor, pembatasan akses admin, dan pengamanan akun pemulihan dapat menjadi bagian dari pengendalian risiko yang perlu diterapkan secara konsisten.

Verifikasi transaksi juga menjadi aspek penting karena bukti pembayaran berupa gambar atau tangkapan layar tidak dengan sendirinya memastikan bahwa dana telah masuk ke rekening penerima. Pemeriksaan mutasi rekening atau saldo melalui aplikasi resmi merupakan langkah yang lebih dapat diandalkan sebelum barang diserahkan atau pesanan dinyatakan selesai. Selain itu, pelaku usaha perlu membangun kebiasaan memverifikasi perubahan informasi pembayaran melalui saluran komunikasi yang telah diketahui kebenarannya. Pendekatan ini memperlihatkan bahwa edukasi *anti-scam* perlu diterjemahkan menjadi prosedur operasional sederhana yang dapat diterapkan oleh pemilik usaha maupun karyawan, bukan hanya menjadi pengetahuan individual. Dengan demikian, kontribusi edukasi keamanan digital bagi UMKM dapat diperluas melalui penerapan prosedur pengamanan yang konsisten, seperti pengelolaan akses akun, verifikasi pembayaran, dan penyimpanan bukti transaksi. Walaupun prosedur tersebut tidak dapat menghilangkan seluruh risiko penipuan, penerapannya dapat membantu mengurangi peluang terjadinya kesalahan yang dimanfaatkan oleh pelaku kejahatan digital.

Peran diskusi partisipatif dan penanganan awal insiden

Sesi tanya jawab memberikan ruang untuk mengklarifikasi materi dan membahas persoalan yang dianggap relevan oleh peserta. Dalam edukasi keamanan digital, ruang interaksi semacam ini penting karena ancaman siber sering kali muncul dalam bentuk yang berubah-ubah dan tidak selalu mudah dikenali melalui penjelasan teoritis. Diskusi memungkinkan narasumber menguraikan alasan di balik suatu tindakan pencegahan, misalnya mengapa pengguna tidak boleh membagikan kode OTP atau mengapa bukti transfer perlu diverifikasi melalui rekening penerima. Namun, efektivitas diskusi tidak seharusnya hanya dinilai dari berlangsungnya pertanyaan dan jawaban; pemahaman peserta perlu dikonfirmasi melalui latihan atau evaluasi yang sesuai.

Rismawati et al. (2026) mengangkat pemberdayaan masyarakat melalui literasi hukum dan digital untuk pencegahan kekerasan siber dan penipuan online. Sementara itu, Syaiful & Khoir (2026) membahas peningkatan literasi dan kesadaran keamanan siber melalui edukasi pencegahan *phishing* dan penipuan online. Kegiatan tersebut relevan sebagai landasan untuk melihat edukasi keamanan digital sebagai proses pemberdayaan, yakni membekali masyarakat dengan pengetahuan yang dapat digunakan ketika menghadapi risiko. Dalam kegiatan di Wonolopo, penekanan pada verifikasi informasi, pengamanan akun, dan penyimpanan bukti insiden merupakan langkah awal untuk mendorong respons yang lebih terarah ketika terjadi dugaan penipuan.

Penanganan insiden juga perlu dibahas sebagai bagian dari literasi keamanan digital. Apabila peserta terlanjur memasang APK yang mencurigakan, langkah yang diperlukan bukan sekadar menghapus aplikasi, tetapi juga mempertimbangkan kemungkinan bahwa kredensial atau akses perangkat telah disalahgunakan. Pengamanan perlu dilakukan dengan menggunakan perangkat lain yang tepercaya untuk menghubungi bank atau penyedia layanan terkait dan mengganti kredensial penting. Jika terdapat indikasi kompromi perangkat, pemeriksaan oleh tenaga teknis yang tepercaya dapat diperlukan. Bukti percakapan dan transaksi sebaiknya disimpan untuk mendukung pelaporan. Penjelasan mengenai respons insiden ini melengkapi pendekatan preventif karena pengguna juga perlu mengetahui tindakan yang dapat diambil setelah pencegahan tidak berhasil.

Untuk memperkuat manfaat kegiatan berikutnya, sesi diskusi dapat dikembangkan menjadi simulasi respons insiden berbasis skenario. Peserta, misalnya, diminta menentukan

langkah yang perlu dilakukan ketika menerima undangan APK mencurigakan, menemukan tautan yang menyerupai layanan resmi, atau menerima bukti transfer yang belum terkonfirmasi. Metode tersebut dapat membantu menilai apakah peserta mampu menerapkan pengetahuan pada situasi praktis. Hasil latihan dapat digunakan untuk mengidentifikasi materi yang perlu diulang atau diperdalam dalam pendampingan selanjutnya.

Interpretasi survei kepuasan dan implikasi evaluasi program

Ringkasan evaluasi kegiatan menunjukkan bahwa 93% peserta menyatakan sangat puas terhadap materi edukasi. Temuan tersebut dapat diinterpretasikan sebagai respons positif terhadap materi yang disajikan. Dalam konteks pengabdian kepada masyarakat, penerimaan peserta merupakan aspek yang penting karena materi yang dinilai relevan dan mudah diikuti dapat menjadi dasar untuk mempertahankan keterlibatan peserta dalam program edukasi berikutnya. Namun, kepuasan merupakan penilaian subjektif terhadap pengalaman mengikuti kegiatan dan tidak identik dengan penguasaan materi atau perubahan perilaku keamanan digital.

Perbedaan antara penerimaan kegiatan dan hasil pembelajaran perlu diperhatikan ketika menafsirkan data evaluasi. Persentase kepuasan sebesar 93% tidak berarti bahwa pengetahuan peserta meningkat sebesar 93%, dan angka tersebut juga tidak menunjukkan bahwa 93% peserta telah mampu mengidentifikasi semua modus penipuan yang dijelaskan. Selain itu, tanpa informasi yang lebih rinci mengenai jumlah responden yang mengisi kuesioner, butir pertanyaan, dan kategori jawaban, hasil tersebut belum dapat dianalisis lebih jauh berdasarkan aspek tertentu. Oleh sebab itu, angka 93% perlu dilaporkan sebagai hasil survei kepuasan sesuai dengan data yang tersedia, tanpa menarik kesimpulan kausal mengenai efektivitas edukasi.

Untuk meningkatkan kualitas evaluasi, kegiatan berikutnya disarankan menggunakan beberapa indikator yang saling melengkapi. Pertama, *pre-test* dan *post-test* dapat digunakan untuk mengukur perubahan pengetahuan peserta mengenai APK palsu, *phishing*, perlindungan data, dan verifikasi transaksi. Kedua, simulasi kasus dapat digunakan untuk menilai kemampuan peserta dalam mengenali pesan mencurigakan dan memilih tindakan yang tepat. Ketiga, survei kepuasan dapat dipertahankan untuk mengevaluasi relevansi materi, kejelasan penyampaian, dan manfaat kegiatan menurut peserta. Jika memungkinkan, tindak lanjut beberapa minggu setelah kegiatan juga dapat dilakukan untuk mengetahui apakah peserta menerapkan langkah pengamanan akun dan transaksi dalam aktivitas usaha mereka.

Penggunaan indikator yang berbeda akan membantu memisahkan tiga aspek evaluasi, yaitu penerimaan peserta, pencapaian pembelajaran, dan penerapan pengetahuan dalam praktik. Pendekatan tersebut dapat menghasilkan dasar evaluasi yang lebih kuat daripada hanya mengandalkan satu persentase kepuasan. Dengan demikian, hasil kegiatan di Wonolopo dapat menjadi pijakan awal untuk mengembangkan program edukasi *anti-scam* yang lebih terukur, berkelanjutan, dan sesuai dengan kebutuhan pelaku UMKM.

Implikasi dan arah pengembangan kegiatan

Kegiatan ini memperlihatkan bahwa edukasi *anti-scam* dapat menjadi salah satu bentuk intervensi preventif untuk memperkenalkan risiko keamanan digital dan langkah-langkah perlindungan yang relevan bagi pelaku UMKM. Materi yang menghubungkan

pengenalan ancaman dengan perlindungan akun, data pribadi, dan transaksi usaha membantu menempatkan keamanan digital sebagai bagian dari pengelolaan usaha. Meskipun demikian, kegiatan satu kali dengan evaluasi yang berfokus pada kepuasan belum cukup untuk menyimpulkan bahwa ketahanan digital peserta telah meningkat secara berkelanjutan.

Arah pengembangan program dapat difokuskan pada pelatihan berbasis kasus, pendampingan pengamanan akun bisnis, penyusunan prosedur verifikasi transaksi, serta evaluasi pembelajaran sebelum dan sesudah kegiatan. Kolaborasi dengan pemerintah kelurahan, komunitas UMKM, lembaga keuangan, dan pihak yang memiliki kompetensi keamanan digital juga dapat dipertimbangkan untuk memperluas jangkauan edukasi. Pengembangan tersebut sejalan dengan kebutuhan untuk mengintegrasikan literasi digital ke dalam praktik usaha sehari-hari. Dengan dukungan materi yang kontekstual, latihan praktis, dan evaluasi yang lebih komprehensif, edukasi *anti-scam* diharapkan dapat membantu pelaku UMKM membangun kebiasaan digital yang lebih aman dan meningkatkan kesiapan mereka dalam menghadapi ancaman penipuan online.

Kesimpulan

Kegiatan pengabdian kepada masyarakat telah dilaksanakan di balai kelurahan Wonolopo, kecamatan Mijen, kota Semarang, dengan melibatkan 45 peserta, terdiri atas 35 laki-laki dan 10 perempuan. Kegiatan ini berfokus pada peningkatan pemahaman masyarakat mengenai modus penipuan digital, khususnya undangan APK palsu, *phishing*, pencurian data pribadi, serta penyalahgunaan akun dan transaksi digital. Melalui penyampaian materi, diskusi, dan tanya jawab, peserta memperoleh informasi praktis mengenai cara mengenali pesan mencurigakan, melindungi informasi pribadi, mengamankan akun, memverifikasi transaksi, dan melakukan tindakan awal ketika menghadapi dugaan penipuan. Hasil survei menunjukkan bahwa 93% peserta menyatakan sangat puas terhadap materi yang disampaikan. Capaian tersebut menunjukkan penerimaan yang positif terhadap kegiatan dan relevansi topik keamanan digital bagi masyarakat, meskipun belum dapat digunakan untuk menyimpulkan peningkatan pengetahuan atau perubahan perilaku peserta secara langsung.

Kegiatan ini memberikan kontribusi praktis berupa penguatan edukasi preventif mengenai keamanan digital sebagai bagian dari pengelolaan risiko usaha UMKM. Pemahaman mengenai pencegahan penipuan online diharapkan dapat mendorong pelaku usaha untuk lebih berhati-hati dalam berkomunikasi, mengelola akun bisnis, melindungi data pribadi, dan melakukan transaksi digital sehingga kepercayaan pelanggan serta keberlangsungan usaha dapat lebih terjaga. Untuk meningkatkan keberlanjutan dan efektivitas program, kegiatan serupa perlu dikembangkan melalui pelatihan berbasis simulasi kasus, pendampingan penerapan keamanan akun dan transaksi, serta evaluasi menggunakan *pre-test* dan *post-test* untuk mengukur perubahan pengetahuan peserta. Dengan demikian, edukasi *anti-scam* dapat menjadi langkah awal dalam membangun ketahanan digital UMKM yang lebih adaptif, aman, dan bertanggung jawab dalam menghadapi perkembangan ancaman di ekosistem ekonomi digital.

Daftar pustaka

Al-Okaily, A., & Al-Okaily, M. (2026). Financial digitalization: how does FinTech innovation enhance financial resilience and competitiveness? An empirical study. *Competitiveness*

Review: An International Business Journal, *36*(3), 576–596. https://doi.org/10.1108/CR-04-2025-0119

Anan, M., Rahmah, S. A., & Risuhendri, R. (2024). Meningkatkan Kesadaran Digital Dalam Pencegahan Penipuan Online Untuk Kelompok UMKM Desa Tanjung Haratan. *ABDI DALEM: Jurnal Pengabdian Kepada Masyarakat*, *1*(2), 56–63. https://doi.org/10.70585/abdidalem.v1i2.29

Eriana, E. S., Zein, A., Wati, F. E., & Buminata, M. S. A. (2025). Sosialisasi Keamanan Digital Untuk Mengatasi Phishing Dan Apk Berbahaya. *Attamkiim: Jurnal Pengabdian Masyarakat*, *2*(1), 85–90. https://doi.org/10.62070/attamkiim.v2i1.248

Faturrahman, F., Subhan, E. S., & Shoalihin, S. (2025). Pengembangan UMKM Berbasis Transformasi Digital Dalam Mendorong Pertumbuhan Ekonomi Lokal. *Advances in Management & Financial Reporting*, *3*(3), 990–1008. https://doi.org/10.60079/amfr.v3i3.622

Ferdinand, A. (2021). *Metode Penelitian Manajemen: Pedoman penelitian Untuk Skripsi, Tesis, Disertasi Ilmiah Manajemen*. Universitas Diponegoro.

Hariyadi, D., Lahitani, A. R., Dwijayanti, I., Kusumaningtyas, K., & Dewi, G. S. (2025). Peningkatan Kewaspadaan Terhadap Kejahatan Siber Pada Aplikasi Whatsapp Di Kalurahan Bangunjiwo. *Jurnal Pengabdian Masyarakat - Teknologi Digital Indonesia.*, *4*(2), 98. https://doi.org/10.26798/jpm.v4i2.1476

Kumar, J., & Rani, V. (2026). Investigating the dynamics of FinTech adoption: an empirical study from the perspective of mobile banking. *Journal of Economic and Administrative Sciences*, *42*(1), 123–140. https://doi.org/10.1108/JEAS-12-2023-0334

Muslikhun, A., Rowiyani, R., & Mukhlidin, M. (2024). Pemanfaatan Aplikasi Get Contact Untuk Mengurangi Tingkat Penipuan Jual Beli Online (Pelatihan Kepada Pelaku UMKM di Desa Margosari Limbangan Kendal). *Jurnal Pengabdian Masyarakat Intimas (Jurnal INTIMAS): Inovasi Teknologi Informasi Dan Komputer Untuk Masyarakat*, *4*(1), 55–62. https://unisbank.ac.id/ojs/index.php/intimas/article/view/9781

Nugroho, H., Nur Ihsan, M., Haryoko, A., Ma`arif, F., & Alifah, F. (2023). Edukasi Keamanan Digital Untuk Meningkatkan Kewaspadaan Masyarakat Terhadap Link Phising. *Alahyan Jurnal Pengabdian Masyarakat Multidisiplin*, *1*(2), 104–111. https://doi.org/10.61492/ecos-preneurs.v1i2.60

Pembayun, J. G., Arisa, F., Yusliwidaka, A., Rhizky, D. P., & Rihardi, S. A. (2026). Sosialisasi Pencegahan Penipuan Online Berbasis E-Commerce Di Desa Sukosari, Kecamatan Bandongan, Kabupaten Magelang. *Jurnal Abdimas Bina Bangsa*, *7*(1), 239–245. https://jabb.lppmbinabangsa.id/index.php/jabb/article/view/2024

Purnamasari, V., & Putri, E. R. P. (2026). Literasi Digital dan Keamanan Siber untuk Pemuda Desa: Waspada Investasi Bodong dan Penipuan Online. *KOMUNITA: Jurnal Pengabdian Dan Pemberdayaan Masyarakat*, *5*(1), 10–19. https://doi.org/10.60004/komunita.v5i1.373

Ramadani, N. (2026). Peningkatan Literasi Digital Melalui Edukasi Keamanan Digital Dan Etika Bermedia Sosial. *Abdi Reksa*, *7*(1), 21–25. https://doi.org/10.33369/abdireksa.v7.i1.21-25

Ramadhan, N. A., Saputra, A. A., Sulestari, P. N., Firmansyah, T. A., Simamora, R. E., Dwinanda, E. B. H., Hafid, D., Pribadi, D. S., & Nafhani, A. (2026). Meningkatkan Kesadaran Hukum Perbankan Masyarakat terhadap Tanggung Jawab Perdata atas Penipuan Online Phishing. *Jurnal Pengabdian Masyarakat Bangsa*, *4*(5), 2490–2500.

https://doi.org/10.59837/jpmba.v4i5.4638

Rismawati, R., Said, T. G., & Amar, M. (2026). Pemberdayaan Masyarakat Melalui Literasi Hukum dan Digital dalam Pencegahan Kekerasan Siber dan Penipuan Online di Desa Mandalle. *Jurnal Pengabdian Kepada Masyarakat Patikala*, *5*(3), 4119–4127. https://doi.org/10.51574/patikala.v5i3.4735

Silmina, E. P., Sarmin, S., Umar, R., & Herman, H. (2025). Meningkatkan Literasi Digital: Perlindungan Data Pribadi dan Pencegahan Penipuan Online di Lingkungan PRA Ngadisuryan. *Jurnal Pengabdian UntukMu NegeRI*, *9*(2), 322–330. https://doi.org/10.37859/jpumri.v9i2.9860

Sugiyono, S. (2020). *Metode Penelitian Kualitatif*. Alfabeta.

Sugiyono, S. (2022). *Quantitative, Qualitative Research Methods*. Alfabeta.

Susan, S., Aditya, A. A., Afgiansyah, S., & Jaza, F. D. (2026). Analisis Resiko Penyalahgunaan Data Pribadi pada Media Sosial. *Jurnal Ilmiah Wahana Pendidikan*, *12*(5), 205–219. https://www.jurnal.peneliti.net/index.php/JIWP/article/view/13203

Syaiful, S., & Khoir, A. (2026). Peningkatan Literasi Dan Kesadaran Keamanan Siber Melalui Edukasi Pencegahan Phishing Dan Penipuan Online Bagi Masyarakat. *Gotong Royong*, *3*(2), 105–112. https://doi.org/10.63935/gr.v3i2.336

Usnur, U. H., Dinata, L. A. I., Sari, A. E., Nadira, N. F., Purba, H. A., & Damanik, N. S. (2026). Penguatan Literasi Digital dalam Membangun Ketahanan Sosial Masyarakat di Era Transformasi Digital. *Islamic Education*, *6*(1), 151–159. https://doi.org/10.57251/ie.v6i1.2214

Zunairoh, & Wijaya, L. I. (2024). Fintech, Social Capital and Performance of Indonesian MSMEs. *Millennial Asia*. https://doi.org/10.1177/09763996241284692