JURNAL PENGABDIAN SOSIAL
e-ISSN : 3031- 0059
Volume 3, No. 10, Tahun 2026
https://ejournal.jurnalpengabdiansosial.com/index.php/jps

Menuju Kampung Sadar Keamanan Digital: Edukasi Pencegahan Penipuan Daring bagi Pengrajin Kayu di Boyolali

Muhnizar Siagian[1], Erina Ikawati[2], Ignatius Agung Satyawan[3], Lukman Fahmi Djarwono[4], Muhammad Chanif Hidayat[5], Andriko Sandria[6], Bintang Indra Wibisono[7], Salieg Luki Munestri[8]

[1,2,3,4,5,6,7,8] *Program Studi Hubungan Internasional, Fakultas Ilmu Sosial dan Politik, Universitas Sebelas Maret, Surakarta, Indonesia*

Received : 21 Juli 2026, Revised : 3 Agustus 2026, Published : 11 Agustus 2026

Corresponding Author
Nama Penulis : Erina Ikawati
E-mail: erinaikawati@staff.uns.ac.id

Abstrak

Digitalisasi pemasaran dan pembayaran memperluas peluang usaha pengrajin kayu, tetapi juga meningkatkan risiko penipuan daring akibat keterbatasan pemahaman keamanan digital. Kegiatan pengabdian ini bertujuan memperkuat pemahaman dasar dan kewaspadaan kolektif anggota Persatuan Pengrajin Seluruh Bekangan sebagai tahap awal menuju Kampung Sadar Keamanan Digital. Kegiatan dilaksanakan di Dukuh Bekangan, Desa Sembungan, Kecamatan Nogosari, Kabupaten Boyolali, pada 23 Juni 2026 dan diikuti oleh 21 pengrajin kayu. Metode edukasi partisipatif berbasis kasus meliputi pemetaan pengetahuan awal secara lisan, pemaparan materi, diskusi pengalaman, simulasi pesan penipuan, demonstrasi verifikasi transaksi, post-test, pemasangan poster dan spanduk, serta tindak lanjut. Materi mencakup perlindungan PIN, kata sandi, dan OTP; phishing; file APK; penyamaran identitas; bukti transfer palsu; keamanan QRIS; pinjaman daring ilegal; perlindungan data pribadi; dan saluran pelaporan resmi. Kegiatan ini diharapkan menjadi langkah awal dalam membangun pengetahuan bersama, kebiasaan saling mengingatkan, dan komitmen terhadap penerapan transaksi digital yang lebih aman.

Kata kunci *– kampung sadar keamanan digital, keamanan digital, penipuan daring, pengrajin kayu, UMKM*

Abstract

The digitalization of marketing and payment systems has expanded business opportunities for woodcraft artisans but has also increased the risk of online fraud due to limited digital security awareness. This community service program aimed to strengthen the basic understanding and collective awareness of members of the Persatuan Pengrajin Seluruh Bekangan as an initial step toward establishing a Digital Security-Aware Village. The program was conducted in Bekangan Hamlet, Sembungan Village, Nogosari District, Boyolali Regency, on June 23, 2026, involving 21 woodcraft artisans. A case-based participatory education approach was implemented, including an oral assessment of participants' initial knowledge, educational sessions, experience-sharing discussions, fraud message simulations, transaction verification demonstrations, post-test, installation of posters and banners, and follow-up activities. The educational materials covered the protection of PINs, passwords, and one-time passwords (OTPs); phishing; malicious APK files; identity impersonation; fake proof of bank transfers; QRIS security; illegal online lending; personal data protection; and official reporting channels. This program is expected to serve as an initial step in fostering shared knowledge, mutual awareness, and a collective commitment to safer digital transactions.

Keywords *- digital security, digital security-aware village, MSMEs, online fraud, woodcraft artisans*

How To Cite : *Siagian, M. ., Ikawati, E. ., Satyawan, I. A. ., Djarwono, L. F. ., Hidayat, M. C. ., Sandria, A. ., Wibisono, B. I. ., & Munestri, S. L. . (2026). Menuju Kampung Sadar Keamanan Digital: Edukasi Pencegahan Penipuan Daring bagi Pengrajin Kayu di Boyolali. Jurnal Pengabdian Sosial, 3(10), 841 - 853. https://doi.org/10.59837/v1ddta95*

PENDAHULUAN

Persatuan Pengrajin Seluruh Bekangan merupakan komunitas pengrajin kayu di Dukuh Bekangan, Desa Sembungan, Kecamatan Nogosari, Kabupaten Boyolali. Anggota kelompok memproduksi perabot dan berbagai kerajinan berbahan kayu serta mulai menggunakan aplikasi percakapan, media sosial, transfer bank, dan layanan pembayaran digital untuk menawarkan produk, berkomunikasi dengan pelanggan, mengonfirmasi pesanan, dan menerima pembayaran. Penggunaan media digital tersebut memperluas jangkauan usaha, tetapi sekaligus membuat sebagian proses transaksi bergantung pada pesan, identitas akun, tautan, dan bukti pembayaran yang diterima melalui perangkat digital. Ketika pemeriksaan identitas dan pembayaran belum dilakukan melalui prosedur yang konsisten, pesan palsu atau bukti transfer yang tidak sah dapat menimbulkan kerugian langsung bagi pelaku usaha (Bai et al., 2021; Kilay et al., 2022).

Pemilihan Persatuan Pengrajin Seluruh Bekangan sebagai mitra tidak semata-mata didasarkan pada profesi mereka sebagai pengrajin kayu, melainkan pada paparan terhadap transaksi digital dan kebutuhan pendampingan yang telah teridentifikasi. Kegiatan pengabdian pada 2025 menunjukkan bahwa sebagian anggota masih mengalami kesulitan membedakan tautan *phishing* dari tautan yang sah serta merasa khawatir ketika menggunakan layanan *mobile banking* (Siagian et al., 2025). Temuan tersebut menunjukkan adanya jarak antara penggunaan teknologi dalam kegiatan usaha dan kemampuan mengelola risiko yang menyertainya. Satu kali penyuluhan juga belum cukup untuk membentuk kebiasaan memeriksa identitas, memastikan pembayaran, melindungi data autentikasi, dan meminta bantuan ketika menghadapi pesan mencurigakan. Oleh karena itu, kegiatan lanjutan diperlukan untuk memperkuat pengetahuan sebelumnya melalui latihan pengambilan keputusan, demonstrasi, pengulangan pesan, dan dukungan antaranggota komunitas.

Kebutuhan tersebut berkaitan dengan proses digitalisasi usaha mikro, kecil, dan menengah secara lebih luas. Aplikasi pesan instan, media sosial, transfer bank, dompet digital, dan *Quick Response Code Indonesian Standard* (QRIS) memungkinkan pelaku usaha berkomunikasi dengan konsumen dan menyelesaikan transaksi secara lebih cepat. Penggunaan layanan e-commerce dan pembayaran elektronik juga dapat mendukung kinerja dan jangkauan pasar UMKM (Kilay et al., 2022). Namun, kemampuan mengoperasikan layanan digital tidak selalu diikuti kemampuan melindungi perangkat, data pribadi, akun, dan transaksi (Afzal et al., 2025; Alharbi et al., 2021; Armenia et al., 2021). Kerangka Kompetensi Digital untuk Warga (*Digital Competence Framework for Citizens atau DigComp 2.2)* yang dikembangkan oleh Uni Eropa menempatkan kemampuan melindungi perangkat, data pribadi, privasi, dan kesejahteraan pengguna sebagai bagian penting dari kompetensi digital. Dengan demikian, digitalisasi usaha tidak cukup diukur dari penggunaan platform, tetapi juga dari kemampuan pengguna mengenali dan mengelola risikonya (Vuorikari et al., 2022).

Risiko yang dihadapi pelaku usaha tidak selalu berbentuk serangan teknis yang rumit. Penipuan daring sering memanfaatkan rekayasa sosial dengan menyamar sebagai pelanggan, petugas bank, penyedia layanan, anggota keluarga, atau pihak lain yang dianggap dapat dipercaya. Pelaku menciptakan rasa mendesak, menawarkan hadiah, menakut-nakuti korban, atau meminta tindakan segera agar calon korban tidak sempat melakukan pemeriksaan (Alkhalil et al., 2021; Lopes et al., 2024; Syafitri et al., 2022). Dalam kegiatan usaha pengrajin, modus tersebut dapat muncul dalam bentuk tangkapan layar bukti transfer palsu, akun pembeli fiktif, tautan hadiah, file APK berkedok undangan atau dokumen pengiriman, permintaan kode OTP, perubahan kode QRIS, penyamaran sebagai anggota keluarga, dan penawaran pinjaman daring yang tidak transparan. Risiko tersebut relevan bagi

usaha berbasis pesanan karena barang dapat diproduksi atau dikirim sebelum pemilik usaha memastikan bahwa dana benar-benar telah diterima.

Mayoritas anggota kelompok yang menjadi sasaran kegiatan berusia di atas 45 tahun dengan pengalaman penggunaan teknologi digital yang beragam. Karakteristik tersebut tidak digunakan untuk menyimpulkan bahwa peserta secara otomatis lebih mudah menjadi korban penipuan. Penelitian mengenai penipuan digital menunjukkan bahwa hubungan antara usia dan kerentanan tidak selalu konsisten, karena risiko juga dipengaruhi oleh pengalaman menggunakan teknologi, keterampilan keamanan digital, tingkat kepercayaan, fungsi kognitif, dan karakter pesan yang diterima (Burton et al., 2022; Shang et al., 2022; Yu et al., 2023). Sejumlah penelitian memang menemukan peningkatan kerentanan pada kelompok usia lebih tua dalam konteks tertentu, tetapi temuan tersebut tidak dapat digeneralisasi kepada seluruh pengguna dewasa (Pehlivanoglu et al., 2024; Pituk et al., 2025; Sur et al., 2023). Dalam kegiatan ini, usia dipertimbangkan terutama untuk memastikan bahwa bentuk komunikasi dan pembelajaran dapat diakses oleh peserta dengan tingkat pengalaman digital yang berbeda (Aly et al., 2025).

Karakteristik usaha dan peserta tersebut memerlukan pendekatan edukasi yang kontekstual. Usaha mikro tidak dapat diperlakukan sebagai kelompok yang homogen karena memiliki perbedaan dalam penggunaan perangkat, pola transaksi, pengalaman digital, dan kemampuan pengamanan (Chaudhary et al., 2023; Chidukwani et al., 2024; Shojaifar & Järvinen, 2021). Materi yang terlalu teknis atau tidak berhubungan dengan kegiatan sehari-hari berisiko sulit dipahami dan tidak diterapkan. Sebaliknya, contoh pesan yang menyerupai pengalaman peserta, simulasi permintaan transfer, demonstrasi pemeriksaan mutasi rekening, serta pembahasan alasan di balik suatu tindakan dapat membantu peserta menghubungkan konsep keamanan dengan keputusan praktis. Kajian mengenai pelatihan keamanan siber menunjukkan bahwa latihan berbasis skenario, contoh realistis, umpan balik, dan pengulangan dapat meningkatkan kemampuan pengguna dalam mengenali serta merespons ancaman digital (Baki & Verma, 2023).

Pendekatan komunitas juga diperlukan karena penipuan daring tidak hanya menimbulkan kerugian finansial, tetapi dapat memunculkan rasa malu, takut disalahkan, dan keengganan untuk menceritakan pengalaman. Hambatan tersebut dapat menyebabkan kejadian tidak dilaporkan dan informasi mengenai modus penipuan tidak menyebar kepada anggota lain. Penelitian mengenai korban kejahatan digital menunjukkan bahwa pengetahuan mengenai saluran bantuan dan dukungan sosial berpengaruh terhadap kesediaan korban untuk mencari pertolongan (Havers et al., 2024; Kemp & Erades Pérez, 2023; Parti & Tahir, 2023). Oleh sebab itu, edukasi dalam kegiatan ini tidak hanya diarahkan pada kemampuan mengenali pesan mencurigakan, tetapi juga pada pembentukan kebiasaan saling mengingatkan dan ruang berbagi yang tidak menyalahkan korban.

Kegiatan tahun 2026 merupakan kelanjutan dari pengabdian tahun sebelumnya dengan mengembangkan materi dari pengenalan risiko menuju latihan pengambilan keputusan dan penguatan kesadaran kolektif. Arah tersebut dirumuskan melalui gagasan Kampung Sadar Keamanan Digital. Istilah ini tidak digunakan untuk menyatakan bahwa seluruh warga telah menguasai keamanan digital atau bahwa lingkungan tersebut telah terbebas dari penipuan. Kampung Sadar Keamanan Digital dipahami sebagai arah pengembangan komunitas yang mengenali risiko, membiasakan pemeriksaan sebelum bertindak, melindungi informasi rahasia, berani meminta bantuan, dan bersedia berbagi informasi mengenai modus penipuan tanpa mempermalukan korban. Pembentukan identitas dan kebiasaan bersama tersebut menjadi fondasi bagi pengembangan prosedur verifikasi, kontak rujukan, dan mekanisme konsultasi yang lebih terstruktur pada tahap berikutnya.

Berdasarkan kondisi tersebut, kegiatan pengabdian ini bertujuan untuk: (1) memperkuat pemahaman dasar pengrajin mengenai bentuk dan ciri penipuan daring; (2) melatih langkah praktis dalam melindungi kredensial, memverifikasi identitas, dan memastikan transaksi; serta (3) membangun kesadaran kolektif sebagai tahap awal menuju Kampung Sadar Keamanan Digital. Artikel ini membahas pelaksanaan edukasi partisipatif berbasis kasus, respons peserta, hasil evaluasi

pembelajaran secara deskriptif, penggunaan media lingkungan, serta keterbatasan dan arah pengembangan program.

METODE

Lokasi, Waktu, dan Peserta

Kegiatan dilaksanakan pada Selasa, 23 Juni 2026, pukul 19.30-21.30 WIB di Dukuh Bekangan, Desa Sembungan, Kecamatan Nogosari, Kabupaten Boyolali. Mitra kegiatan adalah Persatuan Pengrajin Seluruh Bekangan. Sebanyak 21 orang mengikuti rangkaian kegiatan dan mengerjakan post-test secara mandiri. Peserta seluruhnya merupakan pengrajin kayu yang dalam aktivitas usaha maupun rumah tangga telah menggunakan telepon pintar, aplikasi pesan instan, media sosial, transfer bank, atau layanan pembayaran digital. Pelaksanaan pada malam hari disesuaikan dengan waktu luang pengrajin setelah menyelesaikan pekerjaan produksi.

Pendekatan dan Tahapan Pelaksanaan

Kegiatan menggunakan metode edukasi partisipatif berbasis kasus. Pendekatan partisipatif diterapkan dengan menempatkan pengalaman peserta sebagai bahan belajar, sedangkan contoh kasus digunakan untuk menjembatani istilah teknis dengan keputusan praktis. Prinsip ini sejalan dengan pembelajaran orang dewasa yang menekankan relevansi, pengalaman, pemecahan masalah, dan manfaat langsung bagi kehidupan peserta (Aly et al., 2025; Prümmer et al., 2024). Kegiatan tidak diklaim sebagai penerapan *Participatory Learning and Action* secara penuh karena belum mencakup seluruh siklus perencanaan, aksi mandiri, dan evaluasi komunitas. Unsur partisipatif terutama berada pada pemetaan pengalaman, diskusi, simulasi, dan kesepakatan tindak lanjut.

Tabel 1. Tahapan Pelaksanaan Kegiatan

Tahap	Bentuk kegiatan	Isi utama	Luaran langsung
1	Identifikasi awal secara lisan	Pertanyaan mengenai pengalaman menerima pesan mencurigakan, kebiasaan mengecek pembayaran, serta pemahaman tentang PIN dan OTP.	Peta awal pengalaman dan kebutuhan peserta
2	Pemaparan materi	Penjelasan mengenai rekayasa sosial, phishing, file APK, penyamaran identitas, data pribadi, QRIS, dan pinjaman daring ilegal.	Pemahaman mengenai bentuk risiko dan prinsip pencegahan
3	Diskusi dan pembahasan kasus	Peserta menceritakan pengalaman, menilai contoh pesan, dan mendiskusikan alasan suatu tindakan aman atau berisiko.	Pembelajaran berbasis pengalaman dan saling mengingatkan
4	Simulasi dan demonstrasi	Simulasi mengenali pesan penipuan serta demonstrasi memastikan dana melalui mutasi rekening, bukan hanya tangkapan layar.	Latihan pengambilan keputusan dan verifikasi transaksi.
5	Evaluasi pasca-kegiatan	*Post-test* sepuluh soal pilihan ganda yang dikerjakan sendiri sebelum jawaban dibahas bersama.	Profil pemahaman dasar peserta.
6	Media dan tindak lanjut	Pemasangan poster dan spanduk Kampung Sadar Keamanan Digital serta kesepakatan melanjutkan komunikasi dan penguatan program.	Penanda komitmen dan pengingat berulang di lingkungan warga.

Materi Edukasi

Materi disusun berdasarkan risiko yang dekat dengan aktivitas peserta. Topik pertama adalah perlindungan PIN, kata sandi, dan kode OTP sebagai informasi rahasia yang tidak boleh diberikan kepada pihak lain, termasuk orang yang mengaku sebagai petugas bank. Topik kedua membahas ciri phishing, tautan hadiah, pesan mendesak, nomor yang tidak dikenal, dan file APK atau dokumen palsu. Topik ketiga adalah penyamaran sebagai anggota keluarga atau teman untuk meminta transfer

uang. Topik keempat menjelaskan perbedaan antara tangkapan layar bukti transfer dan dana yang benar-benar tercatat dalam mutasi rekening. Topik kelima mencakup keamanan QRIS, perlindungan data pribadi, dan ciri umum pinjaman daring ilegal. Topik terakhir membahas langkah awal setelah mengalami atau hampir mengalami penipuan, yaitu menghentikan komunikasi, tidak mengirim data tambahan, menyimpan bukti, mengamankan akun, menghubungi penyedia layanan keuangan, dan menggunakan saluran pengaduan resmi. Materi mengenai data pribadi juga ditempatkan dalam konteks hak dan kewajiban perlindungan data sebagaimana ditegaskan dalam Undang-Undang Nomor 27 Tahun 2022.

Instrumen dan Analisis Evaluasi

Pengetahuan awal digali melalui tanya jawab lisan sebelum materi. Kegiatan tersebut tidak diperlakukan sebagai *pre-test* karena tidak menggunakan instrumen, prosedur, dan skor yang seragam. Evaluasi formal hanya dilakukan setelah penyampaian materi melalui sepuluh soal pilihan ganda. Setiap soal terdiri atas satu pilihan yang merepresentasikan tindakan aman dan dua pilihan yang tidak direkomendasikan. Dimensi yang diukur mencakup perlindungan kredensial, kewaspadaan terhadap tautan dan file, verifikasi identitas dan permintaan transfer, pengenalan tekanan psikologis, respons awal setelah insiden, serta keamanan akun pada perangkat yang digunakan bersama.

Jawaban dianalisis secara deskriptif melalui jumlah dan persentase jawaban benar pada setiap butir, distribusi skor peserta, serta persentase keseluruhan dari 210 respons yang diperoleh dari 21 peserta dan sepuluh soal. Interpretasi hasil dibatasi pada kemampuan mengenali respons dasar dalam format pilihan ganda. Kerangka evaluasi pelatihan membedakan reaksi, pembelajaran, perilaku, dan hasil akhir; data kegiatan ini terutama berada pada tingkat pembelajaran, sedangkan perubahan perilaku dan penurunan kejadian penipuan belum diukur (Alsalamah & Callinan, 2021). Data kualitatif berasal dari catatan fasilitator mengenai pertanyaan, pengalaman, dan respons peserta selama diskusi. Temuan dikelompokkan berdasarkan jenis ancaman, kebiasaan verifikasi, perlindungan kredensial, dan hambatan pelaporan. Nama peserta tidak dicantumkan. Dokumentasi foto dipilih untuk menunjukkan pelaksanaan materi, diskusi, evaluasi, dan media lingkungan. Publikasi dokumentasi tersebut dilakukan berdasarkan persetujuan mitra dan peserta.

HASIL DAN PEMBAHASAN

Keberlanjutan Program dan Kondisi Awal Peserta

Kegiatan 2026 memperluas program tahun sebelumnya dari pengenalan literasi keamanan digital menuju latihan pengambilan keputusan dan pembentukan identitas komunitas. Pada 2025, peserta memperoleh penjelasan dasar melalui FGD, penyuluhan, dan buku saku (Siagian et al., 2025). Pada kegiatan lanjutan, tim tidak lagi memulai dari asumsi bahwa peserta sama sekali tidak mengetahui penipuan digital. Pertanyaan awal diarahkan untuk melihat pengalaman yang telah mereka hadapi dan tindakan yang biasanya dipilih. Cara ini membantu fasilitator mengidentifikasi bagian yang perlu ditekankan tanpa menjadikan peserta sebagai objek yang dianggap tidak mampu.

Diskusi memperlihatkan bahwa sebagian peserta telah mengenali istilah penipuan daring, tetapi belum selalu menerjemahkannya menjadi prosedur verifikasi yang konsisten. Beberapa peserta pernah menerima file APK berkedok undangan, pesan dari nomor yang mengaku sebagai anggota keluarga, dan permintaan transfer mendadak. Dalam transaksi usaha, tangkapan layar bukti pembayaran masih dapat dipersepsikan sebagai konfirmasi yang cukup, padahal gambar dapat dimanipulasi atau berasal dari transaksi yang gagal. Terdapat pula peserta yang belum memahami bahwa OTP berfungsi sebagai kredensial autentikasi yang tidak boleh disampaikan kepada siapa pun. Temuan ini menguatkan perbedaan antara mengetahui istilah keamanan dan menerapkan perilaku aman.

Tabel 2. Temuan Kualitatif dan Implikasi Edukasi

Temuan dalam diskusi	Risiko yang muncul	Penekanan edukasi
Peserta pernah menerima file APK berkedok undangan atau dokumen.	Instalasi aplikasi berbahaya dan pengambilalihan akun.	Tidak membuka atau memasang file dari pengirim yang belum terverifikasi.
Peserta pernah diminta mentransfer uang oleh nomor yang mengaku sebagai keluarga.	Penyamaran identitas dan pemanfaatan rasa panik.	Konfirmasi melalui telepon, *video call*, atau anggota keluarga lain.
Tangkapan layar bukti pembayaran masih dipercaya sebagai konfirmasi transaksi.	Barang dikirim sebelum dana benar-benar masuk.	Memeriksa mutasi rekening atau notifikasi resmi aplikasi.
Sebagian peserta belum memahami kerahasiaan OTP.	Pengambilalihan rekening atau akun digital.	Memperlakukan OTP seperti PIN dan tidak memberikannya kepada siapa pun.
Peserta kesulitan membedakan pesan resmi dan palsu.	Keputusan hanya berdasarkan logo, nama, atau foto profil.	Memeriksa nomor, alamat, konteks, dan kanal resmi secara terpisah.
Peserta cenderung malu menceritakan pengalaman hampir tertipu.	Kejadian tidak dilaporkan dan pembelajaran tidak menyebar.	Membangun ruang berbagi tanpa menyalahkan korban dan menyimpan bukti.

Sumber: Catatan hasil diskusi kegiatan, 2026.

Rasa malu merupakan temuan penting karena keamanan digital bukan hanya persoalan kecakapan teknis. Korban penipuan sering dinilai kurang hati-hati, sehingga pengalaman yang sebenarnya bermanfaat bagi anggota lain tidak dibicarakan. Padahal, pelaku penipuan sengaja merancang pesan untuk mengeksploitasi urgensi, rasa takut, otoritas, dan hubungan personal. Dalam konteks Kampung Sadar Keamanan Digital, budaya tidak menyalahkan korban menjadi syarat agar warga mau bertanya sebelum bertindak dan segera mencari bantuan setelah terjadi insiden. Temuan Houtti et al. (2024) mengenai rendahnya pelaporan mendukung kebutuhan untuk memperjelas saluran bantuan dan mengurangi hambatan sosial dalam berbagi pengalaman.

Pelaksanaan Edukasi Berbasis Kasus

Pemaparan materi menggunakan bahasa non-teknis dan contoh yang dekat dengan penggunaan *WhatsApp,* transaksi pesanan, serta komunikasi keluarga. Fasilitator menjelaskan bahwa ciri penipuan tidak selalu dapat dikenali hanya dari tampilan pesan. Logo bank, foto profil, nama anggota keluarga, atau penggunaan bahasa yang sopan dapat ditiru. Karena itu, peserta diarahkan untuk memeriksa tindakan yang diminta oleh pesan: apakah meminta data rahasia, mendesak untuk segera mengirim uang, mengarahkan pemasangan aplikasi, atau melarang penerima menghubungi pihak lain. Pola tersebut membantu peserta beralih dari penilaian berdasarkan tampilan menuju penilaian berdasarkan konteks dan konsekuensi tindakan.

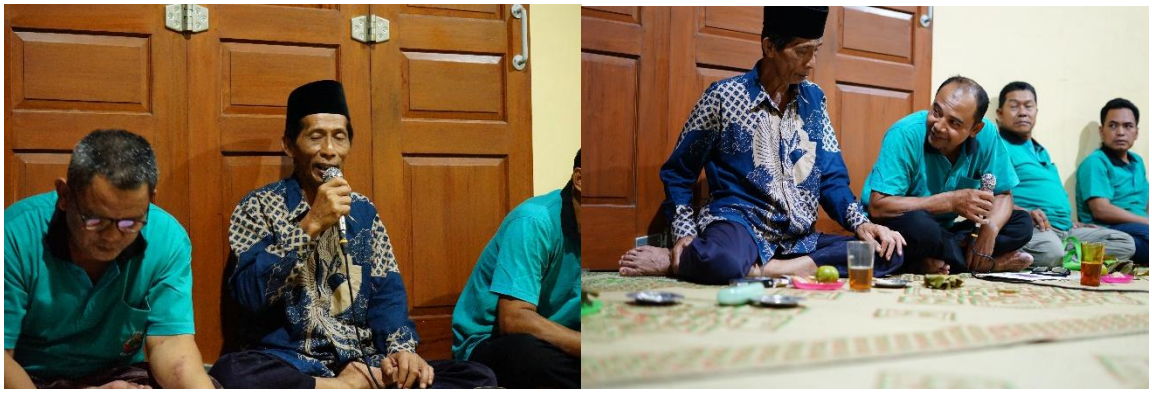
Simulasi dilakukan dengan menampilkan contoh pesan yang berisi hadiah, permintaan transfer, serta file yang diklaim sebagai undangan atau dokumen transaksi. Peserta diminta menentukan bagian yang mencurigakan dan menyebutkan langkah yang perlu dilakukan. Jawaban kemudian dibahas bersama agar peserta memahami alasan di balik respons aman. Metode ini relevan

dengan kajian pelatihan anti-phishing yang menekankan pentingnya latihan, contoh realistis, dan umpan balik (Prümmer et al., 2024). Pengetahuan mengenai tanda ancaman juga perlu dikaitkan dengan tindakan yang spesifik, karena kesadaran dan pengetahuan tidak selalu otomatis menghasilkan perilaku aman (Zwilling et al., 2022).

Gambar 1. Penyampaian materi mengenai modus penipuan daring dan perlindungan kredensial kepada anggota kelompok pengrajin.

Demonstrasi verifikasi transaksi menekankan perbedaan antara bukti visual dan pencatatan dana pada sistem. Peserta diperlihatkan bahwa tangkapan layar dapat diedit, digunakan ulang, atau menunjukkan status yang belum berhasil. Prosedur yang direkomendasikan adalah membuka aplikasi perbankan atau layanan pembayaran melalui perangkat sendiri, memeriksa mutasi atau saldo, mencocokkan nominal dan nama transaksi, lalu mengirim barang setelah dana benar-benar tercatat. Pada QRIS, peserta juga diingatkan untuk memeriksa notifikasi *merchant* dan tidak mengikuti instruksi pembeli yang meminta pengembalian dana melalui kanal yang tidak jelas. Pesan ini diringkas menjadi prinsip: "barang dikirim setelah dana terlihat di akun sendiri, bukan setelah menerima gambar dari pembeli."

Diskusi berlangsung dua arah dan peserta menghubungkan materi dengan pengalaman masing-masing. Pengalaman lokal berfungsi sebagai sumber contoh yang lebih meyakinkan daripada skenario yang sepenuhnya dibuat oleh fasilitator. Pembelajaran orang dewasa cenderung efektif ketika materi memiliki kegunaan langsung, menghargai pengalaman, dan memecahkan masalah yang dirasakan peserta (Aly et al., 2025; Prümmer et al., 2024). Kegiatan juga menghindari bahasa yang menimbulkan ketakutan berlebihan. Tujuannya bukan membuat peserta menolak seluruh layanan digital, melainkan membangun rasa percaya diri untuk menggunakan layanan secara hati-hati. Program kesadaran yang hanya menonjolkan ancaman dapat mendorong penghindaran, sedangkan pengrajin tetap membutuhkan teknologi untuk mempertahankan kegiatan usaha.



Gambar 2. Diskusi berbasis pengalaman dan demonstrasi langkah verifikasi transaksi digital.

Hasil Post-test dan Interpretasinya

Sebanyak 21 peserta mengerjakan post-test secara mandiri sebelum fasilitator membahas jawaban. Hasil evaluasi menunjukkan 201 jawaban benar dari 210 respons atau 95,7%, dengan nilai rata-rata 9,57 dari 10 soal. Sebanyak 12 peserta (57,1%) menjawab seluruh soal dengan benar, sedangkan 9 peserta (42,9%) menjawab 9 dari 10 soal dengan benar. Rekap per butir menunjukkan bahwa enam soal dijawab benar oleh seluruh responden. Persentase terendah terdapat pada butir mengenai file atau aplikasi dari nomor tidak dikenal dan pengenalan pesan yang memaksa atau menakut-nakuti, masing-masing sebesar 85,7%, sedangkan verifikasi permintaan transfer yang mengatasnamakan saudara mencapai 90,5% dan pemeriksaan tautan hadiah mencapai 95,2%. Hasil ini menunjukkan bahwa peserta yang mengikuti evaluasi pada umumnya mampu mengenali tindakan dasar yang direkomendasikan dalam skenario penipuan digital yang diberikan.

Tabel 3. Rekap Hasil Post-test per Butir Soal

No.	Indikator soal	Jawaban benar (n)	Persentase
1	Menolak memberikan PIN atau kata sandi kepada pihak yang mengaku dari bank.	21	100%
2	Memperlakukan OTP sebagai kode rahasia.	21	100%
3	Tidak langsung membuka tautan hadiah dan memeriksa kebenarannya.	20	95,2%
4	Tidak membuka file atau aplikasi dari nomor yang tidak dikenal.	18	85,7%
5	Tidak membagikan PIN, kata sandi, dan OTP.	21	100%
6	Memverifikasi permintaan transfer yang mengatasnamakan saudara.	19	90,5%
7	Mengenali pesan yang memaksa, mendesak, atau menakut-nakuti.	18	85,7%
8	Berhenti membalas, menyimpan bukti, dan meminta bantuan.	21	100%
9	Mengamankan akun setelah menggunakan perangkat bersama.	21	100%
10	Mengonfirmasi permintaan uang melalui kanal lain.	21	100%
	Total	**201 dari 210**	**95,7%**

Sumber: Rekap tim pengabdian, 2026.

Hasil tersebut harus ditafsirkan secara proporsional yakni dengan pertama, *post-test* hanya dilakukan setelah kegiatan sehingga tidak tersedia dasar kuantitatif untuk menyatakan peningkatan. Tanya jawab awal memberi gambaran kebutuhan, tetapi tidak dapat dibandingkan dengan *post-test* sebagai skor. Kedua, pilihan jawaban pada beberapa soal memiliki perbedaan yang cukup jelas antara respons aman dan tidak aman. Skor tinggi dapat menunjukkan bahwa peserta mampu mengenali jawaban yang diharapkan, tetapi belum membuktikan bahwa mereka akan melakukan tindakan yang sama ketika menghadapi pesan yang lebih meyakinkan atau berada dalam tekanan. Ketiga, instrumen belum menguji keterampilan yang lebih kompleks, seperti memeriksa alamat situs, izin aplikasi, legalitas penyedia pinjaman, atau prosedur pemulihan akun.

Pembedaan tersebut penting karena pengetahuan, sikap, dan perilaku merupakan dimensi yang saling terkait tetapi tidak identik. *Human Aspects of Information Security Questionnaire* dikembangkan untuk mengukur beberapa dimensi perilaku keamanan, termasuk pengelolaan kata sandi, penggunaan perangkat, dan penanganan informasi (Xu et al., 2024). Studi komparatif Zwilling et al. (2022) juga menunjukkan adanya kesenjangan antara kesadaran, pengetahuan, dan perilaku. Oleh

karena itu, capaian 95,7% disebut sebagai profil pemahaman dasar pascakegiatan, bukan sebagai efektivitas program sebesar 95,7%, peningkatan pengetahuan sebesar 95,7%, atau bukti perubahan perilaku.

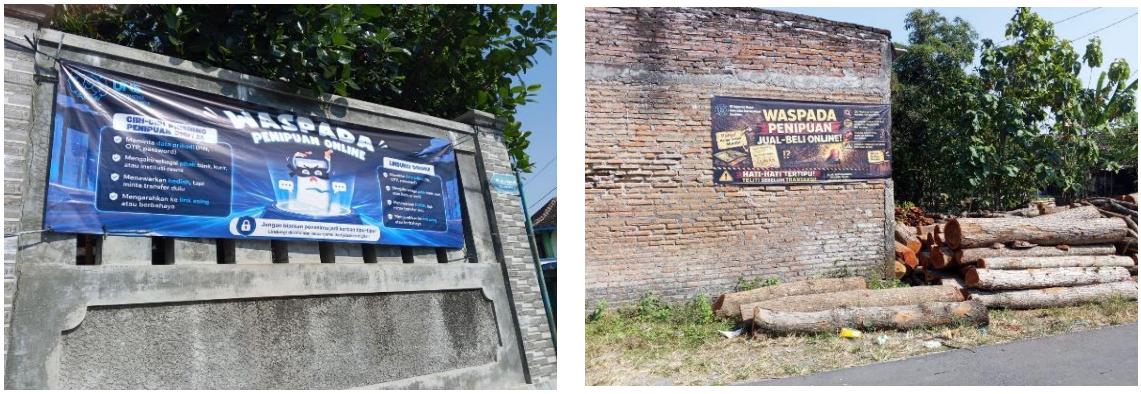
Gambar 3. Pelaksanaan *post-test* dan pembahasan jawaban sebagai bagian dari evaluasi pembelajaran.

Deklarasi Menuju Kampung Sadar Keamanan Digital

Setelah sesi edukasi, kelompok menyepakati penggunaan nama Kampung Sadar Keamanan Digital sebagai identitas program. Kesepakatan tersebut diperkuat melalui pemasangan poster dan spanduk pada salah satu rumah warga. Media ini memiliki dua fungsi. Pertama, sebagai penanda komitmen kelompok bahwa keamanan digital merupakan kepentingan bersama, bukan hanya urusan korban atau pengguna tertentu. Kedua, sebagai media komunikasi risiko yang dapat dilihat berulang kali oleh peserta dan warga lain. Berbeda dari materi presentasi yang hanya terlihat selama pertemuan, media lingkungan mempertahankan visibilitas pesan setelah kegiatan selesai.

Pemasangan spanduk tidak diperlakukan sebagai bukti bahwa kampung telah sepenuhnya aman atau seluruh warga telah berubah perilakunya. Fungsinya lebih dekat dengan kampanye kesadaran dan pembentukan norma. Pesan visual dapat mengingatkan warga untuk tidak membagikan OTP, tidak membuka file asing, memeriksa transaksi, dan bertanya ketika ragu. Dalam program kesadaran keamanan, media seperti poster berperan pada tingkat pengenalan dan pengulangan pesan, sedangkan pelatihan dan praktik diperlukan untuk membangun keterampilan. Karena ancaman berubah, media juga perlu diperbarui agar tidak berhenti sebagai simbol yang kehilangan relevansi.

Identitas Kampung Sadar Keamanan Digital berpotensi memperluas cakupan program dari peserta yang hadir menuju lingkungan sosial mereka. Pengrajin tidak hanya berinteraksi dengan pelanggan, tetapi juga dengan anggota keluarga yang menggunakan perangkat, rekening, dan aplikasi yang sama. Ketika peserta membagikan aturan sederhana kepada keluarga dan tetangga, manfaat program dapat menyebar melalui pembelajaran sebaya. Namun, penyebaran tersebut belum diukur dalam kegiatan ini. Oleh sebab itu, istilah "menuju" dipertahankan untuk menandai bahwa program masih berada pada tahap penjajakan, pengenalan identitas, dan pembentukan komitmen.



Gambar 4. Pemasangan media Kampung Sadar Keamanan Digital.

Implikasi, Tindak Lanjut, dan Keterbatasan

Implikasi praktis kegiatan adalah perlunya mengubah edukasi satu kali menjadi mekanisme sederhana yang dapat digunakan ketika risiko muncul. Pengurus kelompok dapat menetapkan dua atau tiga kontak rujukan, menyusun kartu prosedur "berhenti-periksa-konfirmasi-lapor", dan memperbarui contoh modus secara berkala. Kader tidak perlu diberi label sebagai ahli keamanan siber. Perannya dapat dimulai sebagai penghubung yang membantu anggota menyimpan bukti, mencari sumber resmi, dan menghubungi bank, penyedia layanan, atau kanal pengaduan. Pendekatan bertahap lebih realistis bagi usaha kecil yang memiliki kapasitas dan kebutuhan berbeda (Chaudhary et al., 2023; Chidukwani et al., 2024; Shojaifar & Järvinen, 2021).

Program memiliki beberapa keterbatasan. Pertama, jumlah peserta terbatas pada 21 anggota kelompok sehingga hasil evaluasi tidak dapat digeneralisasi kepada komunitas pengrajin lain. Kedua, instrumen hanya terdiri atas sepuluh soal dengan skenario dasar dan belum melalui uji validitas formal. Ketiga, kegiatan berlangsung selama dua jam dan belum mengukur retensi pengetahuan. Keempat, artikel belum memiliki data observasi perilaku dalam transaksi nyata atau catatan kasus yang berhasil dicegah setelah kegiatan. Terakhir, deklarasi dan media lingkungan belum disertai struktur kader, pembagian peran, dan mekanisme konsultasi yang terdokumentasi.

Keterbatasan tersebut memberikan agenda pengembangan, dimana evaluasi berikutnya dapat menggunakan *pre-test* dan *post-test* dengan skenario setara, simulasi pesan yang lebih ambigu, serta tindak lanjut satu sampai tiga bulan untuk menilai retensi dan perilaku. Peserta dapat diminta mendemonstrasikan verifikasi transaksi, menunjukkan cara memeriksa legalitas layanan, atau menjelaskan langkah setelah akun terindikasi diambil alih. Dokumentasi konsultasi dapat dilakukan tanpa menyimpan data pribadi korban. Pada tingkat program, pengurus kelompok dapat menetapkan dua atau tiga kontak rujukan, jadwal pembaruan informasi, dan aturan bahwa setiap anggota boleh bertanya tanpa takut dipermalukan.

Kontribusi kegiatan ini terletak pada pergeseran dari literasi penggunaan teknologi menuju kesadaran keamanan yang berbasis keputusan dan dukungan komunitas. Program tidak hanya menjelaskan jenis ancaman, tetapi juga mempraktikkan aturan yang dapat digunakan peserta seperti berhenti sejenak, periksa informasi, konfirmasi melalui kanal lain, dan minta bantuan. Deklarasi serta media lingkungan memberikan identitas bersama, sedangkan pengakuan atas keterbatasan mencegah artikel mengklaim perubahan yang belum terukur. Dengan demikian, Kampung Sadar Keamanan Digital dipahami sebagai proses sosial yang perlu dipelihara melalui pengulangan, praktik, pembaruan informasi, dan kelembagaan bertahap.

KESIMPULAN

Edukasi partisipatif berbasis kasus membantu anggota Persatuan Pengrajin Seluruh Bekangan menghubungkan risiko penipuan digital dengan keputusan dalam aktivitas usaha dan kehidupan

sehari-hari. Kegiatan menunjukkan bahwa persoalan keamanan tidak hanya berkaitan dengan pengetahuan mengenai jenis penipuan, tetapi juga kebiasaan verifikasi yang belum konsisten, kepercayaan terhadap bukti visual, respons terhadap pesan yang mendesak, dan keraguan untuk meminta bantuan. Simulasi pesan serta demonstrasi pemeriksaan transaksi membuat materi lebih konkret melalui tindakan utama, yaitu melindungi kredensial, memeriksa dana pada akun sendiri, mengonfirmasi permintaan melalui kanal berbeda, menyimpan bukti, dan mencari bantuan ketika ragu. Secara praktis, kegiatan menjadi tahap awal pembentukan perlindungan berbasis komunitas melalui pesan yang disepakati, media pengingat, dan norma untuk tidak menyalahkan korban. Evaluasi hanya menggambarkan kemampuan peserta mengenali jawaban aman segera setelah kegiatan dan belum membuktikan peningkatan pengetahuan maupun perubahan perilaku. Keterbatasan utama meliputi instrumen yang sederhana dan belum tervalidasi, jumlah peserta yang terbatas, serta belum adanya pemantauan pascakegiatan. Program lanjutan perlu menggunakan evaluasi sebelum dan sesudah kegiatan, simulasi yang lebih kontekstual, pemantauan retensi dan perilaku, prosedur verifikasi yang ringkas, serta kontak rujukan komunitas yang terhubung dengan kanal pelaporan resmi.

UCAPAN TERIMA KASIH

Tim pengabdian menyampaikan terima kasih kepada Universitas Sebelas Maret atas dukungan melalui skema pendanaan Pengabdian kepada Masyarakat Hibah Grup Riset tahun 2026 dengan Nomor Perjanjian Penugasan Pengabdian: 463/UN27.22/PT.01.03/2026, kepada pengurus dan seluruh anggota Persatuan Pengrajin Seluruh Bekangan atas partisipasi dan keterbukaan dalam berbagi pengalaman, serta kepada perangkat dan warga Dukuh Bekangan yang mendukung pelaksanaan kegiatan.

DAFTAR PUSTAKA

Afzal, M., Meraj, M., Kaur, M., & Ansari, M. S. (2025). How does cybersecurity awareness help in achieving digital financial inclusion in rural India under escalating cyber fraud scenario? *Journal of Cyber Security Technology, 9*(2), 88–126. https://doi.org/10.1080/23742917.2024.2347674

Alharbi, F., Alsulami, M., Al-Solami, A., Al-Otaibi, Y., Al-Osimi, M., Al-Qanor, F., & Al-Otaibi, K. (2021). The impact of cybersecurity practices on cyberattack damage: The perspective of small enterprises in Saudi Arabia. *Sensors, 21*(20), 6901. https://doi.org/10.3390/s21206901

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science, 3*, Article 563060. https://doi.org/10.3389/fcomp.2021.563060

Alsalamah, A., & Callinan, C. (2021). The Kirkpatrick model for training evaluation: Bibliometric analysis after 60 years (1959–2020). *Industrial and Commercial Training, 54*(1), 36–63. https://doi.org/10.1108/ICT-12-2020-0115

Aly, H., Liu, Y., Khan, S., Ghaiumy Anaraky, R., Byrne, K., & Knijnenburg, B. P. (2025). Digital privacy education: Customized interventions for U.S. older and younger adults in rural and urban settings. *Technology in Society, 81*, Article 102805. https://doi.org/10.1016/j.techsoc.2024.102805

Armenia, S., Angelini, M., Nonino, F., Palombi, G., & Schlitzer, M. F. (2021). A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. *Decision Support Systems, 147*, Article 113580. https://doi.org/10.1016/j.dss.2021.113580

Bai, C., Quayson, M., & Sarkis, J. (2021). COVID-19 pandemic digitization lessons for sustainable development of micro- and small-enterprises. *Sustainable Production and Consumption, 27*, 1989–2001. https://doi.org/10.1016/j.spc.2021.04.035

Baki, S., & Verma, R. M. (2023). Sixteen years of phishing user studies: What have we learned? *IEEE Transactions on Dependable and Secure Computing, 20*(2), 1200–1212. https://doi.org/10.1109/TDSC.2022.3151103

Burton, A., Cooper, C., Dar, A., Mathews, L., & Tripathi, K. (2022). Exploring how, why and in what contexts older adults are at risk of financial cybercrime victimisation: A realist review. *Experimental Gerontology, 159*, Article 111678. https://doi.org/10.1016/j.exger.2021.111678

Chaudhary, S., Gkioulos, V., & Katsikas, S. (2023). A quest for research and knowledge gaps in cybersecurity awareness for small and medium-sized enterprises. *Computer Science Review, 50*, Article 100592. https://doi.org/10.1016/j.cosrev.2023.100592

Chidukwani, A., Zander, S., & Koutsakis, P. (2024). Cybersecurity preparedness of small-to-medium businesses: A Western Australia study with broader implications. *Computers & Security, 145*, Article 104026. https://doi.org/10.1016/j.cose.2024.104026

Havers, B., Tripathi, K., Burton, A., Martin, W., & Cooper, C. (2024). Exploring the factors preventing older adults from reporting cybercrime and seeking help: A qualitative, semistructured interview study. *Health & Social Care in the Community, 2024*, Article 1314265. https://doi.org/10.1155/2024/1314265

Houtti, M., Roy, A., Gangula, V. N. R., & Walker, A. (2024). A survey of scam exposure, victimization, types, vectors, and reporting in 12 countries. *Journal of Online Trust and Safety, 2*(4). https://doi.org/10.54501/jots.v2i4.204

Kemp, S., & Erades Pérez, N. (2023). Consumer fraud against older adults in digital society: Examining victimization and its impact. *International Journal of Environmental Research and Public Health, 20*(7), 5404. https://doi.org/10.3390/ijerph20075404

Kilay, A. L., Simamora, B. H., & Putra, D. P. (2022). The influence of e-payment and e-commerce services on supply chain performance: Implications of open innovation and solutions for the digitalization of micro, small, and medium enterprises (MSMEs) in Indonesia. *Journal of Open Innovation: Technology, Market, and Complexity, 8*(3), 119. https://doi.org/10.3390/joitmc8030119

Lopes, A., Mamede, H. S., Reis, L., & Santos, A. (2024). Common techniques, success attack factors and obstacles to social engineering: A systematic literature review. *Emerging Science Journal, 8*(2), 761–794. https://doi.org/10.28991/ESJ-2024-08-02-025

Parti, K., & Tahir, F. (2023). 'If we don't listen to them, we make them lose more than money': Exploring reasons for underreporting and the needs of older scam victims. *Social Sciences, 12*(5), 264. https://doi.org/10.3390/socsci12050264

Pehlivanoglu, D., Shoenfelt, A., Hakim, Z., Heemskerk, A., Zhen, J., Mosqueda, M., Wilson, R. C., Huentelman, M., Grilli, M. D., Turner, G., Spreng, R. N., & Ebner, N. C. (2024). Phishing vulnerability compounded by older age, apolipoprotein E e4 genotype, and lower cognition. *PNAS Nexus, 3*(8), Article pgae296. https://doi.org/10.1093/pnasnexus/pgae296

Pituk, P., Chutipattana, N., Laor, P., Sukdee, T., Kittikun, J., Jitwiratnukool, W., Fajriyah, R., & Saisanan Na Ayudhaya, W. (2025). Digital media victimization among older adults in upper-southern Thailand. *Informatics, 12*(1), 24. https://doi.org/10.3390/informatics12010024

Prümmer, J., van Steen, T., & van den Berg, B. (2024). A systematic review of current cybersecurity training methods. *Computers & Security, 136*, Article 103585. https://doi.org/10.1016/j.cose.2023.103585

Republik Indonesia. (2022). *Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi*.

Shang, Y., Wu, Z., Du, X., Jiang, Y., Ma, B., & Chi, M. (2022). The psychology of the internet fraud victimization of older adults: A systematic review. *Frontiers in Psychology, 13*, Article 912242. https://doi.org/10.3389/fpsyg.2022.912242

Shojaifar, A., & Järvinen, H. (2021). Classifying SMEs for approaching cybersecurity competence and awareness. In *Proceedings of the 16th International Conference on Availability, Reliability and Security* (pp. 1–7). Association for Computing Machinery. https://doi.org/10.1145/3465481.3469200

Siagian, M., Satyawan, I. A., Djarwono, L. F., Munestri, S. L., Sandria, A., Wibisono, B. I., Ikawati, E., &

Hidayat, M. C. (2025). Peningkatan literasi keamanan digital untuk mencegah penipuan online pada pengrajin kayu di Boyolali. *Community Transformation Review, 1*(1), 34–45. https://journal.uii.ac.id/CTR/article/view/43432

Sur, A., DeLiema, M., Vock, D. M., Boyle, P., & Yu, L. (2023). A microsimulation of well-being and literacy interventions to reduce scam susceptibility in older adults. *Journal of Applied Gerontology, 42*(12), 2360–2370. https://doi.org/10.1177/07334648231196850

Syafitri, W., Shukur, Z., Mokhtar, U. A., Sulaiman, R., & Ibrahim, M. A. (2022). Social engineering attacks prevention: A systematic literature review. *IEEE Access, 10*, 39325–39343. https://doi.org/10.1109/ACCESS.2022.3162594

Vuorikari, R., Kluzer, S., & Punie, Y. (2022). *DigComp 2.2: The digital competence framework for citizens—With new examples of knowledge, skills and attitudes*. Publications Office of the European Union. https://doi.org/10.2760/115376

Xu, X. S., Hong, W. C. H., Kolletar-Zhu, K., Zhang, Y. F., & Chi, C. Y. (2024). Validation and application of the Human Aspects of Information Security Questionnaire for undergraduates: Effects of gender, discipline and grade level. *Behaviour & Information Technology, 43*(12), 2799–2820. https://doi.org/10.1080/0144929X.2023.2260876

Yu, S.-J., Kuo, C.-T., & Tseng, Y.-C. (2023). Association of financial literacy and risk preference with fraud exposure and victimization among middle-aged and older adults in China. *Journal of Applied Gerontology, 42*(1), 89–98. https://doi.org/10.1177/07334648221121775

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Çetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems, 62*(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269