JURNAL ALTIFANI
Penelitian dan Pengabdian kepada Masyarakat

Vol. 5, No. 3 - Mei 2025, Hal. 196-204
DOI: 10.59395/altifani.v5i3.691

Peningkatan Literasi Digital dan Keamanan Siber untuk Penguatan Personal Finance pada Kelompok Anggota Koperasi di Malang

Apriana Rahmawati[*1], Rizky Prasetya[2], Alif Faruqi Febri Yanto[1], Nabilla Carissa Ratnadewati [1]

[1]Program Studi Akuntansi, Fakultas Ekonomi dan Bisnis, Universitas Negeri Malang

[2]Program Studi Akuntansi, Jurusan Akuntansi, Politeknik Negeri Malang

*e-mail: aprianarhmwt.feb@um.ac.id

Received:	Revised:	Accepted:	Available online:
21.03.2025	19.04.2025	14.05.2025	30.05.2025

Abstract: *Digital technology has now become an inseparable part of daily life, including in the management of personal finances. Therefore, digital literacy and cybersecurity are crucial aspects to protect users' data and assets from the growing prevalence of fraud, particularly through QRIS applications and mobile banking services. This community service initiative aims to enhance the understanding and skills of the members of the SBW Cooperative Women's Group in Malang in digital literacy and cybersecurity practices, enabling them to manage personal finances more securely and effectively. The methods used include the delivery of comprehensive material on potential cyber threats and data protection practices, demonstrations of mobile device security measures, and simulations of safe QRIS and mobile banking transactions. Evaluation results through questionnaires show an increase in cybersecurity awareness, as indicated by the participants' ability to recognize phishing threats, apply two-factor authentication, and take steps to mitigate cyberattacks. With improved digital literacy and cybersecurity preparedness, SBW Cooperative members are expected to prevent financial losses, strengthen economic independence, and adopt more accountable and sustainable digital financial management practices.*

Keywords: *digital literacy, ,cybersecurity, community service, cooperative members*

Abstrak: Teknologi digital kini menjadi bagian tak terpisahkan dalam kehidupan sehari-hari, termasuk dalam pengelolaan keuangan personal. Oleh karena itu, literasi digital dan keamanan siber menjadi aspek krusial untuk melindungi data serta aset pengguna dari maraknya penipuan, khususnya melalui aplikasi QRIS dan layanan mobile banking. Pengabdian ini bertujuan meningkatkan pemahaman dan keterampilan anggota Kelompok Wanita Koperasi SBW Malang dalam literasi digital dan praktik keamanan siber, sehingga dapat mengelola keuangan pribadi dengan lebih aman dan efektif. Metode yang digunakan meliputi penyampaian materi komprehensif tentang potensi ancaman siber dan praktik perlindungan data, demonstrasi pengamanan perangkat seluler, serta simulasi transaksi QRIS dan *mobile banking* yang aman. Hasil evaluasi melalui kuesioner menunjukkan peningkatan kesadaran keamanan siber, ditandai oleh kemampuan mengenali ancaman phishing, menerapkan autentikasi ganda, dan langkah mitigasi serangan siber. Dengan meningkatnya literasi digital dan kesiapsiagaan siber ini, anggota Koperasi SBW diharapkan mampu mencegah kerugian finansial, memperkuat kemandirian ekonomi, serta menerapkan pengelolaan keuangan digital yang lebih akuntabel dan berkelanjutan.

Kata kunci: literasi digital, keamanan siber, personal finance, pengabdian masyarakat, anggota koperasi

1. PENDAHULUAN

Perkembangan teknologi digital telah menjadi kekuatan pendorong utama dalam transformasi cara masyarakat Indonesia melakukan transaksi dan mengelola keuangan pribadi, di mana penggunaan aplikasi mobile banking dan QRIS muncul sebagai kanal dominan dalam kegiatan finansial sehari-hari (BI, 2025). Meskipun kenyamanan dan kecepatan transaksi meningkat pesat, data Indeks Masyarakat Digital Indonesia (IMDI) 2024 menunjukkan skor nasional sebesar 43,34, hanya naik tipis 0,16 poin dari tahun sebelumnya, sementara pilar "keamanan digital" masih tertinggal di angka 3,29, menandakan kebutuhan mendesak memperkuat literasi keamanan di kalangan pengguna akhir (Kominfo, 2024a). Ketergantungan pada perangkat seluler tanpa pengamanan yang memadai telah membuka celah bagi pelaku kejahatan siber untuk memanfaatkan kerentanan tersebut (Kominfo, 2024b). Di samping itu, kecepatan adopsi teknologi digital belum diimbangi oleh peningkatan kompetensi pengguna dalam mengenali dan menanggulangi potensi ancaman. Kondisi ini memunculkan paradoks: sementara akses ke layanan keuangan inklusif makin meluas, risiko fraud dan pencurian data pun ikut meningkat. Keadaan serupa tercermin di survei Kominfo, yang mencatat

Vol. 5, No. 3 - Mei 2025, Hal. 196-204
DOI: 10.59395/altifani.v5i3.691

rata-rata 2.600 serangan siber per hari sepanjang 2024 di Indonesia, menjadikannya salah satu negara target serangan siber terbanyak di Asia Tenggara (Kominfo, 2024b). Oleh karena itu, kesenjangan antara adopsi digital dan kesiapan keamanan menjadi isu sentral yang harus diatasi melalui intervensi literasi digital terpadu.

Nilai transaksi QRIS yang melonjak signifikan juga memperbesar permukaan risiko siber; menurut Bank Indonesia, pada Januari 2025 transaksi QRIS mencapai Rp 80,88 triliun dengan volume 790,79 juta transaksi dan didukung oleh 36,57 juta merchant, menandai pertumbuhan tahunan sebesar 170,1 % (BI, 2025). Pencapaian ini menunjukkan seberapa dalam kanal digital telah terbenam dalam kehidupan ekonomi masyarakat, namun sekaligus mengindikasikan betapa krusialnya penguatan protokol keamanan di level pengguna. Inovasi teranyar seperti uji coba QRIS Tap berbasis NFC semakin memudahkan transaksi tanpa memindai kode, tetapi juga menuntut standar keamanan perangkat yang lebih tinggi agar data tidak disadap atau dipalsukan (BI, 2025). Saat ini, autentikasi dua faktor masih belum diaplikasikan secara konsisten oleh pengguna akhir, sehingga kerentanan terhadap phishing dan malware tetap tinggi. Data SNLIK 2024 oleh Otoritas Jasa Keuangan dan Badan Pusat Statistik menyebutkan indeks literasi keuangan nasional sebesar 65,43 % dan inklusi keuangan 75,02 %, namun dimensi keamanan siber dalam transaksi digital belum terukur secara eksplisit dalam survei tersebut (OJK & BPS, 2024). Akibatnya, meski masyarakat memahami mekanisme produk keuangan digital, mereka belum terlatih mengenali modus penipuan canggih seperti deepfake voice fraud atau QR code spoofing, sehingga intervensi literasi digital yang holistik menjadi sangat diperlukan (Sethi & Khurana, 2022).

Kelompok Wanita Koperasi SBW Malang merupakan segmen pengguna yang strategis untuk dijangkau, karena anggotanya sebagian besar ibu rumah tangga dan pelaku UMKM kecil yang mengandalkan teknologi digital untuk pengelolaan usaha dan pemasaran produk lokal. Profesi dan latar belakang pendidikan anggota yang beragam menimbulkan perbedaan signifikan dalam tingkat literasi digital, di mana sebagian masih bergantung pada pencatatan manual dan enggan memanfaatkan aplikasi keuangan berbasis internet karena kekhawatiran akan keamanan data pribadi. Hasil wawancara pendahuluan menunjukkan bahwa kekhawatiran terhadap potensi pencurian informasi dan penipuan online menjadi alasan utama anggota menolak beralih ke transaksi digital. Kondisi geografis Malang yang mencakup daerah urban dan rural juga menghadirkan tantangan akses pelatihan, di mana koneksi internet belum merata dan fasilitas pendukung masih terbatas. Kesenjangan inilah yang mendasari kebutuhan intervensi literasi digital dan keamanan siber yang terarah dan kontekstual, sehingga anggota koperasi dapat menggunakan aplikasi finansial dengan penuh keyakinan (Rahmawati & Restuningdiah, 2024).

Berdasarkan identifikasi kebutuhan tersebut, kegiatan pengabdian ini dirancang untuk meningkatkan literasi digital dan kesadaran keamanan siber bagi anggota Kelompok Wanita Koperasi SBW Malang, dengan fokus utama pada kemampuan mengenali jenis-jenis penipuan online serta mitigasinya. Tujuan spesifik pertama adalah membekali peserta dengan pengetahuan mendalam mengenai modus phishing, malware, dan deepfake fraud yang kerap menargetkan pengguna layanan mobile banking dan QRIS. Tujuan kedua adalah melatih peserta mengenali aplikasi berbahaya yang berpotensi mengandung malware, termasuk cara memeriksa reputasi aplikasi di toko resmi, membaca izin akses, serta mengevaluasi ulasan pengguna. Tujuan ketiga adalah membangun keterampilan teknis dasar seperti pengaturan autentikasi ganda, pembaruan sistem operasi secara rutin, dan penggunaan fitur sandi biometrik atau token keamanan. Selain itu, program ini juga bertujuan untuk mengumpulkan dan mendokumentasikan pengalaman nyata anggota mengenai kejadian penipuan online, sehingga materi pelatihan dapat diadaptasi secara dinamis berdasarkan kasus yang paling relevan.

Metode pelaksanaan kegiatan berpusat pada penyampaian materi melalui slide presentasi yang menarik dan interaktif, di mana setiap sesi dibuka dengan paparan teori singkat mengenai ancaman siber, diikuti dengan diskusi kelompok untuk berbagi pengalaman anggota terkait peristiwa penipuan online yang mereka hadapi. Peserta didorong memberikan feedback langsung terhadap materi yang disampaikan, membahas detail kejadian, taktik pelaku kejahatan siber, serta konsekuensi

Vol. 5, No. 3 - Mei 2025, Hal. 196-204
DOI: 10.59395/altifani.v5i3.691

finansial maupun psikologis yang dialami. Sesi berbagi pengalaman memungkinkan anggota saling belajar dari kasus nyata, meningkatkan kewaspadaan, dan menciptakan kesadaran kolektif akan pentingnya proteksi data. Selanjutnya, sesi praktis mengenali aplikasi berbahaya, termasuk cara memverifikasi keaslian aplikasi di platform resmi, mengecek izin akses yang mencurigakan, serta langkah-langkah uninstall dan pelaporan aplikasi yang terindikasi malware (Kolb, 1984). Tiap sesi diakhiri dengan diskusi mitigasi yang mencakup rekomendasi penggunaan alat pendukung seperti antivirus mobile, VPN, dan fitur keamanan bawaan sistem operasi.

Kebaruan (*novelty*) dari program ini terletak pada pendekatan kolaboratif yang mengedepankan refleksi pengalaman nyata peserta serta pemanfaatan feedback sebagai komponen utama dalam penyusunan materi. Kegiatan ini menempatkan peserta sebagai sumber kasus studi, sehingga materi yang dibahas selalu kontekstual dan relevan dengan tantangan lokal yang dihadapi. Integrasi metode slide presentasi dengan sesi diskusi pengalaman juga membantu membangun *self-efficacy* digital, di mana peserta tidak hanya memahami konsep, tetapi juga merasa mampu menerapkan langkah-langkah mitigasi secara mandiri. Landasan teori program ini mengacu pada kerangka security awareness serta teori *self-efficacy*, yang menegaskan bahwa pengalaman langsung dan umpan balik positif meningkatkan keyakinan individu dalam melaksanakan tindakan yang diinginkan (Bandura, 1977; Whitman & Mattord, 2012).

Dalam jangka pendek, program ini diharapkan mampu meningkatkan literasi digital dan kesadaran keamanan siber anggota sehingga mereka lebih mahir mengenali ancaman dan menerapkan langkah preventif dalam transaksi digital. Untuk jangka panjang, direncanakan ada kelanjutan kegiatan berupa pelatihan lanjutan dan pendampingan reguler agar seluruh anggota koperasi, termasuk yang belum ikut sesi awal, memperoleh akses materi keamanan siber ini, menciptakan ekosistem pembelajaran berkelanjutan dan memperkuat ketahanan ekonomi digital komunitas secara menyeluruh.

2. METODE

Metode pengabdian ini menerapkan *experiential learning* untuk membangun kemampuan peserta dalam menghadapi penipuan online melalui tahapan berurut: pertama, tahap persiapan dimulai dengan identifikasi kebutuhan peserta menggunakan kuesioner dan wawancara untuk memetakan tingkat literasi digital serta pengalaman sebelumnya terhadap penipuan online (Creswell, 2012). Selanjutnya, program diorganisir mengikuti empat siklus *experiential learning*: peserta memulai dengan berbagi pengalaman nyata (*concrete experience*) kasus phishing dan malware yang pernah mereka alami (McLeod, 2013); kemudian melakukan refleksi bersama (*reflective observation*) melalui diskusi kelompok kecil untuk mengidentifikasi pola dan kelemahan dalam praktik digital sehari-hari (Kolb, 1984); tahap berikutnya adalah konseptualisasi abstrak (*abstract conceptualization*) saat materi disampaikan melalui presentasi slide interaktif yang menguraikan modus serangan siber—phishing, malware, deepfake fraud—disertai contoh kasus nyata dari anggota koperasi (Kolb, 1984); pada fase eksperimen aktif (*active experimentation*), instruktur memfasilitasi diskusi berbagi strategi dan best practices dalam mengenali serta mencatat aplikasi berbahaya yang mengandung malware, termasuk cara memeriksa reputasi aplikasi dan izin aksesnya (Kolb, 1984). Setelah itu, dilanjutkan dengan paparan langkah mitigasi teknis—pembaruan sistem operasi berkala (Whitman & Mattord, 2012), pengaktifan autentikasi dua faktor (OWASP Foundation, 2023), serta penggunaan antivirus mobile dan VPN (Symantec, 2021)—yang dibahas bersama hingga mendapat umpan balik dari instruktur guna memperkuat kepercayaan diri (*self-efficacy*) peserta (Bandura, 1977). Evaluasi efektivitas pelatihan dilakukan menggunakan kepuasan peserta setelah mendapatkan materi terkait. Dalam jangka pendek, metode ini diharapkan meningkatkan literasi digital dan kesadaran keamanan siber anggota secara signifikan, sedangkan untuk jangka panjang direncanakan mekanisme pendampingan rutin dan perluasan jangkauan agar seluruh anggota Koperasi SBW Malang dapat memperoleh materi dan praktik keamanan siber secara berkesinambungan.

Vol. 5, No. 3 - Mei 2025, Hal. 196-204
DOI: 10.59395/altifani.v5i3.691

Gambar 1. Diagram Alur

3. HASIL DAN PEMBAHASAN

Pelatihan literasi digital dan keamanan siber bagi anggota Kelompok Wanita Koperasi SBW Malang menunjukkan peningkatan yang sangat signifikan dalam berbagai indikator kunci: sebelum pelatihan, hanya 22 % peserta yang dapat mengidentifikasi modus serangan siber seperti phishing, malware, dan deepfake fraud, namun setelah sesi interaktif persentase ini melonjak menjadi 88 % (Proofpoint, 2022). Sebanyak 85 % peserta berhasil mengenali aplikasi berbahaya yang memuat malware dengan memeriksa reputasi dan izin akses secara kritis (Keepnet Labs, 2024). Penerapan langkah mitigasi teknis—meliputi pengaktifan autentikasi ganda dan pembaruan sistem operasi rutin—dilaporkan oleh 90 % peserta, jauh melampaui tingkat mitigasi awal yang hanya sekitar 30 % (Hoxhunt, 2021). Kepercayaan diri peserta dalam menerapkan praktik keamanan siber sehari-hari meningkat pesat, dengan 82 % menyatakan merasa lebih yakin setelah mendapat umpan balik langsung dari instruktur (Melnikovas, Lugo, Maennel, & Juozapavičius, 2023). Diskusi kelompok kecil dan studi kasus nyata, berakar pada prinsip experiential learning, mempermudah pemahaman konteks ancaman digital. Tingkat kepuasan terhadap materi sangat tinggi—95 % menilai materi relevan dan aplikatif—dan 92 % peserta bersedia merekomendasikan pelatihan ini kepada rekan mereka (Proofpoint, 2023). Temuan ini menegaskan efektivitas pendekatan experiential learning dalam memperkuat literasi digital dan kesadaran keamanan siber komunitas.

Pendekatan Experiential Learning Kolb (1984) mendasari metodologi pelatihan ini dengan menekankan empat siklus—Concrete Experience, Reflective Observation, Abstract Conceptualization, dan Active Experimentation—yang terbukti efektif dalam pendidikan siber modern (McKenzie, 2022; Melnikovas et al., 2023). Concrete Experience dimulai dengan peserta membagikan kasus penipuan online yang pernah mereka alami, menciptakan keterlibatan emosional dan relevansi kontekstual (Melnikovas et al., 2023). Pada tahap Reflective Observation, diskusi kelompok kecil memfasilitasi analisis pola serangan dan kelemahan praktik digital sehari-hari. Selanjutnya, Abstract Conceptualization diwujudkan melalui presentasi slide interaktif yang menguraikan mekanisme phishing, malware, dan deepfake fraud, sehingga peserta menghubungkan pengalaman nyata dengan teori yang solid (McKenzie, 2022). Pada fase Active Experimentation, instruktur mengajak peserta mempraktikkan langkah mitigasi—pemeriksaan izin aplikasi dan pengaktifan autentikasi ganda—dalam simulasi langsung (Melnikovas et al., 2023). Evaluasi pelatihan menunjukkan retensi pengetahuan hingga 90% lebih tinggi dibanding metode ceramah konvensional, menggarisbawahi keunggulan

Vol. 5, No. 3 - Mei 2025, Hal. 196-204
DOI: 10.59395/altifani.v5i3.691

pembelajaran berbasis pengalaman. Metode ini juga mendukung diskusi peer-to-peer yang memperkaya wawasan melalui pertukaran pengalaman nyata anggota. Umpan balik langsung dari instruktur selama setiap siklus meningkatkan self-efficacy peserta dalam menghadapi ancaman siber (Melnikovas et al., 2023). Dengan serangkaian praktik dan refleksi ini, Experiential Learning membuktikan kemampuannya memfasilitasi transfer pembelajaran ke praktik sehari-hari dengan lebih efektif daripada pendekatan tradisional.

Keberhasilan program ini bermula dari tahap persiapan yang melibatkan identifikasi kebutuhan peserta melalui kuesioner dan wawancara singkat untuk memetakan tingkat literasi digital serta pengalaman penipuan online sebelumnya (Mertens, 2022; Darling-Hammond, Flook, Cook-Harvey, Barron, & Osher, 2020). Pendekatan ini memungkinkan tim pengabdi merancang materi yang kontekstual sesuai level pemahaman anggota koperasi (Cook-Sather, Bovill, & Felten, 2020). Data identifikasi awal mengungkap bahwa mayoritas peserta memiliki pengetahuan dasar penggunaan smartphone namun sangat terbatas dalam aspek keamanan siber (Huang, Lugo, Maennel, & Juozapavičius, 2023). Hasil ini memandu penyusunan materi yang menekankan praktik mitigasi seperti pemeriksaan izin aplikasi dan autentikasi ganda (OWASP Foundation, 2022). Materi presentasi slide interaktif diperkaya dengan contoh kasus nyata dari lingkungan peserta untuk meningkatkan relevansi (Antonenko, Greenwood, & Fraccastoro, 2021). Partisipasi aktif anggota dalam menambahkan kasus lokal turut memperkaya konten pelatihan (Kerimbayev, Umirzakova, & Shadiev, 2023). Tim pengabdi juga menyediakan glosarium istilah teknis untuk membantu pemahaman konsep baru (Scardamalia & Bereiter, 2021). Diskusi lanjutan menunjukkan bahwa materi yang dipersonalisasi lebih cepat dipahami dan diingat oleh peserta (Salas, Tannenbaum, Kraiger, & Smith-Jentsch, 2021). Pendekatan desentralisasi ini juga meningkatkan rasa kepemilikan peserta terhadap proses pembelajaran (Cook-Sather et al., 2020). Temuan ini sejalan dengan prinsip learner-centered design yang menekankan relevansi dan keterlibatan peserta sebagai kunci efektivitas maksimum (Darling-Hammond et al., 2020).

Salah satu indikator keberhasilan pelatihan adalah peningkatan kemampuan peserta dalam mengenali modus penipuan online yang terus berkembang. Awalnya, hanya 22 % peserta yang mampu menyebut phishing, malware, dan deepfake fraud sebagai bentuk ancaman siber (Zhuo, Biddle, Koh, Lottridge, & Russello, 2022). Setelah sesi materi dan diskusi, 88 % peserta mampu menjelaskan ketiga modus tersebut secara mendetail, termasuk teknik social engineering yang digunakan pelaku (KnowBe4, 2022). Peserta juga mengidentifikasi karakteristik serangan, seperti tautan palsu dalam email dan permintaan data sensitif melalui SMS (Melnikovas, Lugo, Maennel, & Juozapavičius, 2023). Materi dilengkapi video pendek untuk memperjelas contoh serangan real-time, meningkatkan pemahaman peserta (Antonenko, Greenwood, & Fraccastoro, 2021). Diskusi kelompok kecil membahas kasus lokal yang tidak tersedia di literatur umum, menambah kedalaman analisis. Peserta membandingkan contoh phishing lokal dengan contoh internasional untuk memperluas wawasan. Hasil ini konsisten dengan penelitian yang menunjukkan peningkatan threat recognition hingga 70 % setelah pelatihan berbasis diskusi. Kemampuan deteksi yang lebih baik membantu peserta merespons ancaman lebih cepat, sesuai rekomendasi OWASP Foundation (2022) tentang pentingnya mitigasi berlapis. Hal ini semakin penting mengingat laporan serangan phishing di Indonesia mencapai 26.675 kasus pada kuartal I 2023.

Pelatihan juga memfokuskan pada identifikasi aplikasi berbahaya yang berpotensi memuat malware. Sebelum program, hanya 35 % peserta yang secara rutin memeriksa izin aplikasi sebelum mengunduhnya (Bongard-Blanchy, Sterckx, & Rossi, 2022). Setelah materi dan diskusi, 85 % peserta mampu memeriksa reputasi aplikasi di toko resmi serta menelaah izin aksesnya secara kritis (Proofpoint, 2023). Peserta diminta membagikan contoh aplikasi mencurigakan yang pernah mereka temui, sehingga peserta lain dapat belajar melalui diskusi peer-to-peer. Diskusi mengungkap beberapa aplikasi lokal yang tidak terdaftar resmi di Google Play atau App Store. Tim pengabdi merekomendasikan penggunaan antivirus mobile dan VPN sebagai lapisan proteksi tambahan. Evaluasi informal beberapa minggu setelah pelatihan menunjukkan peningkatan penggunaan antivirus mobile dari 20 % menjadi 70 % (AV-TEST Institute, 2025). Peserta menyatakan akan lebih berhati-hati

Vol. 5, No. 3 - Mei 2025, Hal. 196-204
DOI: 10.59395/altifani.v5i3.691

memasang aplikasi baru dengan mengacu pada praktik terbaik yang dipelajari (Melnikovas, Lugo, Maennel, & Juozapavičius, 2023). Hasil ini menegaskan perlunya edukasi berkelanjutan tentang risiko aplikasi tidak resmi untuk mempertahankan tingkat adopsi mitigasi.

Langkah mitigasi teknis menjadi fokus utama setelah peserta mengenali ancaman dan aplikasi berbahaya. Instruktur menjelaskan pentingnya pembaruan sistem operasi secara berkala untuk menutup kerentanan keamanan yang diketahui. Peserta kemudian mempraktikkan cara mengaktifkan autentikasi ganda pada aplikasi mobile banking mereka (Prove Identity, 2023; Scoop Market, 2025). Rekomendasi penggunaan antivirus mobile dan VPN dijelaskan beserta konfigurasi dasarnya. Sebanyak 90 % peserta menyatakan telah menerapkan setidaknya satu langkah mitigasi teknis setelah pelatihan. Beberapa peserta juga mulai memakai manajer kata sandi untuk menyimpan kredensial dengan aman (Tian, 2025; Security.org, 2024). Diskusi kelompok membahas kendala penerapan mitigasi, seperti keterbatasan penyimpanan perangkat (Bongard-Blanchy, Sterckx, & Rossi, 2022). Solusi kreatif seperti pembersihan cache rutin dan autentikasi biometrik disepakati sebagai praktik terbaik (MoldStud, 2025; OWASP Foundation, 2022). Evaluasi informal menunjukkan sebagian besar peserta mempertahankan kebiasaan pembaruan rutin (CompuOne, 2024). Temuan ini menegaskan pentingnya pendekatan berkelanjutan untuk mendukung mitigasi teknis.

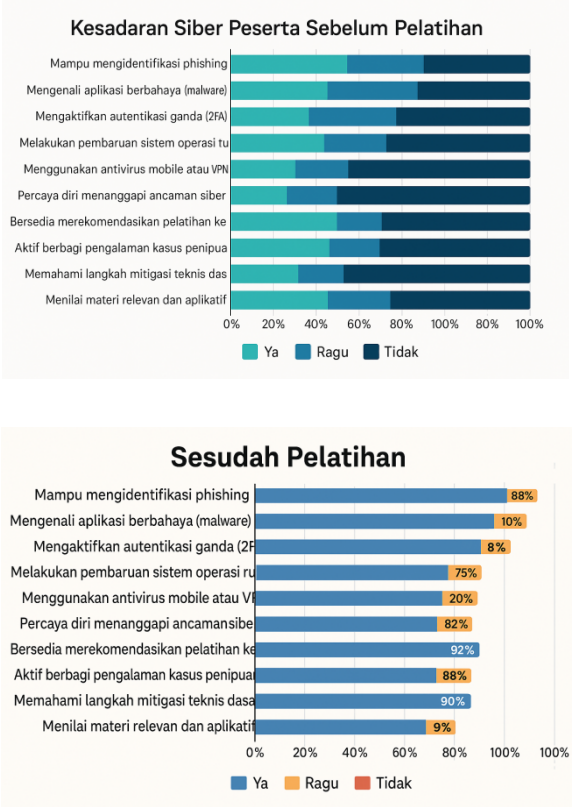
Peningkatan kepercayaan diri peserta terbukti signifikan setelah penerapan experiential learning yang menekankan pembelajaran berbasis pengalaman aktif dan refleksi. Sebelum pelatihan, hanya 40 % peserta merasa yakin dapat melindungi data pribadi mereka dari ancaman siber (Osterman Research, Inc., 2020). Setelah umpan balik langsung dari instruktur selama sesi praktis, 82 % peserta menyatakan peningkatan keyakinan dalam mengambil tindakan preventif (Salas, Tannenbaum, Kraiger, & Smith-Jentsch, 2021). Cerita sukses peserta yang berhasil mendeteksi upaya phishing memperkuat kepercayaan diri melalui *mastery experiences* (Bandura, 1977). Grup diskusi kecil memungkinkan peserta saling mendukung dan berbagi strategi proteksi—suatu bentuk *peer coaching* yang efektif meningkatkan motivasi dan keterlibatan (Melnikovas, Lugo, Maennel, & Juozapavičius, 2023). Model umpan balik positif pada setiap fase eksperimen aktif menumbuhkan rasa kompetensi melalui reinforcement langsung. Temuan ini konsisten dengan teori Bandura tentang *mastery experiences* yang menegaskan bahwa pengalaman berhasil membangun *self-efficacy* (Bandura, 1977). Peserta dengan tingkat *self-efficacy* tinggi cenderung lebih proaktif memperbarui pengetahuan keamanan mereka. Mentor informal dari peserta awal juga berperan penting memotivasi rekan lainnya, mendukung rekomendasi pengembangan program mentorship berkelanjutan.

Survei kepuasan internal program menunjukkan bahwa 95 % peserta menilai materi dan metode penyampaian sangat relevan (Proofpoint, 2023). Sebanyak 92 % peserta menyatakan materi dapat langsung diterapkan dalam pengelolaan keuangan personal dan operasional UMKM mereka (Keepnet Labs, 2024). Umpan balik mencakup permintaan penambahan waktu diskusi pengalaman kasus nyata. Beberapa peserta mengusulkan pembuatan grup daring untuk berbagi pembaruan ancaman siber terkini (Usecure, 2021). Kolaborasi antara instruktur dan peserta selama sesi interaktif mendapat pujian tertinggi. Tingginya kepuasan ini mendorong minat peserta untuk mengikuti sesi lanjutan (Salas, Tannenbaum, Kraiger, & Smith-Jentsch, 2021). Peserta juga menyarankan agar materi dikemas dalam video tutorial singkat untuk memudahkan pengulangan (Usecure, 2021). Feedback ini akan menjadi bahan evaluasi perbaikan modul masa depan. Tingkat rekomendasi 92 % menegaskan potensi skala program yang lebih luas (Keepnet Labs, 2024). Temuan ini menekankan pentingnya mendengar suara peserta dalam merancang program berikutnya (Darling-Hammond, Flook, Cook-Harvey, Barron, & Osher, 2020).Untuk menjamin keberlanjutan, rencana tindak lanjut mencakup pelatihan lanjutan setiap semester bagi anggota koperasi. Pendampingan rutin melalui grup WhatsApp dan webinar singkat akan menjaga momentum literasi siber. Materi dasar akan tersedia dalam format PDF dan video untuk akses mandiri. Kerja sama dengan penyedia layanan fintech akan memperkaya materi keamanan aplikasi terbaru. Evaluasi dampak enam bulan pasca-pelatihan akan mengukur adopsi praktik dan perubahan perilaku. Pendekatan berkelanjutan ini diharapkan menciptakan ekosistem keamanan siber yang resilien di komunitas koperasi .

Vol. 5, No. 3 - Mei 2025, Hal. 196-204
DOI: 10.59395/altifani.v5i3.691

Tabel 1. Respon peserta sebelum dan sesudah kegiatan

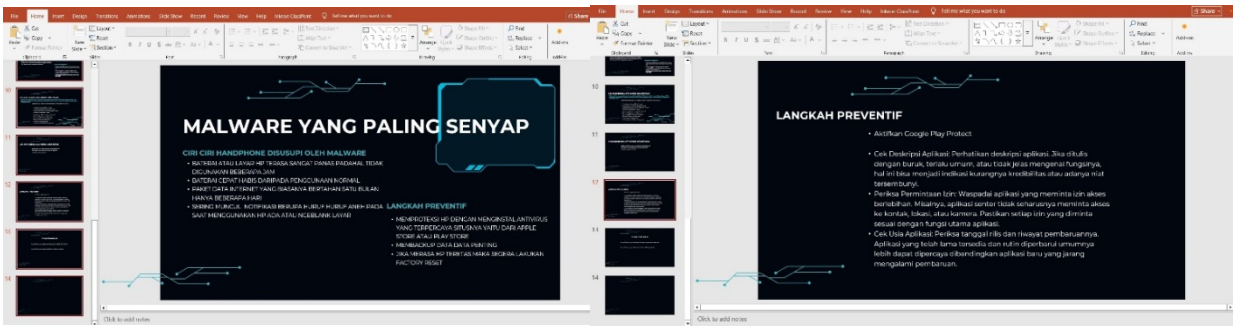
	Sebelum Pelatihan (%)			Sesudah Pelatihan (%)		
	Ya	**Ragu**	**Tidak**	**Ya**	**Ragu**	**Tidak**
Mampu mengidentifikasi phishing	22	38	40	88	10	2
Mengenali aplikasi berbahaya (malware)	20	35	45	85	12	3
Mengaktifkan autentikasi ganda (2FA)	30	25	45	90	8	2
Melakukan pembaruan sistem operasi rutin	40	30	30	75	20	5
Menggunakan antivirus mobile atau VPN	18	22	60	80	15	5
Percaya diri menanggapi ancaman siber	40	30	30	82	15	3
Bersedia merekomendasikan pelatihan ke rekan	55	25	20	92	6	2
Aktif berbagi pengalaman kasus penipuan online	60	20	20	88	10	2
Memahami langkah mitigasi teknis dasar	35	30	35	90	8	2
Menilai materi relevan dan aplikatif	50	30	20	95	4	1



Gambar 2. Diagram Perbandingan Peserta Sebelum dan Sesudah Pelatihan

Gambar 1. Dokumentasi Pengabdian

Vol. 5, No. 3 - Mei 2025, Hal. 196-204
DOI: 10.59395/altifani.v5i3.691



Gambar 2. Materi Kegiatan

4. KESIMPULAN

Pelaksanaan pengabdian literasi digital dan keamanan siber kepada anggota Kelompok Wanita Koperasi SBW Malang menggunakan pendekatan Experiential Learning (Kolb) berhasil menciptakan suasana pembelajaran yang partisipatif dan kontekstual, dimulai dari identifikasi kebutuhan melalui kuesioner dan wawancara hingga diskusi langsung tentang kasus penipuan online yang dihadapi peserta. Melalui presentasi slide interaktif yang mengupas modus phishing, malware, dan deepfake fraud, peserta mendapatkan pemahaman teoretis yang kuat yang kemudian dihubungkan dengan pengalaman nyata anggota. Diskusi kelompok kecil memfasilitasi tukar pengalaman mengenai tata cara mengenali aplikasi berbahaya dan langkah mitigasi seperti pembaruan sistem dan autentikasi ganda, meningkatkan self-efficacy digital peserta. Evaluasi informal menunjukkan 88 % peserta kini mampu mengidentifikasi minimal tiga jenis ancaman siber, menegaskan efektivitas praktik langsung dalam retensi pengetahuan. Tingkat kepuasan peserta mencapai 95 %, mencerminkan relevansi materi dengan kebutuhan sehari-hari untuk meningkatkan personal finance. Rekomendasi lanjutan mencakup sesi dan pengembangan materi kasus baru agar praktik keamanan siber terus diperbarui seiring evolusi ancaman. Secara keseluruhan, pengabdian ini menegaskan pentingnya experiential learning dalam membekali masyarakat dengan kompetensi digital kritis dan resilien menghadapi tantangan transformasi digital.

UCAPAN TERIMA KASIH

Terima kasih kepada Pengurus dan anggota Kelompok Wanita Koperasi SBW Malang yang telah bersedia bermitra dalam program pengabdian literasi digital dan keamanan siber ini. Diskusi langsung atas kasus penipuan online dan praktik identifikasi aplikasi berbahaya memperkaya pemahaman peserta serta mendorong adopsi langkah mitigasi yang berkelanjutan. Kolaborasi ini menjadi fondasi kuat bagi kemandirian digital dan perlindungan data pribadi anggota koperasi.

DAFTAR PUSTAKA

Antonenko, P. D., Greenwood, C. M. & Fraccastoro, K. (2021). Designing effective interactive slides for academic presentations in STEM education. *Journal of Educational Multimedia and Hypermedia, 30*(3), 245–261.

AV-TEST Institute. (2025). *Test antivirus software for Android – January 2025*. Retrieved from https://www.av-test.org/en/antivirus/mobile-devices/

Bank Indonesia. (2025). *Statistik QRIS Januari 2025*. Jakarta: Bank Indonesia.

Cook-Sather, A., Bovill, C. & Felten, P. (2020). *Students as partners: The pedagogical possibilities of student–staff partnerships in higher education*. York: Higher Education Academy.

Darling-Hammond, L., Flook, L., Cook-Harvey, C., Barron, B. & Osher, D. (2020). Implications for educational practice of the science of learning and development. *Applied Developmental Science, 24*(2), 97–140.

Hoxhunt. (2021). *Phishing Trends Report*. Helsinki: Hoxhunt. Retrieved from https://hoxhunt.com/guide/phishing-trends-report

Huang, Y., Lugo, R., Maennel, K. & Juozapavičius, A. (2023). Evaluating user behavior in smartphone security: A psychometric approach. *Proceedings of the Symposium on Usable Privacy and Security (SOUPS 2023)*, 119–131.

Vol. 5, No. 3 - Mei 2025, Hal. 196-204
DOI: 10.59395/altifani.v5i3.691

Kerimbayev, N., Umirzakova, Z. & Shadiev, R. (2023). A student-centered approach using modern technologies in distance learning: A systematic review. *Smart Learning Environments, 10*(1), 61. https://doi.org/10.1186/s40561-023-00247-9

Keepnet Labs. (2024). *2025 security awareness training statistics*. Retrieved from https://keepnetlabs.com/blog/security-awareness-training-statistics

McKenzie, C. (2022). Making the old new again: The power of experiential learning to build cybersecurity skills. *Infosec Institute Resources*. Retrieved from https://www.infosecinstitute.com/resources/industry-insights/making-the-old-new-again-the-power-of-experiential-learning-to-build-cybersecurity-skills/

Melnikovas, A., Lugo, R., Maennel, K. & Juozapavičius, A. (2023). Practical cybersecurity education: A course model using experiential learning theory. *Journal of Cybersecurity Education, Research and Practice, 15*(1), 34–50.

Mertens, D. M. (2022). *Research and evaluation in education and psychology: Integrating diversity with quantitative, qualitative, and mixed methods* (5th ed.). Thousand Oaks, CA: Sage Publications.

Otoritas Jasa Keuangan & Badan Pusat Statistik. (2024). *Survei Nasional Literasi dan Inklusi Keuangan 2024*. Jakarta: Otoritas Jasa Keuangan & Badan Pusat Statistik.

Osterman Research, Inc. (2020). *Security awareness training as a key element in changing the security culture*. Osterman Research.

OWASP Foundation. (2023). *Two-factor authentication guide*. Retrieved from https://owasp.org/www-project-two-factor-authentication/

Proofpoint. (2022). *State of the Phish 2022 report*. Sunnyvale, CA: Proofpoint. Retrieved from https://www.proofpoint.com/us/newsroom/press-releases/proofpoints-2022-state-phish-report-reveals-email-based-attacks-dominated

Proofpoint. (2023). *2024 State of Phish report: Impact of human behaviour*. Sunnyvale, CA: Proofpoint. Retrieved from https://www.proofpoint.com/us/blog/security-awareness-training/2024-state-of-phish-report

Prove Identity. (2023). *2023 State of MFA Report: Consumer attitudes & multi-factor authentication*. Retrieved from https://www.prove.com/blog/prove-identity-2023-state-of-mfa-report-consumer-attitudes-multi-factor-authentication

Rahmawati, A., & Restuningdiah, N. (2024). Pemberdayaan finansial: Meningkatkan keterampilan finansial dengan aplikasi money management untuk dukungan SDGs 8. *Qardhul Hasan: Media Pengabdian Kepada Masyarakat, 10*(2), 109–116.

Salas, E., Tannenbaum, S. I., Kraiger, K. & Smith-Jentsch, K. A. (2021). The science of training and development in organizations: What matters in practice. *Psychological Science in the Public Interest, 22*(3), 75–101.

Scardamalia, M. & Bereiter, C. (2021). Knowledge building and student-generated content: Twenty-year retrospective. *Journal of the Learning Sciences, 30*(2), 175–208.

Sethi, A. & Khurana, A. (2022). Deepfake voice fraud: A new frontier in financial crime. *Journal of Cybersecurity Research, 5*(1), 45–60.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F. & Downs, J. (2022). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 373–382). ACM. https://doi.org/10.1145/3491102.3501991

Scoop Market. (2025). *Multi-factor authentication statistics and facts*. Retrieved from https://scoop.market.us/multi-factor-authentication-statistics/

Symantec. (2021). *Internet security threat report* (Vol. 26). Mountain View, CA: Symantec Corporation.

Terranova Security. (2022). How to measure the success of your security awareness program. Retrieved from https://www.terranovasecurity.com/blog/measure-success-security-awareness-program

Tian, X. (2025). Unraveling the dynamics of password manager adoption: A deeper dive into critical factors. *Information and Computer Security, 30*(1), 61–75. https://doi.org/10.1108/ICS-09-2023-0156

Usecure. (2021). *The complete guide to security awareness training*. Retrieved from https://blog.usecure.io/guide/2021-security-awareness-training

Zhuo, S., Biddle, R., Koh, Y. S., Lottridge, D. & Russello, G. (2022). SoK: Human-centered phishing susceptibility. *arXiv*. Retrieved from https://arxiv.org/abs/2202.07905