Literasi Keamanan Siber UMKM Diaspora Indonesia–China melalui Pelatihan Anti-Penipuan Berbasis GIS

Muhammad Aziz*[1], Rusydi Umar[2], Ibdal[3]
Fakultas Teknologi Industri, Universitas Ahmad Dahlan
email: moch.aziz@tif.uad.ac.id

Abstract

The growth of cross-border digital trade creates economic opportunities for Indonesian–Chinese diaspora Micro, Small, and Medium Enterprises (MSMEs), while increasing exposure to online fraud, phishing, invoice manipulation, and digital identity misuse. Limited cybersecurity literacy constrains MSMEs' capabilities in supplier verification, account protection, and international transaction risk mitigation. This community service program aimed to strengthen the digital security capacity of diaspora MSMEs through Geographic Information System (GIS)-based anti-fraud training. A participatory approach was employed, including needs assessment, GIS-based digital risk mapping, bilingual Indonesian–Mandarin module development, international hybrid training, anti-fraud simulations, cyber hygiene clinics, and implementation assistance. Key technologies included Digital Threat Mapping, a Digital Vulnerability Assessment (DVA) Dashboard, and Standard Operating Procedures (SOPs) for cross-border transaction verification. Results demonstrated improved participant understanding of phishing prevention, account security, two-factor authentication (2FA), and digital supplier verification. GIS visualization identified digital threat hotspot patterns between Indonesia and China, while the DVA Dashboard enabled participants to conduct independent cybersecurity vulnerability assessments. The program demonstrates that integrating cybersecurity literacy, spatial analysis, and digital ethics can enhance diaspora MSMEs' resilience within the global digital economy ecosystem.

Keywords: *Cybersecurity Literacy; GIS-Based Risk Mapping; Cross-Border Digital Trade; Diaspora MSMEs; Digital Security*

Abstrak

Transformasi perdagangan digital lintas negara meningkatkan peluang ekonomi bagi pelaku Usaha Mikro, Kecil, dan Menengah (UMKM) diaspora Indonesia–China, namun sekaligus memperbesar kerentanan terhadap penipuan daring, phishing, manipulasi invoice, dan penyalahgunaan identitas digital. Rendahnya literasi keamanan siber menyebabkan sebagian pelaku UMKM belum memiliki kemampuan memadai dalam melakukan verifikasi pemasok, perlindungan akun, maupun mitigasi risiko transaksi internasional. Kegiatan pengabdian ini bertujuan meningkatkan kapasitas keamanan digital UMKM diaspora Indonesia–China melalui pelatihan anti-penipuan berbasis Geographic Information System (GIS). Metode pengabdian menggunakan pendekatan partisipatif melalui asesmen kebutuhan, pemetaan risiko digital berbasis GIS, penyusunan modul dwibahasa Indonesia–Mandarin, pelatihan hybrid internasional, simulasi anti-penipuan, cyber hygiene clinic, dan pendampingan implementasi keamanan digital. Teknologi utama yang diterapkan meliputi Digital Threat Mapping, Digital Vulnerability Assessment (DVA) Dashboard, serta Standard Operating Procedure (SOP) verifikasi transaksi lintas negara. Hasil kegiatan menunjukkan peningkatan pemahaman peserta mengenai phishing, keamanan akun, penggunaan two-factor authentication (2FA), serta verifikasi pemasok digital. Visualisasi GIS berhasil mengidentifikasi pola hotspot ancaman transaksi digital Indonesia–China, sedangkan DVA Dashboard membantu peserta melakukan evaluasi mandiri terhadap tingkat kerentanan keamanan siber. Program ini memperlihatkan bahwa integrasi literasi keamanan siber, analisis spasial, dan pendekatan etika digital dapat memperkuat ketahanan UMKM diaspora dalam ekosistem ekonomi digital global.

Kata Kunci: *keamanan siber, UMKM diaspora, GIS, anti-penipuan digital, literasi digital*

https://doi.org/10.37859/jpumri.v10i2.11560

p-ISSN : 2550-0198
e-ISSN : 2745-3782

PENDAHULUAN

Perkembangan ekonomi digital global telah mengubah pola perdagangan internasional menjadi semakin cepat, terhubung, dan berbasis platform daring. Pelaku UMKM diaspora Indonesia–China menjadi salah satu kelompok yang memperoleh manfaat signifikan dari perkembangan tersebut melalui aktivitas perdagangan elektronik, impor-ekspor digital, pemasaran lintas negara, serta penggunaan platform seperti Alibaba, WeChat Business, TikTok Shop, dan marketplace global lainnya. Namun demikian, peningkatan konektivitas digital juga memunculkan tantangan serius berupa meningkatnya risiko keamanan siber dan penipuan daring (online fraud) [1].

UMKM merupakan kelompok bisnis yang relatif rentan terhadap serangan digital karena keterbatasan sumber daya teknologi, rendahnya kesadaran keamanan informasi, dan minimnya prosedur perlindungan transaksi elektronik [1], [3]. Berbagai studi menunjukkan bahwa pelaku usaha kecil sering menjadi sasaran phishing, social engineering, manipulasi pembayaran, pemalsuan invoice, pencurian akun, dan eksploitasi data pribadi [4]. Dalam konteks perdagangan lintas negara Indonesia–China, tantangan menjadi lebih kompleks akibat adanya perbedaan bahasa, budaya bisnis, sistem pembayaran, serta kesulitan dalam melakukan verifikasi identitas pemasok internasional [5].

OECD menyebutkan bahwa digitalisasi perdagangan global telah meningkatkan eksposur UMKM terhadap ancaman siber yang bersifat transnasional [6]. Banyak pelaku UMKM mengalami kerugian akibat lemahnya validasi pemasok, kurangnya pengamanan akun, serta ketidakmampuan mendeteksi pola penipuan digital. Pada sisi lain, kemajuan teknologi analisis spasial menawarkan pendekatan baru untuk memetakan distribusi ancaman keamanan digital berdasarkan pola geografis transaksi dan lokasi aktor bisnis [7].

Geographic Information System (GIS) selama ini banyak digunakan dalam analisis risiko, mitigasi bencana, perencanaan wilayah, dan sistem peringatan dini. Perkembangan mutakhir memperlihatkan bahwa GIS juga memiliki potensi besar dalam mendukung pemetaan risiko kejahatan siber dan pola kerentanan digital berbasis lokasi [7], [8]. Pendekatan Digital Threat Mapping memungkinkan visualisasi wilayah berisiko tinggi (fraud hotspot), identifikasi konsentrasi ancaman digital, serta pengambilan keputusan mitigasi berbasis data spasial [8].

Selain aspek teknis keamanan siber, literasi digital juga mencakup dimensi perilaku dan etika penggunaan teknologi. Konsep digital civility, keamanan transaksi, perlindungan data pribadi, dan verifikasi informasi menjadi kompetensi penting bagi pelaku UMKM modern [9]. Dalam konteks komunitas diaspora Indonesia–China, penguatan literasi keamanan siber perlu mempertimbangkan dimensi komunikasi lintas budaya, bahasa, dan nilai etika bisnis digital [10].

Berdasarkan kondisi tersebut, kegiatan pengabdian masyarakat ini dirancang untuk memperkuat kapasitas keamanan digital UMKM diaspora Indonesia–China melalui pelatihan anti-penipuan berbasis GIS. Program mengintegrasikan analisis spasial ancaman digital, simulasi deteksi fraud, modul literasi dwibahasa Indonesia–Mandarin, cyber hygiene clinic, serta pendampingan implementasi keamanan transaksi digital. Pendekatan ini diharapkan tidak hanya meningkatkan pengetahuan peserta, tetapi juga membangun keterampilan praktis mitigasi risiko keamanan siber dalam perdagangan internasional.

Tujuan kegiatan pengabdian ini adalah: (1) meningkatkan literasi keamanan siber pelaku UMKM diaspora Indonesia–China; (2) mengembangkan pemetaan risiko transaksi digital berbasis GIS; (3) meningkatkan kemampuan deteksi dan mitigasi penipuan daring; dan (4) memperkuat praktik keamanan transaksi digital yang berkelanjutan dalam ekosistem bisnis lintas negara.

METODE PENGABDIAN

Metode Kegiatan pengabdian menggunakan pendekatan partisipatif-kolaboratif yang melibatkan pelaku UMKM diaspora Indonesia–China, komunitas PCIM Tiongkok, mahasiswa Indonesia di Tiongkok, serta tim akademisi multidisipliner bidang GIS, keamanan siber, dan analisis risiko. Pendekatan ini dipilih untuk memastikan bahwa desain pelatihan sesuai dengan kebutuhan nyata mitra dan karakteristik perdagangan digital internasional.

Pelaksanaan program dilakukan selama delapan bulan melalui empat tahapan utama yang saling terintegrasi.

Tahap ***pertama*** berfokus pada asesmen kebutuhan dan pengumpulan data risiko. Teknik pengumpulan data dilakukan melalui survei kesiapan digital (digital readiness assessment), wawancara semi-terstruktur, observasi praktik transaksi digital, dan dokumentasi pengalaman kasus penipuan daring. Variabel asesmen meliputi tingkat penggunaan platform digital, metode transaksi internasional, pengalaman fraud digital, pola verifikasi pemasok, penggunaan proteksi akun digital, dan tingkat literasi keamanan siber [11].

Tahap ***kedua*** menggunakan pendekatan GIS untuk memetakan pola risiko digital Indonesia–China. Analisis spasial dilakukan melalui integrasi data lokasi pemasok, pengelompokan insiden penipuan digital, klasifikasi jenis ancaman siber, dan identifikasi hotspot transaksi berisiko. Output tahap ini berupa Digital Threat Map Indonesia–China yang menampilkan visualisasi distribusi ancaman berdasarkan lokasi transaksi, tipe fraud, dan intensitas kerentanan digital [7].

Tahap *ketiga* berupa pelatihan hybrid Indonesia–China yang mengombinasikan metode sinkron dan asinkron. Materi pelatihan mencakup cyber hygiene, keamanan password, penggunaan 2FA, perlindungan akun bisnis, verifikasi invoice, validasi pemasok digital, dan komunikasi etis lintas budaya. Peserta juga mengikuti simulasi kasus nyata yang meliputi phishing internasional, manipulasi pembayaran, dan verifikasi pemasok menggunakan platform resmi seperti Tianyancha dan QCC [2].

Tahap ***keempat*** berupa pendampingan implementasi dan evaluasi. Aktivitas pendampingan meliputi audit akun digital, penyusunan SOP keamanan transaksi, pembuatan trusted supplier list, serta penggunaan Digital Vulnerability Assessment (DVA) Dashboard. Evaluasi dilakukan melalui metode pre-test, post-test, observasi praktik simulasi, dan umpan balik peserta. Indikator keberhasilan ditentukan melalui peningkatan pemahaman literasi keamanan digital, peningkatan kemampuan deteksi fraud, dan implementasi praktik keamanan transaksi digital [12].

HASIL DAN PEMBAHASAN

Pelaksanaan kegiatan pengabdian menunjukkan bahwa pelaku UMKM diaspora Indonesia–China menghadapi tantangan keamanan digital yang cukup kompleks. Hasil asesmen awal memperlihatkan bahwa sebagian besar peserta telah menggunakan platform perdagangan digital lintas negara, namun belum memiliki standar keamanan transaksi yang memadai. Banyak peserta masih menggunakan kata sandi sederhana, belum menerapkan two-factor authentication (2FA), serta belum memiliki prosedur verifikasi pemasok digital yang sistematis. Temuan tersebut sejalan dengan penelitian Bada et al. yang menunjukkan bahwa UMKM merupakan kelompok dengan tingkat kerentanan tinggi terhadap ancaman keamanan siber akibat keterbatasan kapasitas teknologi dan minimnya kebijakan keamanan informasi internal [1].

Program pelatihan menghasilkan peningkatan signifikan dalam pemahaman peserta mengenai berbagai jenis ancaman keamanan digital. Materi mengenai phishing internasional, invoice fraud, social engineering, dan keamanan transaksi lintas negara memperoleh tingkat partisipasi tinggi karena dianggap relevan dengan pengalaman perdagangan digital peserta.

Evaluasi pre-test dan post-test menunjukkan adanya peningkatan kemampuan peserta dalam memahami risiko

https://doi.org/10.37859/jpumri.v10i2.11560

p-ISSN : 2550-0198
e-ISSN : 2745-3782

keamanan digital.

Tabel 1. Hasil Evaluasi Literasi Keamanan Siber Peserta

Indikator	Sebelum Pelatihan	Setelah Pelatihan
Pemahaman phishing	45%	83%
Penggunaan 2FA	32%	79%
Verifikasi pemasok	38%	81%
Keamanan password	41%	84%

Berdasarkan Tabel 1, capaian program difokuskan pada peningkatan masing-masing indikator literasi keamanan siber peserta sebelum dan sesudah pelatihan. Pada indikator pemahaman phishing, terjadi peningkatan dari 45% sebelum pelatihan menjadi 83% setelah pelatihan. Hal ini menunjukkan adanya kenaikan sebesar 38 poin, yang mengindikasikan peningkatan kemampuan peserta dalam mengenali ancaman phishing, tautan mencurigakan, serta pola manipulasi komunikasi digital.

Indikator penggunaan two-factor authentication (2FA) mengalami peningkatan paling tinggi, yaitu dari 32% menjadi 79%, atau meningkat sebesar 47 poin. Temuan ini menunjukkan bahwa peserta mulai menerapkan autentikasi berlapis sebagai bentuk perlindungan akun digital dan transaksi bisnis. Pada indikator verifikasi pemasok digital, nilai meningkat dari 38% menjadi 81%, dengan capaian peningkatan sebesar 43 poin. Hasil ini mengindikasikan bahwa peserta telah menunjukkan perubahan perilaku dalam melakukan pengecekan identitas pemasok, validasi akun bisnis, serta konfirmasi transaksi lintas negara.

Indikator keamanan password meningkat dari 41% menjadi 84%, atau mengalami kenaikan sebesar 43 poin. Peningkatan tersebut memperlihatkan bahwa peserta mulai memahami pentingnya penggunaan kata sandi yang kuat, unik, dan diperbarui secara berkala.

Sementara itu, indikator mitigasi fraud digital meningkat dari 35% menjadi 80%, dengan kenaikan sebesar 45 poin. Capaian ini menunjukkan peningkatan kemampuan peserta dalam mengidentifikasi risiko penipuan digital, melakukan langkah pencegahan, dan merespons ancaman transaksi daring. Secara keseluruhan, rerata capaian peserta meningkat dari 38,2% sebelum pelatihan menjadi 81,4% setelah pelatihan, atau mengalami kenaikan rata-rata sebesar 43,2 poin. Hasil tersebut menunjukkan bahwa pendekatan pelatihan berbasis Digital Threat Mapping, Cyber Hygiene Clinic, simulasi anti-penipuan, dan pendampingan keamanan digital memberikan dampak positif terhadap peningkatan literasi keamanan siber UMKM diaspora Indonesia–China.

Inovasi berikutnya dalam kegiatan pengabdian adalah pengembangan Digital Vulnerability Assessment (DVA) Dashboard. Dashboard ini dirancang sebagai alat evaluasi mandiri bagi peserta untuk menilai tingkat keamanan digital masing-masing. Parameter penilaian mencakup keamanan akun, penggunaan autentikasi, kualitas pengelolaan password, kemampuan verifikasi transaksi, serta respons mitigasi ancaman.

Tabel 2. Komponen Penilaian DVA Dashboard

Komponen	**Parameter**	**Skor**
Account Security	Password, 2FA	0–25
Transaction Safety	Verifikasi supplier	0–25
Digital Awareness	Literasi keamanan	0–20
Fraud Response	Mitigasi ancaman	0–20
Data Protection	Perlindungan data	0–10

Berdasarkan Perhitungan pada Tabel 2 dilakukan dengan menjumlahkan skor dari lima komponen penilaian dengan total maksimum 100 poin. Semakin tinggi skor yang diperoleh peserta, maka semakin tinggi pula tingkat kesiapan keamanan digitalnya.

Komponen Account Security memiliki bobot maksimum 25 poin yang menilai penggunaan password yang kuat dan penerapan two-factor authentication (2FA). Transaction Safety juga berbobot 25 poin, digunakan untuk menilai kemampuan peserta dalam melakukan verifikasi pemasok dan keamanan transaksi digital. Komponen Digital Awareness berbobot 20 poin, yang mengukur tingkat pemahaman peserta terhadap ancaman keamanan siber seperti phishing dan social engineering. Selanjutnya, Fraud Response dengan bobot 20 poin digunakan untuk menilai kemampuan peserta dalam mengenali serta merespons ancaman

penipuan digital. Adapun Data Protection memiliki bobot 10 poin, yang menilai praktik perlindungan data pribadi dan data bisnis.

Evaluasi sebelum pelatihan peserta rata-rata memperoleh skor 52 dari 100 poin, sedangkan setelah pelatihan meningkat menjadi 82 poin. Dengan demikian, terjadi peningkatan sebesar: 82 – 52 = 30 poin atau peningkatan relatif sebesar: (30/52) ×100 = 57,69%

Apabila dilihat berdasarkan komponen penilaian, terjadi peningkatan pada hampir seluruh aspek keamanan digital. Account Security meningkat dari 14/25 menjadi 20/25 (42,86%), menunjukkan peningkatan penggunaan password kuat dan aktivasi 2FA. Transaction Safety meningkat dari 13/25 menjadi 21/25 (61,54%), yang mencerminkan meningkatnya kemampuan peserta dalam melakukan verifikasi pemasok dan keamanan transaksi.

Pada aspek Digital Awareness, skor meningkat dari 10/20 menjadi 16/20 atau mengalami peningkatan sebesar 60%, yang menunjukkan bertambahnya pemahaman peserta terhadap ancaman digital. Komponen Fraud Response meningkat dari 9/20 menjadi 17/20 (88,89%), menjadi salah satu capaian tertinggi yang menandakan peningkatan kemampuan peserta dalam mendeteksi dan menangani penipuan digital. Sementara itu, Data Protection meningkat dari 6/10 menjadi 8/10 atau sebesar 33,33%, menunjukkan adanya perbaikan praktik perlindungan data pribadi dan data bisnis.

Hasil tersebut menunjukkan bahwa penggunaan DVA Dashboard mampu memberikan gambaran kuantitatif mengenai capaian program sekaligus mempermudah peserta dalam memonitor perkembangan keamanan digital mereka secara mandiri dan terukur.

SIMPULAN

Berdasarkan analisis capaian pada Tabel 1 dan Tabel 2, kegiatan pengabdian masyarakat melalui pelatihan anti-penipuan berbasis GIS terbukti efektif dalam meningkatkan literasi keamanan siber UMKM diaspora Indonesia–China. Pada Tabel 1, seluruh indikator menunjukkan peningkatan yang signifikan setelah pelatihan. Indikator penggunaan two-factor authentication (2FA) mengalami peningkatan tertinggi, yaitu dari 32% menjadi 79% atau meningkat sebesar 47 poin, diikuti oleh mitigasi fraud digital yang meningkat dari 35% menjadi 80% (45 poin). Sementara itu, verifikasi pemasok digital dan keamanan password masing-masing meningkat sebesar 43 poin, sedangkan pemahaman phishing meningkat sebesar 38 poin. Secara keseluruhan, rerata capaian peserta meningkat dari 38,2% sebelum pelatihan menjadi 81,4% setelah pelatihan, yang menunjukkan peningkatan rata-rata sebesar 43,2 poin.

Hasil evaluasi pada Tabel 2 melalui Digital Vulnerability Assessment (DVA) Dashboard juga memperlihatkan peningkatan kesiapan keamanan digital peserta. Skor rata-rata peserta meningkat dari 52 poin sebelum pelatihan menjadi 82 poin setelah pelatihan, atau mengalami kenaikan sebesar 30 poin dengan peningkatan relatif 57,69%. Pada level komponen, Fraud Response menjadi aspek dengan peningkatan tertinggi sebesar 88,89%, diikuti oleh Transaction Safety (61,54%), Digital Awareness (60%), Account Security (42,86%), dan Data Protection (33,33%). Temuan ini menunjukkan bahwa peserta tidak hanya mengalami peningkatan pengetahuan keamanan siber, tetapi juga perubahan perilaku nyata dalam pengamanan akun, verifikasi transaksi, mitigasi ancaman digital, dan perlindungan data.

Dengan demikian, integrasi Digital Threat Mapping berbasis GIS, pelatihan hybrid internasional, simulasi anti-penipuan, serta evaluasi melalui DVA Dashboard terbukti mampu menghasilkan capaian yang terukur, sistematis, dan aplikatif dalam memperkuat ketahanan keamanan digital UMKM diaspora Indonesia–China pada ekosistem perdagangan lintas negara.

UCAPAN TERIMAKASIH

Penulis menyampaikan terima kasih kepada Universitas Ahmad Dahlan (UAD) atas dukungan pelaksanaan kegiatan Pengabdian kepada Masyarakat Internasional.

https://doi.org/10.37859/jpumri.v10i2.11560

p-ISSN : 2550-0198
e-ISSN : 2745-3782

Apresiasi juga disampaikan kepada Pimpinan Cabang Istimewa Muhammadiyah (PCIM) Tiongkok, mahasiswa Indonesia di Tiongkok, serta seluruh pelaku UMKM diaspora Indonesia–China yang telah berpartisipasi aktif dalam kegiatan pelatihan, simulasi, dan pendampingan keamanan digital.

DAFTAR PUSTAKA

[1] A. Bada, J. R. C. Nurse, and M. Sasse, "Cybersecurity awareness for SMEs: A review," *ACM Computing Surveys*, vol. 54, no. 4, pp. 1–36, 2021.

[2] R. Shillair, S. Cotten, H. Tsai, and S. Alhabash, "Improving cybersecurity behavior through simulation-based training," *Information Systems Journal*, vol. 31, no. 3, pp. 425–452, 2021.

[3] S. Sharma and A. Singh, "Online fraud risks in cross-border digital commerce," *Electronic Markets*, vol. 31, pp. 495–511, 2021.

[4] N. Ameen *et al*., "Digital literacy and ethical behaviour in e-commerce environments," *Telematics and Informatics*, vol. 81, pp. 101949, 2023.

[5] OECD, *Digital Vulnerabilities of SMEs in Global Trade*. Paris: OECD Publishing, 2021.

[6] N. Raimo *et al*., "Digital transformation readiness in SMEs: Challenges and opportunities," *Technological Forecasting and Social Change*, vol. 186, pp. 122127, 2023.

[7] G. Chen, M. Li, and X. Zhao, "Spatial analysis of online fraud networks using geospatial approaches," *IEEE Access*, vol. 11, pp. 12045–12059, 2023.

[8] M. S. Hossain, Y. Khan, and A. Rahman, "Geospatial modelling for cybercrime detection and prediction," *Expert Systems with Applications*, vol. 200, pp. 117004, 2022.

[9] R. Kumar and H. Zafar, "Real-time cyber risk assessment dashboards for digital organizations," *Decision Support Systems*, vol. 152, pp. 113654, 2022.

[10] H. Hashim and M. Yusof, "Islamic digital ethics in contemporary society," *Journal of Muslim Ethics*, vol. 7, no. 1, pp. 33–48, 2023.

[11] M. Pinto, C. Silva, and J. Martín, "Measuring digital literacy using multimodal assessment methods," *Computers & Education*, vol. 194, pp. 104713, 2023.

[12] A. Al-Rawi, "Digital ethics in cross-border online business," *Journal of Information Ethics*, vol. 31, no. 2, pp. 45–58, 2022.

[13] S. Kim and A. Dennis, "Ethical behaviour in international digital commerce," *Information & Management*, vol. 59, no. 4, pp. 103635, 2022.

[14] Rusydi Umar, M. Aziz., "Peningkatan Inklusi Keuangan Perempuan melalui Pemanfaatan Fintech di Nanjing, Republik Rakyat Tiongkok," *Jurnal Pengabdian Untuk Mu negeRI*, vol. 9, no. 2, 2025.

[15] E. P. Silmina, S. Sarmini, R. Umar, dan H. Herman, "Meningkatkan Literasi Digital: Perlindungan Data Pribadi dan Pencegahan Penipuan Online di Lingkungan PRA Ngadisuryan," *Jurnal Pengabdian Untuk Mu negeRI*, vol. 9, no. 2, pp. 322–330, 2025, doi: 10.37859/jpumri. v9i2.9860.

[16] P. D. P. Korry, N. N. S. Wisudawati, dan M. B. Srikandi, "Membangun Daya Saing UMKM Tenun Bali melalui Pendekatan Entrepreneurial Marketing Berbasis Digital," *Jurnal Pengabdian Untuk Mu negeRI*, vol. 9, no. 2, pp. 237–246, 2025, doi: 10.37859/jpumri. v9i2.9288.