Jurnal Inovasi dan Pengabdian
ISSN 3109-8916 (online)
https://athallahpublishing.com/index.php/bhaktika/index

OPEN ACCESS

Vol. 2, No. 1, 2026

DOI: 10.64845/bhaktika.v1i2

Penyuluhan dan Edukasi Tantangan Bagi Pelaku Usaha dalam Menghadapi Masalah *Cybercrime* di Era Digital

Yusuf Setyadi[1], **Haris Iriyanto**[2], **M. Fariz Rahman Hidayat**[3] **Tias Ekaliana**[4]
[1, 2, 3,4] *Universitas Siber Asia, Indonesia*
Corresponding Author: yusufsetyadi@lecturer.unsia.ac.id

A B S T R A C T

The development of digital technology brings both opportunities and challenges for businesses, particularly in addressing the threat of cybercrime. Crimes such as phishing, account hacking, online fraud, and personal data theft are on the rise, often targeting small and medium-sized businesses. This outreach and education program aims to increase business owners' understanding, awareness, and ability to identify and anticipate various forms of cyber threats in the digital era. The method used is an educational approach through outreach, interactive discussions, and mentoring for business owners. The results of the activity indicate an increase in participant awareness of the importance of digital security, the use of secure software, and caution when accessing suspicious links, emails, and messages. With this outreach, it is hoped that business owners will be able to implement preventive measures to protect their data and business continuity from the risk of cybercrime.

Keywords: Counseling, Education, Business Actors, Cybercrime, Digital Security

Received:	Revised:	Accepted:	Available online:
01.10.2025	01.11.2025	01.01.2026	19.02.2026

A B S T R A C T

Perkembangan teknologi digital membawa peluang sekaligus tantangan bagi pelaku usaha, khususnya dalam menghadapi ancaman kejahatan dunia maya (*cybercrime*). Modus kejahatan seperti *phishing*, peretasan akun, penipuan daring, dan pencurian data pribadi semakin meningkat dan banyak menyasar pelaku usaha kecil dan menengah. Kegiatan penyuluhan dan edukasi ini bertujuan untuk meningkatkan pemahaman, kewaspadaan, serta kemampuan pelaku usaha dalam mengidentifikasi dan mengantisipasi berbagai bentuk ancaman siber di era digital. Metode yang digunakan berupa pendekatan edukatif melalui sosialisasi, diskusi interaktif, dan pendampingan kepada pelaku usaha. Hasil kegiatan menunjukkan adanya peningkatan kesadaran peserta terhadap pentingnya keamanan digital, penggunaan perangkat lunak yang aman, serta kehati-hatian dalam mengakses tautan, email, dan pesan mencurigakan. Dengan adanya penyuluhan ini, diharapkan pelaku usaha mampu menerapkan langkah-langkah preventif guna melindungi data dan keberlangsungan usahanya dari risiko *cybercrime*.

Keywords: Penyuluhan, Edukasi, Pelaku Usaha, Cybercrime, Keamanan Digital

Received:	Revised:	Accepted:	Available online:
01.10.2025	01.11.2025	01.01.2026	19.02.2026

PENDAHULUAN

Perkembangan teknologi digital dalam satu dekade terakhir telah membawa perubahan signifikan dalam berbagai aspek kehidupan, termasuk dalam sektor ekonomi dan bisnis. Transformasi digital mendorong pelaku usaha untuk memanfaatkan internet, media sosial, marketplace, serta berbagai aplikasi berbasis teknologi dalam menjalankan dan mengembangkan usahanya. Digitalisasi memberikan kemudahan dalam promosi, transaksi, komunikasi dengan pelanggan, hingga pengelolaan keuangan secara lebih efisien. Namun, di balik kemudahan tersebut, muncul tantangan baru berupa meningkatnya risiko kejahatan dunia maya (*cybercrime*) yang semakin kompleks dan terorganisir (UNCTAD, 2021). Fenomena *cybercrime* mengalami peningkatan signifikan sejak percepatan digitalisasi pascapandemi COVID-19. Ketergantungan masyarakat dan pelaku usaha terhadap teknologi digital membuka peluang bagi pelaku kejahatan untuk memanfaatkan celah keamanan sistem dan rendahnya literasi digital pengguna (Interpol, 2022). Bentuk kejahatan siber yang umum terjadi antara lain *phishing*, peretasan akun media sosial dan perbankan, penipuan daring, penyebaran malware, hingga pencurian data pribadi. Pelaku usaha, khususnya UMKM, menjadi salah satu kelompok yang rentan menjadi sasaran karena umumnya memiliki sistem keamanan digital yang terbatas (World Bank, 2023).

UMKM memiliki peran strategis dalam perekonomian nasional, baik sebagai penyerap tenaga kerja maupun sebagai penggerak ekonomi lokal. Di Indonesia, kontribusi UMKM terhadap Produk Domestik Bruto (PDB) dan penciptaan lapangan kerja sangat signifikan (Kementerian Koperasi dan UKM, 2022). Namun demikian, sebagian besar UMKM masih menghadapi kendala dalam hal literasi digital dan keamanan siber. Banyak pelaku usaha yang memanfaatkan platform digital tanpa pemahaman yang memadai terkait risiko keamanan data dan transaksi elektronik. Kondisi ini menjadikan UMKM sebagai target empuk kejahatan siber. Perkembangan teknologi terkini seperti *Artificial Intelligence* (AI) turut memperumit lanskap keamanan siber. AI pada dasarnya merupakan inovasi yang memberikan banyak manfaat, seperti otomatisasi layanan pelanggan, analisis perilaku konsumen, hingga optimalisasi pemasaran digital. Akan tetapi, teknologi ini juga dapat dimanfaatkan oleh pelaku kejahatan untuk menciptakan modus penipuan yang semakin canggih, seperti *deepfake*, serangan *automated phishing*, dan manipulasi data berbasis algoritma (OECD, 2023). Hal ini menuntut pelaku usaha untuk tidak hanya memahami penggunaan teknologi, tetapi juga menyadari potensi risiko yang menyertainya.

Rendahnya tingkat kesadaran terhadap keamanan digital menjadi faktor utama meningkatnya kasus *cybercrime* di kalangan pelaku usaha. Banyak pelaku UMKM yang masih mudah tergiur tawaran promosi peningkatan penjualan melalui tautan atau aplikasi tidak resmi. Selain itu, praktik penggunaan kata sandi yang lemah, tidak adanya autentikasi ganda, serta kurangnya pembaruan sistem keamanan menjadi celah yang sering dimanfaatkan oleh pelaku kejahatan (ENISA, 2022). Tanpa edukasi yang memadai, pelaku usaha berpotensi mengalami kerugian finansial, kehilangan data pelanggan, bahkan penurunan reputasi usaha. Kondisi tersebut menunjukkan bahwa permasalahan *cybercrime* bukan hanya persoalan teknis, melainkan juga persoalan literasi dan kesadaran kolektif. Upaya preventif melalui penyuluhan dan edukasi menjadi langkah strategis untuk meningkatkan pemahaman pelaku usaha terhadap

ancaman siber. Penyuluhan tidak hanya memberikan informasi mengenai jenis-jenis kejahatan siber, tetapi juga membekali pelaku usaha dengan keterampilan praktis dalam mengidentifikasi, menilai, dan mengantisipasi potensi ancaman (ITU, 2021). Edukasi keamanan siber yang berkelanjutan diyakini mampu mengurangi risiko kerugian akibat serangan digital.

Di tingkat lokal, tantangan yang dihadapi pelaku usaha sering kali diperparah oleh keterbatasan akses informasi dan pendampingan. Pelaku usaha di wilayah desa atau daerah berkembang umumnya belum mendapatkan pelatihan keamanan digital secara sistematis. Padahal, digitalisasi telah menjangkau hingga ke pelosok desa melalui penggunaan media sosial dan aplikasi pesan instan sebagai sarana promosi dan transaksi. Tanpa pendampingan yang tepat, pemanfaatan teknologi digital justru dapat meningkatkan risiko kerentanan terhadap kejahatan siber (UNDP, 2022). Penyuluhan dan edukasi menjadi pendekatan yang relevan dalam konteks pemberdayaan pelaku usaha di era digital. Kegiatan ini berfungsi sebagai media transfer pengetahuan sekaligus sarana membangun kesadaran kritis terhadap risiko digital. Melalui pendekatan partisipatif, pelaku usaha dapat berbagi pengalaman, mengidentifikasi permasalahan yang dihadapi, serta merumuskan langkah antisipatif secara bersama-sama. Pendekatan edukatif yang kontekstual terbukti efektif dalam meningkatkan perubahan perilaku dan kewaspadaan terhadap risiko keamanan (World Economic Forum, 2024).

Lebih jauh, penguatan literasi digital juga sejalan dengan agenda pembangunan nasional dalam menciptakan ekosistem ekonomi digital yang aman dan berkelanjutan. Pemerintah Indonesia telah mendorong transformasi digital UMKM melalui berbagai program, namun aspek keamanan siber masih perlu mendapat perhatian lebih serius. Tanpa perlindungan yang memadai, transformasi digital dapat menimbulkan kerentanan baru yang mengancam keberlanjutan usaha (Kominfo, 2023). Berdasarkan uraian tersebut, dapat dipahami bahwa tantangan *cybercrime* di era digital merupakan isu yang mendesak dan membutuhkan respons strategis. Pelaku usaha tidak hanya dituntut untuk adaptif terhadap perkembangan teknologi, tetapi juga harus memiliki kemampuan dalam mengelola risiko keamanan digital. Penyuluhan dan edukasi menjadi instrumen penting dalam membangun kapasitas pelaku usaha agar mampu menghadapi ancaman siber secara proaktif. Dengan demikian, kegiatan penyuluhan dan edukasi mengenai tantangan *cybercrime* bagi pelaku usaha menjadi relevan untuk dilaksanakan. Upaya ini diharapkan dapat meningkatkan kewaspadaan, memperkuat literasi digital, serta membantu pelaku usaha dalam mengidentifikasi, mencegah, dan menangani potensi ancaman siber.

BAHAN DAN METODE

Penelitian ini menggunakan pendekatan kualitatif dengan tujuan untuk memahami secara mendalam efektivitas kegiatan penyuluhan dan edukasi dalam meningkatkan kewaspadaan pelaku usaha terhadap ancaman *cybercrime* di era digital. Pendekatan kualitatif dipilih karena mampu menggali persepsi, pengalaman, dan respons pelaku usaha terhadap fenomena kejahatan siber secara kontekstual dan

komprehensif (Creswell & Poth, 2021). Dalam konteks ini, penelitian tidak hanya berfokus pada angka atau data statistik, tetapi lebih menekankan pada pemahaman proses, dinamika sosial, serta perubahan kesadaran yang terjadi setelah kegiatan penyuluhan dilaksanakan. Desain penelitian yang digunakan adalah studi kasus deskriptif. Studi kasus dipilih karena memungkinkan peneliti mengeksplorasi fenomena secara mendalam dalam konteks nyata, khususnya pada pelaku usaha yang menjadi sasaran kegiatan penyuluhan (Yin, 2022). Pendekatan ini relevan untuk menganalisis bagaimana pelaku usaha memahami ancaman *cybercrime*, bagaimana bentuk tantangan yang dihadapi, serta sejauh mana edukasi yang diberikan mampu meningkatkan literasi dan kewaspadaan digital mereka. Studi kasus juga memberikan ruang untuk mengidentifikasi faktor-faktor pendukung dan penghambat dalam pelaksanaan penyuluhan keamanan siber.

Subjek penelitian terdiri dari pelaku usaha mikro, kecil, dan menengah (UMKM) yang aktif menggunakan platform digital dalam kegiatan usahanya. Pemilihan informan dilakukan secara purposive sampling, yaitu berdasarkan pertimbangan bahwa responden memiliki pengalaman langsung dalam penggunaan teknologi digital untuk kegiatan usaha dan pernah menghadapi atau berpotensi menghadapi risiko kejahatan siber (Sugiyono, 2023). Selain pelaku usaha, penelitian ini juga melibatkan perangkat desa atau pihak terkait yang berperan dalam mendukung kegiatan penyuluhan sebagai informan tambahan untuk memperoleh perspektif yang lebih luas. Teknik pengumpulan data dilakukan melalui wawancara mendalam, observasi, dan dokumentasi. Wawancara mendalam dilakukan secara semi-terstruktur untuk memberikan ruang bagi informan dalam menjelaskan pengalaman, pemahaman, dan kekhawatiran mereka terkait ancaman *cybercrime*. Pertanyaan wawancara difokuskan pada bentuk ancaman yang pernah dialami, tingkat pemahaman tentang keamanan digital, kebiasaan penggunaan aplikasi dan media sosial, serta respons setelah mengikuti kegiatan penyuluhan. Teknik wawancara semi-terstruktur dinilai efektif dalam penelitian kualitatif karena memungkinkan eksplorasi data yang fleksibel namun tetap terarah (Moleong, 2021).

Observasi dilakukan selama kegiatan penyuluhan berlangsung untuk mengamati partisipasi, respons, serta interaksi peserta dalam sesi diskusi. Observasi ini bertujuan untuk melihat secara langsung tingkat antusiasme, pemahaman, dan perubahan sikap peserta terhadap isu keamanan siber. Observasi partisipatif terbatas memungkinkan peneliti memahami konteks sosial dan dinamika kelompok dalam proses edukasi (Patton, 2020). Melalui observasi, peneliti dapat mengidentifikasi indikator perubahan perilaku, seperti peningkatan kewaspadaan dalam membuka tautan, penggunaan kata sandi yang lebih kuat, atau kesadaran untuk tidak mengunduh aplikasi yang tidak jelas sumbernya. Dokumentasi juga menjadi bagian penting dalam penelitian ini. Dokumen yang dianalisis meliputi materi penyuluhan, daftar hadir peserta, catatan diskusi, serta laporan kegiatan. Analisis dokumentasi membantu memperkuat data hasil wawancara dan observasi, serta memberikan gambaran mengenai isi dan fokus materi edukasi yang disampaikan (Bowen, 2021). Dokumentasi ini juga berfungsi sebagai bukti pelaksanaan kegiatan dan dasar untuk melakukan evaluasi.

Analisis data dilakukan secara interaktif dan berkelanjutan menggunakan model analisis data kualitatif yang meliputi reduksi data, penyajian data, dan penarikan kesimpulan (Miles et al., 2020). Pada tahap reduksi data, peneliti menyaring informasi

yang relevan dengan fokus penelitian, seperti tingkat pemahaman awal tentang *cybercrime*, bentuk ancaman yang sering dialami, serta perubahan sikap setelah penyuluhan. Data yang telah direduksi kemudian disajikan dalam bentuk narasi deskriptif untuk memudahkan identifikasi pola dan tema utama. Tahap akhir adalah penarikan kesimpulan yang dilakukan secara bertahap dengan mempertimbangkan konsistensi data dari berbagai sumber. Untuk menjaga keabsahan data, penelitian ini menggunakan teknik triangulasi sumber dan triangulasi teknik. Triangulasi sumber dilakukan dengan membandingkan informasi dari pelaku usaha dan perangkat desa, sedangkan triangulasi teknik dilakukan dengan membandingkan hasil wawancara, observasi, dan dokumentasi (Lincoln & Guba, 2021). Selain itu, peneliti juga melakukan *member checking*, yaitu meminta konfirmasi kepada beberapa informan terkait hasil interpretasi data guna memastikan kesesuaian makna dan menghindari bias penafsiran (Nowell et al., 2022).

HASIL DAN PEMBAHASAN

Berdasarkan hasil wawancara mendalam, observasi selama kegiatan penyuluhan, serta analisis dokumentasi, ditemukan bahwa ancaman *cybercrime* terhadap pelaku usaha di era digital merupakan permasalahan nyata yang berdampak langsung pada keberlangsungan usaha. Transformasi digital yang semakin masif mendorong pelaku usaha memanfaatkan media sosial, aplikasi pesan instan, marketplace, dan layanan perbankan digital dalam aktivitas bisnis sehari-hari. Namun, pemanfaatan teknologi tersebut belum sepenuhnya diimbangi dengan pemahaman yang memadai mengenai keamanan siber. Kondisi ini sejalan dengan temuan bahwa percepatan digitalisasi tanpa penguatan literasi digital meningkatkan risiko serangan siber pada sektor usaha kecil (World Bank, 2023). Hasil penelitian menunjukkan bahwa sebagian besar pelaku usaha pernah menerima pesan mencurigakan berupa tautan promosi, pemberitahuan hadiah, atau notifikasi akun yang mengatasnamakan platform resmi. Beberapa di antaranya bahkan hampir menjadi korban *phishing* karena kurangnya pemahaman dalam memverifikasi keaslian pesan. Fenomena ini memperlihatkan bahwa pola kejahatan siber semakin adaptif dan memanfaatkan kelemahan psikologis korban, seperti rasa panik atau keinginan memperoleh keuntungan cepat (Interpol, 2022).

Tingkat Pemahaman dan Kerentanan Pelaku Usaha terhadap Cybercrime

Hasil penelitian menunjukkan bahwa tingkat pemahaman pelaku usaha mengenai *cybercrime* masih berada pada kategori dasar. Sebagian besar informan mengetahui istilah penipuan online, namun belum memahami secara spesifik berbagai bentuk serangan siber seperti *phishing*, *malware*, *ransomware*, atau rekayasa sosial (*social engineering*). Minimnya literasi ini membuat pelaku usaha lebih rentan terhadap berbagai modus kejahatan digital (ENISA, 2022). Banyak pelaku usaha menggunakan satu kata sandi untuk beberapa akun sekaligus dan belum menerapkan autentikasi dua faktor (*two-factor authentication*). Kebiasaan ini meningkatkan risiko peretasan akun bisnis, terutama pada platform media sosial dan marketplace. Temuan ini selaras

dengan laporan OECD (2023) yang menyebutkan bahwa usaha kecil cenderung memiliki sistem keamanan digital yang lemah karena keterbatasan pengetahuan dan sumber daya.

Selain itu, perkembangan teknologi seperti *Artificial Intelligence* (AI) turut memperumit lanskap ancaman siber. Beberapa informan mengaku pernah menerima pesan suara atau video yang tampak meyakinkan, padahal berpotensi merupakan hasil manipulasi berbasis AI (*deepfake*). Modus ini menunjukkan bahwa teknologi canggih tidak hanya dimanfaatkan untuk inovasi bisnis, tetapi juga untuk melakukan penipuan yang lebih kompleks (World Economic Forum, 2024). Kerentanan pelaku usaha juga dipengaruhi oleh rendahnya kesadaran terhadap pentingnya perlindungan data pelanggan. Sebagian besar pelaku usaha belum memahami bahwa kebocoran data dapat berdampak pada hilangnya kepercayaan konsumen dan reputasi usaha. Padahal, keamanan data menjadi aspek krusial dalam membangun ekosistem ekonomi digital yang berkelanjutan (UNCTAD, 2021). Dengan demikian, hasil penelitian pada subpembahasan ini menunjukkan bahwa tantangan utama yang dihadapi pelaku usaha bukan hanya pada aspek teknis, tetapi juga pada aspek kesadaran dan literasi digital yang masih terbatas.

Efektivitas Penyuluhan dan Edukasi dalam Meningkatkan Literasi Keamanan Digital

Kegiatan penyuluhan dan edukasi yang dilaksanakan menunjukkan dampak positif terhadap peningkatan pemahaman pelaku usaha. Berdasarkan observasi dan hasil wawancara pasca-kegiatan, sebagian besar peserta mengaku lebih memahami jenis-jenis ancaman siber dan langkah-langkah pencegahannya. Penyampaian materi secara interaktif dan berbasis studi kasus nyata membantu peserta memahami risiko secara konkret (ITU, 2021). Materi penyuluhan mencakup pengenalan modus *phishing*, cara mengenali tautan mencurigakan, pentingnya penggunaan kata sandi yang kuat, serta penerapan autentikasi ganda. Selain itu, peserta juga diberikan simulasi sederhana untuk mengidentifikasi email atau pesan yang berpotensi sebagai penipuan. Pendekatan partisipatif ini terbukti efektif dalam meningkatkan keterlibatan dan pemahaman peserta (UNDP, 2022).

Setelah mengikuti penyuluhan, beberapa pelaku usaha langsung mengganti kata sandi akun bisnis mereka dan mulai mengaktifkan fitur keamanan tambahan. Perubahan perilaku ini menunjukkan bahwa edukasi yang tepat dapat memengaruhi kesadaran dan tindakan preventif secara langsung. Hal ini sejalan dengan temuan bahwa pelatihan keamanan siber yang kontekstual mampu meningkatkan kesiapsiagaan pelaku usaha kecil terhadap ancaman digital (Kominfo, 2023). Namun demikian, tantangan yang masih dihadapi adalah keberlanjutan edukasi. Penyuluhan satu kali belum cukup untuk membentuk kebiasaan keamanan digital secara permanen. Oleh karena itu, diperlukan program pendampingan berkelanjutan agar literasi digital dapat terus ditingkatkan seiring perkembangan modus kejahatan siber yang dinamis (OECD, 2023). Dengan demikian, dapat disimpulkan bahwa penyuluhan dan edukasi memiliki peran signifikan dalam meningkatkan literasi keamanan digital, meskipun perlu didukung oleh program lanjutan yang lebih sistematis.

Strategi Antisipatif dan Penguatan Ketahanan Digital Pelaku Usaha

Berdasarkan hasil penelitian, penguatan ketahanan digital pelaku usaha memerlukan strategi yang terintegrasi antara edukasi, kebijakan lokal, dan dukungan teknologi. Salah satu langkah utama adalah membangun budaya keamanan digital di tingkat komunitas usaha. Kesadaran kolektif akan pentingnya keamanan siber dapat mengurangi risiko serangan yang memanfaatkan kelengahan individu (World Bank, 2023). Pelaku usaha juga disarankan untuk menggunakan perangkat lunak resmi dan rutin memperbarui sistem keamanan. Penggunaan aplikasi bajakan atau tidak resmi berpotensi membawa malware yang dapat mencuri data usaha. Selain itu, penerapan pencadangan data (*backup*) secara berkala menjadi langkah preventif untuk mengantisipasi serangan *ransomware* (ENISA, 2022).

Peran perangkat desa atau pemerintah lokal juga penting dalam mendukung ketahanan digital pelaku usaha. Dukungan dapat berupa penyediaan pelatihan rutin, penyebaran informasi terkait modus terbaru *cybercrime*, serta kerja sama dengan lembaga terkait dalam membangun sistem keamanan digital berbasis komunitas (UNDP, 2022). Di sisi lain, pemanfaatan AI secara bijak juga perlu ditekankan. Pelaku usaha dapat menggunakan teknologi AI untuk meningkatkan efisiensi pemasaran dan pelayanan pelanggan, namun tetap harus memahami potensi penyalahgunaannya. Edukasi mengenai etika dan keamanan penggunaan AI menjadi bagian penting dalam membangun ketahanan digital jangka panjang (World Economic Forum, 2024). Secara keseluruhan, strategi antisipatif yang efektif mencakup peningkatan literasi digital, penerapan standar keamanan dasar, kolaborasi antar pelaku usaha, serta dukungan kebijakan yang berkelanjutan. Ketahanan digital bukan hanya tanggung jawab individu, tetapi juga tanggung jawab kolektif dalam ekosistem ekonomi digital.

SIMPULAN

Berdasarkan hasil penelitian dan pembahasan, dapat disimpulkan bahwa tantangan *cybercrime* di era digital merupakan ancaman nyata bagi pelaku usaha, khususnya UMKM yang активно memanfaatkan teknologi digital dalam aktivitas bisnisnya. Perkembangan teknologi, termasuk pemanfaatan *Artificial Intelligence* (AI), di satu sisi memberikan peluang inovasi dan efisiensi, namun di sisi lain juga meningkatkan kompleksitas modus kejahatan siber seperti *phishing*, peretasan, manipulasi data, dan penipuan digital. Rendahnya literasi keamanan siber dan keterbatasan pemahaman teknis menjadi faktor utama yang menyebabkan pelaku usaha berada pada posisi rentan terhadap serangan digital. Kegiatan penyuluhan dan edukasi yang dilaksanakan terbukti memberikan dampak positif dalam meningkatkan kesadaran dan pemahaman pelaku usaha terhadap ancaman *cybercrime*. Melalui pendekatan partisipatif dan berbasis studi kasus, pelaku usaha mampu mengenali bentuk-bentuk serangan siber serta memahami langkah-langkah preventif, seperti penggunaan kata sandi yang kuat, aktivasi autentikasi ganda, kehati-hatian dalam mengakses tautan, serta penggunaan perangkat lunak resmi. Perubahan perilaku awal yang ditunjukkan peserta setelah penyuluhan menjadi indikator bahwa edukasi

keamanan digital merupakan strategi efektif dalam membangun kewaspadaan. Namun demikian, peningkatan literasi digital tidak dapat dilakukan secara instan dan satu kali kegiatan. Diperlukan pendampingan berkelanjutan, dukungan kebijakan lokal, serta kolaborasi antara pelaku usaha dan pemangku kepentingan untuk membangun ketahanan digital yang lebih kuat. Dengan penguatan edukasi, kesadaran kolektif, dan penerapan praktik keamanan siber yang konsisten, pelaku usaha diharapkan mampu menghadapi tantangan *cybercrime* secara proaktif serta menjaga keberlanjutan usahanya di tengah dinamika transformasi digital yang terus berkembang.

Ucapan Terimakasih

Penulis mengucapkan terima kasih kepada Universitas Siber Asia Jakarta atas dukungan, sehingga seluruh rangkaian kegiatan dapat berjalan secara efektif dan memberikan manfaat bagi penguatan pendidikan.

REFERENSI

Bowen, G. A. (2021). Document analysis as a qualitative research method. *Qualitative Research Journal, 21*(3), 27–40.

Creswell, J. W., & Poth, C. N. (2021). *Qualitative inquiry and research design: Choosing among five approaches* (4th ed.). Sage Publications.

ENISA. (2022). *ENISA threat landscape 2022*. European Union Agency for Cybersecurity.

Interpol. (2022). *Global crime trend report 2022: Cybercrime and digital threats*. INTERPOL.

ITU. (2021). *Global cybersecurity outlook 2021*. International Telecommunication Union.

Kementerian Koperasi dan UKM Republik Indonesia. (2022). *Perkembangan data usaha mikro, kecil, dan menengah (UMKM) tahun 2022*. KemenKop UKM RI.

Kominfo. (2023). *Laporan literasi digital Indonesia 2023*. Kementerian Komunikasi dan Informatika Republik Indonesia.

Lincoln, Y. S., & Guba, E. G. (2021). *Naturalistic inquiry* (Updated ed.). Sage Publications.

Miles, M. B., Huberman, A. M., & Saldaña, J. (2020). *Qualitative data analysis: A methods sourcebook* (4th ed.). Sage Publications.

Moleong, L. J. (2021). *Metodologi penelitian kualitatif* (Edisi revisi). PT Remaja Rosdakarya.

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2022). Thematic analysis: Striving to meet the trustworthiness criteria. *International Journal of Qualitative Methods, 21*, 1–13.

OECD. (2023). *Digital security risk management: OECD digital economy outlook 2023*. OECD Publishing.

UNCTAD. (2021). *Digital economy report 2021: Cross-border data flows and development*.

United Nations Publications.

UNDP. (2022). *Digital transformation and inclusive development report 2022*. United Nations Development Programme.

World Bank. (2023). *World development report 2023: Digital transformation and development*. World Bank Publications.

World Economic Forum. (2024). *Global cybersecurity outlook 2024*. World Economic Forum.

Yin, R. K. (2022). *Case study research and applications: Design and methods* (6th ed.). Sage Publications.