

PELATIHAN LITERASI DIGITAL DAN KEAMANAN DATA BAGI UMKM DI ERA TRANSFORMASI DIGITAL

**Doni Gunawan¹, M. Bayu Wibawa², Mahendar Dwi Payana³, Ayu Helinda⁴,
Mirza Purnandi⁵, Maulidin⁶**

Universitas Ubudiyah Indonesia, Jalan Alue Naga Tibang Kecamatan Syiah Kuala, Banda Aceh
Korespondensi: doni@uui.ac.id

Abstrak

Transformasi digital di sektor UMKM mendorong peningkatan pemanfaatan teknologi, namun belum diiringi dengan kesadaran akan pentingnya keamanan siber. Kegiatan pengabdian masyarakat ini bertujuan untuk meningkatkan literasi dan keterampilan dasar keamanan siber pelaku UMKM di Banda Aceh melalui pelatihan partisipatif berbasis praktik. Materi yang diberikan meliputi ancaman siber seperti phishing, malware, dan social engineering serta praktik dasar keamanan digital seperti penggunaan kata sandi yang kuat, autentikasi dua faktor, dan pengelolaan identitas digital. Kegiatan dilaksanakan selama dua hari di Aula Kecamatan Ulee Kareng dengan 30 peserta dari berbagai sektor UMKM. Evaluasi pre-test dan post-test menunjukkan peningkatan pemahaman sebesar rata-rata 35%, dan peserta menunjukkan keterampilan dasar dalam melindungi sistem digital usaha mereka. Kegiatan ini membuktikan efektivitas pendekatan partisipatif dalam meningkatkan literasi keamanan siber dan mendorong terbentuknya komunitas UMKM digital yang lebih tangguh.

Kata kunci: keamanan siber, UMKM, literasi digital, edukasi, transformasi digital

Abstract

Digital transformation in the MSME sector has increased technology usage but is not always accompanied by cybersecurity awareness. This community service aimed to enhance basic cybersecurity literacy and skills among MSME actors in Banda Aceh through a participatory and practical training model. Topics included threats such as phishing, malware, and social engineering, and practical safeguards like strong passwords, two-factor authentication, and digital identity management. The training was held over two days at Ulee Kareng District Hall with 30 participants from various MSME sectors. Evaluation through pre-test and post-test revealed a 35% average improvement in understanding, with participants demonstrating basic skills in protecting their business digital systems. This activity proves the effectiveness of participatory approaches in increasing cybersecurity awareness and fostering more resilient digital MSME communities.

Keywords: cybersecurity, MSMEs, digital literacy, education, digital transformation

PENDAHULUAN

Perkembangan digitalisasi bisnis UMKM menawarkan kemudahan dalam transaksi dan pemasaran daring, namun juga membawa ancaman keamanan siber yang semakin kompleks. Ketiadaan pemahaman tentang keamanan digital menjadikan pelaku UMKM rentan terhadap pencurian data, peretasan akun, hingga penipuan online. Kementerian Kominfo (2020) mencatat bahwa 88% UMKM belum memiliki kesiapan dalam menghadapi ancaman siber. Pemberdayaan pelaku UMKM melalui edukasi keamanan siber sangat penting untuk mendukung keberlangsungan usaha mereka di era digital. Universitas Ubudiyah Indonesia melalui program pengabdian ini menghadirkan pelatihan yang dirancang dengan pendekatan edukatif dan partisipatif agar peserta dapat memahami dan mempraktikkan langkah-langkah dasar perlindungan digital secara langsung.

Kegiatan usaha kecil dan menengah (UMKM) merupakan tulang punggung perekonomian Indonesia. Di era transformasi digital, UMKM menjadi semakin bergantung pada teknologi informasi untuk mendukung operasional bisnis, mulai dari pemasaran hingga sistem pembayaran. Namun demikian, pertumbuhan digitalisasi ini tidak diiringi dengan pemahaman yang memadai tentang pentingnya keamanan data dan perlindungan informasi digital. Kondisi ini menyebabkan pelaku UMKM sangat rentan terhadap berbagai bentuk ancaman siber seperti penipuan online, peretasan akun bisnis, hingga pencurian data konsumen. Serangan siber yang sebelumnya banyak menasar perusahaan besar kini juga menargetkan usaha skala kecil karena sistem keamanannya yang lemah dan kurangnya edukasi teknis.

Beberapa studi menyebutkan bahwa sebagian besar UMKM tidak menggunakan kata sandi yang kuat dan sering mengabaikan pentingnya pencadangan data. Mereka juga belum familiar dengan metode perlindungan seperti autentikasi dua faktor

atau penggunaan perangkat lunak antivirus yang legal dan mutakhir. Kelemahan dalam keamanan digital ini tidak hanya berisiko terhadap kerugian finansial, tetapi juga dapat berdampak pada reputasi bisnis dan kepercayaan pelanggan. Oleh karena itu, peningkatan literasi digital dengan fokus pada keamanan siber menjadi kebutuhan mendesak, khususnya dalam ekosistem UMKM yang berkembang pesat.

Pemerintah melalui Kementerian Komunikasi dan Informatika telah mendorong peningkatan kapasitas digital UMKM melalui berbagai inisiatif. Namun, pelaksanaan di lapangan sering kali terbatas pada pelatihan umum tanpa menyentuh aspek krusial seperti keamanan siber secara mendalam. Dalam konteks ini, perguruan tinggi memiliki peran strategis untuk menjembatani kesenjangan pengetahuan melalui program pengabdian masyarakat. Kegiatan pelatihan berbasis praktik yang dilakukan oleh dosen dan mahasiswa dapat menjadi pendekatan efektif dalam menyampaikan konsep-konsep teknis secara sederhana dan aplikatif.

Universitas Ubudiyah Indonesia merespons kebutuhan ini dengan menyelenggarakan pelatihan keamanan siber dasar bagi pelaku UMKM di Banda Aceh. Program ini dirancang tidak hanya sebagai transfer ilmu, tetapi juga sebagai upaya kolaboratif untuk membentuk komunitas usaha yang sadar digital dan tangguh menghadapi risiko siber. Pelatihan ini menggunakan pendekatan edukatif-partisipatif dengan materi yang relevan dan langsung diterapkan dalam praktik usaha peserta. Diharapkan kegiatan ini dapat menjadi model edukasi keamanan digital yang replikatif dan berkelanjutan, serta menjadi bagian dari agenda strategis pemberdayaan UMKM secara nasional.

METODE

Pelatihan dilaksanakan pada 1 Oktober 2022, di Aula Kecamatan Ulee Kareng, Banda Aceh. Peserta merupakan 30 pelaku UMKM dari sektor kuliner, kerajinan, dan jasa digital yang aktif menggunakan teknologi namun memiliki pemahaman terbatas tentang

keamanan siber. Pelatihan ini menggunakan pendekatan edukatif dan partisipatif yang menekankan pada interaksi aktif antara narasumber dan peserta pelatihan. Pendekatan edukatif diwujudkan dalam bentuk penyampaian materi yang sistematis dan disesuaikan dengan kebutuhan pelaku UMKM yang sebagian besar berasal dari latar belakang non-teknis.

Sementara itu, pendekatan partisipatif difokuskan pada keterlibatan peserta melalui diskusi kelompok, simulasi kasus, dan praktik langsung dalam mengamankan akun dan data bisnis. Kegiatan dilaksanakan secara luring (tatap muka) selama dua hari, yakni pada tanggal 5 dan 6 Agustus 2022, bertempat di Aula Kantor Kecamatan Ulee Kareng, Banda Aceh. Pemilihan lokasi ini mempertimbangkan aksesibilitas bagi peserta yang merupakan pelaku UMKM di sekitar wilayah kota. Jadwal kegiatan berlangsung dari pukul 09.00 hingga 15.00 WIB setiap harinya, dengan pembagian waktu untuk sesi materi, praktik, diskusi, serta evaluasi.

Sasaran dari kegiatan ini adalah 30 pelaku UMKM aktif yang telah menggunakan media sosial atau platform digital dalam menjalankan bisnisnya, namun belum memiliki pemahaman yang cukup terkait keamanan digital. Peserta berasal dari berbagai sektor seperti kuliner, kerajinan tangan, fashion, dan jasa layanan berbasis daring. Partisipasi mereka diperoleh melalui koordinasi dengan Dinas Koperasi dan Komunitas UMKM Digital setempat. Materi pelatihan mencakup empat topik utama yaitu: (1) Pengenalan ancaman siber yang umum terjadi, seperti phishing, malware, ransomware, dan social engineering; (2) Praktik penggunaan kata sandi yang kuat dan manajemen akun; (3) Pengelolaan data dan privasi konsumen, termasuk pentingnya pencadangan data (backup); serta (4) Simulasi serangan dan studi kasus yang relevan dengan keseharian pelaku UMKM.

Metode penyampaian menggunakan kombinasi ceramah interaktif dengan media presentasi, studi kasus, serta simulasi praktik langsung. Dalam sesi simulasi, peserta diberi

latihan untuk mengidentifikasi email phishing, membuat password yang kuat, dan mengaktifkan autentikasi dua faktor pada akun bisnis mereka. Peserta juga diajak untuk menganalisis serangan digital sederhana dan menyusun rencana tindakan preventif. Untuk mengukur efektivitas pelatihan, dilakukan evaluasi berupa pre-test dan post-test guna menilai perubahan pemahaman peserta. Selain itu, tim pelaksana juga melakukan observasi keterlibatan peserta dan wawancara singkat untuk menangkap respon, kebutuhan lanjutan, serta potensi pengembangan kegiatan serupa ke depannya. Data yang diperoleh kemudian dianalisis secara deskriptif untuk menghasilkan laporan dampak kegiatan secara komprehensif.

HASIL PELAKSANAAN KEGIATAN DAN PEMBAHASAN

Keserta menunjukkan peningkatan signifikan dalam pemahaman keamanan siber, dengan rata-rata peningkatan skor sebesar 35%. Peserta yang sebelumnya tidak mengenal phishing atau tidak menggunakan password kuat, kini mampu menerapkan praktik keamanan dasar. Dalam simulasi, sebagian peserta langsung mengamankan akun bisnis mereka. Peserta juga aktif dalam diskusi dan menyatakan bahwa materi mudah dipahami karena disampaikan dengan pendekatan visual dan konteks lokal. Grup WhatsApp pascapelatihan terus aktif digunakan sebagai wadah konsultasi dan berbagi informasi.

1. Penyampaian Materi Teoritis – peserta diberikan pemahaman dasar mengenai ancaman siber seperti phishing, malware, ransomware, social engineering, serta kebiasaan digital yang rawan risiko.
2. Simulasi Kasus – peserta diminta mengidentifikasi contoh email phishing, membuat password yang aman, dan mengaktifkan autentikasi dua faktor.
3. Praktik Langsung – peserta mempraktikkan pengamanan akun bisnis mereka, serta cara backup data dan mengelola informasi pelanggan secara aman.
4. Diskusi Kelompok – peserta berbagi

pengalaman terkait kejadian siber yang pernah dialami serta cara penanganannya.

5. Evaluasi – melalui pre-test dan post-test serta umpan balik kualitatif.

Dari hasil pre-test, mayoritas peserta menunjukkan tingkat pemahaman rendah; 70% peserta belum pernah mendengar istilah *phishing* dan tidak menggunakan autentikasi dua faktor. Setelah pelatihan, hasil post-test menunjukkan rata-rata peningkatan skor pemahaman sebesar 35%. Sebanyak 85% peserta mengalami peningkatan nilai lebih dari 30%, dan lebih dari 90% peserta dapat membuat password kuat dan mengenali tanda-tanda email palsu. Selain hasil tes, pengamatan lapangan menunjukkan antusiasme tinggi peserta dalam sesi praktik. Beberapa peserta langsung mengamankan akun marketplace mereka, mengaktifkan fitur keamanan tambahan, dan membagikan pengalaman digital mereka selama sesi diskusi. Peserta juga sangat terbantu dengan modul pelatihan visual dan penggunaan bahasa non-teknis (Astuti & Mulyani, 2019).

Program ini juga berhasil membangun jejaring digital berkelanjutan. Grup WhatsApp yang dibuat pasca pelatihan terus digunakan sebagai forum konsultasi, tanya-jawab, serta berbagi tips keamanan digital. Hal ini menunjukkan bahwa dampak kegiatan tidak hanya berhenti pada dua hari pelatihan, tetapi berlanjut sebagai proses pembelajaran kolektif (Kolb, 2015).

Pelaksanaan pelatihan ini mengungkap bahwa kesadaran keamanan siber di kalangan UMKM masih tergolong rendah, meskipun mereka sudah aktif menggunakan perangkat digital untuk menjalankan bisnis. Minimnya pengetahuan dasar membuat UMKM rentan terhadap serangan digital seperti pencurian data, peretasan akun, dan penipuan online. Namun, hasil pelatihan ini membuktikan bahwa dengan pendekatan yang tepat dan penyampaian yang sederhana, pelaku UMKM dapat memahami dan menerapkan prinsip-prinsip keamanan digital dasar. Simulasi dan praktik langsung terbukti menjadi metode yang efektif untuk membantu peserta memahami konsep yang

sebelumnya dianggap teknis atau sulit. Kegiatan ini juga menunjukkan pentingnya dukungan edukatif berkelanjutan.

Banyak peserta menyatakan bahwa mereka berharap ada pelatihan lanjutan dengan topik-topik seperti keamanan transaksi digital, perlindungan data pelanggan, dan manajemen risiko digital. Ini menjadi masukan penting bagi penyelenggara dan institusi pendidikan untuk merancang program pembinaan berkelanjutan bagi UMKM. Dari sisi kebermanfaatan, pelatihan ini tidak hanya meningkatkan kapasitas peserta, tetapi juga mendorong terbentuknya komunitas pembelajar digital di kalangan UMKM. Grup WhatsApp yang dibuat selama pelatihan terus aktif digunakan peserta untuk berbagi informasi, bertanya seputar keamanan digital, dan berbagi peluang pelatihan lainnya.

Secara keseluruhan, kegiatan ini memberikan dampak positif dalam memperkuat literasi digital dan ketahanan siber pelaku UMKM, yang pada akhirnya akan meningkatkan keberlanjutan dan kepercayaan pelanggan terhadap bisnis mereka di era digital. Kegiatan pelatihan ini menunjukkan bahwa kesadaran terhadap keamanan siber belum menjadi prioritas utama bagi pelaku UMKM. Banyak peserta yang mengakui bahwa mereka lebih fokus pada aspek promosi dan penjualan, sementara aspek perlindungan data serta keamanan transaksi belum menjadi perhatian khusus. Hal ini tentu berisiko terhadap keberlangsungan usaha mereka, apalagi di era digital yang penuh dengan ancaman siber. Dalam konteks ini, pelatihan berhasil membangun kesadaran baru bahwa keamanan siber adalah bagian integral dari digitalisasi usaha. Melalui contoh kasus dan simulasi nyata, peserta memahami bahwa serangan siber tidak hanya terjadi pada perusahaan besar, tetapi juga dapat menasar UMKM melalui metode sederhana seperti tautan phishing atau pencurian akun media sosial. Hal ini menjadi titik balik penting dalam cara pandang mereka terhadap teknologi. Kegiatan ini juga memberikan gambaran bahwa pemberdayaan digital bagi UMKM tidak cukup hanya dengan pelatihan pemasaran atau e-commerce, tetapi juga harus

mencakup penguatan kapasitas perlindungan data dan sistem informasi. Keamanan siber merupakan komponen penting dari transformasi digital UMKM, yang dapat meningkatkan kepercayaan pelanggan dan menjaga reputasi usaha.

Keberhasilan pelatihan ini turut didukung oleh metode penyampaian yang menggunakan pendekatan partisipatif dan kontekstual. Penggunaan studi kasus lokal dan pengalaman nyata para pelaku usaha membuat peserta merasa lebih dekat dan relevan dengan materi yang disampaikan. Ini memperkuat pentingnya penyusunan modul pelatihan yang menyesuaikan dengan latar belakang audiensi. Lebih lanjut, kegiatan ini membuka peluang terbentuknya jejaring pendampingan digital berkelanjutan antara dosen, mahasiswa, dan komunitas UMKM. Adanya grup komunikasi pascapelatihan yang aktif menunjukkan bahwa peserta membutuhkan ruang diskusi dan konsultasi lebih lanjut. Ke depan, universitas dan pemerintah daerah dapat berperan sebagai fasilitator bagi terbentuknya sistem pendampingan ini dalam rangka meningkatkan ketahanan digital sektor UMKM secara menyeluruh.

Selain meningkatkan pengetahuan peserta, pelatihan ini juga memberikan efek psikologis yang positif, yakni menumbuhkan rasa percaya diri dalam menggunakan teknologi secara lebih aman. Sebelumnya, beberapa peserta merasa ragu dalam menggunakan fitur digital tertentu karena takut menjadi korban penipuan online. Setelah mengikuti pelatihan, mereka merasa lebih siap dan berani untuk memanfaatkan teknologi dengan tetap memperhatikan aspek keamanan. Dari hasil diskusi kelompok, diketahui pula bahwa pelaku UMKM sangat membutuhkan informasi yang terus diperbarui seiring perkembangan modus kejahatan digital. Banyak di antara mereka yang belum mengetahui bahwa bentuk serangan seperti social engineering dan scam berbasis aplikasi kini semakin canggih. Hal ini menunjukkan pentingnya pelatihan berkelanjutan serta akses informasi yang

mudah dijangkau dalam bahasa yang sederhana dan non-teknis.

Pelatihan ini juga menunjukkan bahwa sinergi antara akademisi dan pelaku UMKM memiliki dampak yang kuat dalam penguatan kapasitas digital masyarakat. Melalui keterlibatan langsung dosen dan mahasiswa dalam proses edukasi, terjadi transfer pengetahuan yang tidak hanya satu arah, tetapi juga memperkaya pengalaman kedua belah pihak. UMKM mendapatkan ilmu praktis, sementara akademisi memperoleh wawasan nyata tentang tantangan lapangan. Dalam konteks keberlanjutan program, hasil pelatihan ini dapat menjadi bahan evaluasi dan dasar pengembangan modul pelatihan keamanan siber tahap lanjut. Materi lanjutan dapat meliputi keamanan transaksi digital berbasis QR code, pengelolaan data pelanggan, pengamanan akun toko online, hingga dasar-dasar regulasi perlindungan data pribadi (UU PDP). Modul lanjutan ini penting untuk meningkatkan resiliensi UMKM terhadap ancaman digital yang semakin kompleks.

Akhirnya, keberhasilan kegiatan ini menunjukkan bahwa peningkatan literasi keamanan digital merupakan investasi strategis dalam membangun ekosistem UMKM yang tangguh di era digital. Pelatihan seperti ini harus menjadi agenda rutin dan terstruktur oleh pemerintah daerah, perguruan tinggi, dan komunitas digital. Dengan kolaborasi lintas sektor, transformasi digital UMKM dapat berlangsung secara inklusif, aman, dan berkelanjutan.

KESIMPULAN

Kegiatan edukasi dan pelatihan keamanan siber dasar bagi UMKM di era digital ini telah dilaksanakan dengan lancar dan mencapai hasil yang positif. Pelatihan ini berhasil meningkatkan pemahaman dan kesadaran pelaku UMKM tentang pentingnya perlindungan data dan keamanan aktivitas digital dalam menjalankan usaha. Melalui metode interaktif dan praktik langsung, peserta mampu mengidentifikasi risiko digital, membuat sistem keamanan sederhana, serta menerapkan langkah-langkah pengamanan

pada akun bisnis dan perangkat digital mereka. Hasil pre-test dan post-test menunjukkan peningkatan signifikan dalam pengetahuan peserta, yang mengindikasikan bahwa pendekatan pembelajaran yang digunakan sudah efektif. Peserta juga menyatakan kepuasan terhadap materi yang disampaikan karena relevan dengan kebutuhan mereka sehari-hari.

Antusiasme tinggi dari peserta mencerminkan pentingnya pelatihan serupa diadakan secara berkelanjutan. Kegiatan ini tidak hanya berdampak pada aspek pengetahuan teknis, tetapi juga membuka kesadaran peserta bahwa keamanan digital merupakan bagian penting dari transformasi UMKM menuju era digital yang lebih profesional dan aman

DAFTAR PUSTAKA

- Astuti, R., & Mulyani, S. (2019). Model pembelajaran berbasis aktivitas untuk meningkatkan partisipasi siswa. *Jurnal Pendidikan Interaktif*, 5(1), 24–33.
- Badan Ketahanan Pangan. (2023). *Laporan tahunan ketahanan pangan nasional 2022*. Kementerian Pertanian Republik Indonesia.
- Dewey, J. (1938). *Experience and education*. Macmillan.
- FAO. (2021). *The State of Food Security and Nutrition in the World 2021*. Food and Agriculture Organization.
- Ismail, R. (2022). Integrasi pangan lokal dan pendidikan karakter melalui pertanian berkelanjutan di Aceh. *Jurnal Pangan dan Sosial*, 10(2), 145–158.
- Kolb, D. A. (2015). *Experiential learning: Experience as the source of learning and development* (2nd ed.). Pearson Education.
- Kolb, D. A. (2015). *Experiential learning: Experience as the source of learning and development* (2nd ed.). Pearson Education.
- Lestari, R., & Suryani, A. (2020). Membangun kesadaran pangan melalui pendidikan berbasis proyek. *Jurnal Ketahanan Pangan Indonesia*, 8(2), 100–112.
- Nasution, T., & Rachmawati, E. (2021). Persepsi generasi muda terhadap ketahanan pangan di era globalisasi. *Jurnal Ketahanan Nasional*, 27(1), 55–70.
- Nugroho, H., Prasetyo, Y., & Wardani, T. (2021). Pembelajaran berbasis pengalaman untuk menumbuhkan perilaku konsumsi berkelanjutan. *Jurnal Pendidikan Berkelanjutan*, 3(1), 33–45.
- Trilling, B., & Fadel, C. (2009). *21st century skills: Learning for life in our times*. Jossey-Bass.
- WFP. (2020). *Global report on food crises*. World Food Programme.

DOKUMENTASI KEGIATAN

