HIKMAYO Jurnal Pengabdian Masyarakat
Volume 4. Nomor 2. Oktober 2025 Hal 30– 46
http://jurnal.amayogyakarta.ac.id/index.php/HIKMAYO

PENDAMPINGAN LITERASI KEAMANAN SIBER BAGI UMKM DI DAERAH ISTIMEWA YOGYAKARTA

Denies Priantinah[1], Abdullah Taman[2], Dian Juliani[3]
[1,2,3]Program Studi Akuntansi, Departemen Pendidikan Akuntansi, Fakultas Ekonomi dan Bisnis, Universitas Negeri Yogyakarta
Email: denies_priantinah@uny.ac.id*

ABSTRACT

Digital transformation opens up great opportunities for Micro, Small, and Medium Enterprises (MSMEs), but on the other hand, it increases the risk of cybercrime. This community service activity aims to increase cybersecurity awareness among MSMEs in the Special Region of Yogyakarta through an educational and participatory approach. The implementation method consists of four stages, namely socialization of cybersecurity literacy, training on digital security tools (antivirus, firewall, VPN), simulation of attacks and secure transactions, and assistance in implementing digital security practices. The activity was attended by 42 MSME players from the culinary, fashion, and digital creative services sectors. The evaluation results showed a significant increase in the participants' knowledge level, with an average pre-test score of 3.14 increasing to 4.54 on the post-test (Likert scale 1–5), or a 45% increase in digital security awareness. A total of 79% of participants were women, and 61.9% were from the culinary sector, indicating the dominance of women entrepreneurs in the adoption of cyber literacy. Participants also reported an increase in confidence in managing secure digital transactions, especially on the WhatsApp platform, which was used by 73.8% of participants. This activity proved to be effective in strengthening the digital resilience of MSMEs through practical, application-based training. Going forward, it is recommended that tiered training programs be developed in collaboration with technology institutions and that continuous monitoring be conducted to maintain the sustainability of digital security practices among MSMEs.

***Keywords**: cybersecurity awareness, digital literacy, MSMEs, digital transactions.*

ABSTRAK

Transformasi digital membuka peluang besar bagi pelaku Usaha Mikro, Kecil, dan Menengah (UMKM), namun di sisi lain meningkatkan risiko terhadap kejahatan siber. Kegiatan pengabdian kepada masyarakat ini bertujuan untuk meningkatkan *cybersecurity awareness* pelaku UMKM di Daerah Istimewa Yogyakarta melalui pendekatan edukatif dan partisipatif. Metode pelaksanaan mencakup empat tahap, yaitu sosialisasi literasi keamanan siber, pelatihan perangkat keamanan digital (antivirus, firewall, VPN), simulasi serangan dan transaksi aman,

HIKMAYO Jurnal Pengabdian Masyarakat
Volume 4. Nomor 2. Oktober 2025 Hal 30– 46
http://jurnal.amayogyakarta.ac.id/index.php/HIKMAYO

serta pendampingan penerapan praktik keamanan digital. Kegiatan diikuti oleh 42 pelaku UMKM dari sektor kuliner, fesyen, dan jasa kreatif digital. Hasil evaluasi menunjukkan peningkatan signifikan dalam tingkat pengetahuan peserta, dengan skor rata-rata pre-test sebesar 3,14 meningkat menjadi 4,54 pada post-test (skala Likert 1–5), atau peningkatan 45% dalam kesadaran keamanan digital. Sebanyak 79% peserta merupakan perempuan, dan 61,9% berasal dari sektor kuliner, yang menunjukkan dominasi pelaku usaha perempuan dalam adopsi literasi siber. Peserta juga melaporkan peningkatan kepercayaan diri dalam mengelola transaksi digital secara aman, terutama pada platform WhatsApp yang digunakan oleh 73,8% peserta. Kegiatan ini terbukti efektif dalam memperkuat ketahanan digital UMKM melalui pelatihan aplikatif berbasis praktik. Ke depan, disarankan pengembangan program pelatihan berjenjang dengan kolaborasi lembaga teknologi dan monitoring berkelanjutan untuk menjaga keberlanjutan praktik keamanan digital di kalangan UMKM.
Kata kunci: *cybersecurity awareness*, literasi digital, UMKM, transaksi digital.

I. PENDAHULUAN

Dalam era digital yang terus berkembang pesat, penggunaan teknologi informasi dan internet telah menjadi bagian tak terpisahkan dari kehidupan sehari-hari manusia di seluruh dunia. Perkembangan teknologi informasi dan komunikasi (TIK) telah merevolusi cara individu, organisasi, dan pelaku usaha berinteraksi, bertransaksi, serta menjalankan aktivitas ekonomi. Era digital ditandai oleh integrasi teknologi seperti *cloud computing*, kecerdasan buatan (*artificial intelligence*), dan *Internet of Things* (IoT), yang secara signifikan meningkatkan efisiensi dan konektivitas global. Namun, bersamaan dengan berbagai manfaat tersebut, muncul pula risiko yang tidak dapat diabaikan, salah satunya adalah ancaman keamanan siber (*cybersecurity threats*) yang semakin kompleks dan sering kali menimbulkan dampak merugikan bagi individu, organisasi, bahkan masyarakat secara luas.

Kerugian ekonomi global akibat kejahatan siber diperkirakan mencapai USD 10,5 triliun pada tahun 2025, meningkat hampir tiga kali lipat dibandingkan satu dekade sebelumnya (Morgan, 2020). Fakta ini menegaskan bahwa ancaman keamanan digital bukan lagi sekadar isu teknologi, melainkan ancaman strategis yang berpengaruh langsung terhadap stabilitas ekonomi global dan keberlanjutan bisnis lintas sektor. Dalam konteks ekonomi digital yang terus

berkembang, keamanan informasi menjadi fondasi penting yang menopang kepercayaan publik terhadap sistem digital dan infrastruktur ekonomi berbasis data.

Konteks ini memiliki relevansi yang besar bagi Indonesia, di mana digitalisasi kini menjadi pilar utama strategi pertumbuhan ekonomi nasional. Transformasi digital telah memungkinkan pelaku UMKM untuk memperluas pasar melalui e-commerce, sistem pembayaran digital, dan strategi pemasaran daring. Namun, seiring dengan manfaatnya, pemanfaatan teknologi juga membawa risiko yang tak terhindarkan, terutama terkait dengan keamanan informasi.

Ancaman kejahatan siber terhadap UMKM kini semakin marak dan kompleks. Dampak dari serangan tersebut dapat berupa kehilangan data pelanggan, pencurian identitas, gangguan operasional, hingga kerugian finansial yang signifikan. Dalam konteks ini, kesadaran dan pemahaman terhadap keamanan siber menjadi faktor kunci yang menentukan keberlangsungan usaha di tengah meningkatnya risiko digital.

Pentingnya literasi keamanan siber (*cybersecurity literacy*) di lingkungan UMKM semakin ditekankan dalam berbagai penelitian. Literasi ini tidak hanya mencakup keterampilan teknis, tetapi juga aspek psikologis dan perilaku digital, seperti kemampuan mengenali serangan *phishing*, malware, serta manipulasi sosial (*social engineering*). Individu yang memiliki pemahaman mendalam tentang keamanan siber lebih mampu mendeteksi dan menghindari serangan (Hadnagy, 2018). Sejalan dengan itu, Peningkatan literasi keamanan siber di kalangan UMKM menjadi strategi penting untuk mempertahankan keberlanjutan bisnis di tengah ancaman siber yang semakin kompleks, melalui peningkatan kewaspadaan, respons cepat terhadap insiden, serta dukungan kebijakan nasional di bidang keamanan siber (Balafif, 2023).

Berbagai studi juga menunjukkan bahwa pelaku UMKM perlu memahami risiko keamanan siber dan menerapkan langkah-langkah efektif untuk melindungi transaksi digital (Erdogan et al., 2023; Yudhiyati et al., 2021). Pendidikan dan pelatihan keamanan siber yang

berkelanjutan sangat diperlukan untuk meningkatkan kesadaran serta kepatuhan terhadap praktik transaksi digital yang aman (Wong et al., 2022; Yusnanto et al., 2023). Pengenalan *cybersecurity awareness* kepada pelaku UMKM menjadi langkah awal yang strategis dalam membangun kesadaran tentang bahaya transaksi digital yang tidak aman (Suartana et al., 2022), terutama mengingat meningkatnya kebutuhan akan perlindungan data di era digital (Isnaini et al., 2020).

Selain itu, berbagai inisiatif literasi digital seperti penyuluhan, sosialisasi, dan pelatihan terbukti memberikan dampak positif terhadap peningkatan literasi keamanan siber di kalangan pelaku UMKM. Program edukasi dan pendampingan mampu membekali masyarakat agar memahami penggunaan teknologi secara bijak dan aman (Ramadhan, 2024), sekaligus meningkatkan kemampuan mereka dalam menghadapi tantangan transaksi digital (Puspitasari & Pratama, 2022). Hasil pengukuran tingkat kematangan keamanan siber UMKM di Indonesia menunjukkan bahwa sebagian besar pelaku usaha masih berada dalam kategori “Buruk” dan “Kurang” (Ajhari et al., 2023), menandakan masih adanya kesenjangan signifikan antara tingkat literasi keamanan digital dan kebutuhan aktual di lapangan.

Fenomena ini juga tampak jelas di Daerah Istimewa Yogyakarta (DIY), yang dikenal sebagai salah satu wilayah dengan ekosistem UMKM kreatif paling dinamis di Indonesia. Pelaku UMKM di daerah ini masih membutuhkan edukasi dan pendampingan intensif untuk memahami ancaman digital serta mengimplementasikan praktik perlindungan data yang efektif. Meskipun pemerintah dan lembaga swasta telah melaksanakan berbagai program literasi digital, sebagian besar masih berfokus pada kemampuan dasar seperti pemasaran daring dan manajemen keuangan, bukan pada aspek keamanan siber yang krusial (Yudhiyati et al., 2021).

Di tengah derasnya arus digitalisasi dan semakin meningkatnya ancaman siber, terdapat kesenjangan nyata antara urgensi keamanan digital dan tingkat kesiapan pelaku UMKM di Indonesia, khususnya di Yogyakarta. Peningkatan literasi keamanan siber menjadi kebutuhan

mendesak untuk memperkuat ketahanan digital UMKM, menjaga keberlangsungan bisnis, serta memastikan transformasi digital yang aman, inklusif, dan berkelanjutan di era ekonomi berbasis data.

Berdasarkan kondisi tersebut, kegiatan pengabdian masyarakat ini dirancang untuk menjawab kebutuhan nyata pelaku UMKM terhadap peningkatan kesadaran dan kemampuan dalam menghadapi ancaman digital. Pendampingan ini berfokus pada peningkatan literasi keamanan siber bagi UMKM di Daerah Istimewa Yogyakarta melalui pendekatan edukatif, partisipatif, dan aplikatif.

Secara khusus, kegiatan ini bertujuan untuk:

1. Meningkatkan kesadaran dan pemahaman pelaku UMKM terhadap berbagai bentuk ancaman keamanan siber yang berpotensi merugikan usaha mereka.
2. Membekali pelaku UMKM dengan keterampilan praktis keamanan digital, seperti manajemen kata sandi, penggunaan perangkat lunak antivirus, dan pengenalan modus serangan digital.
3. Membangun budaya sadar keamanan digital di lingkungan UMKM sebagai bagian dari adaptasi terhadap transformasi ekonomi digital.

Melalui kegiatan ini diharapkan tercipta model pengabdian masyarakat yang dapat direplikasi di wilayah lain untuk memperkuat ketahanan digital nasional, sekaligus mendorong terbentuknya ekosistem UMKM yang tangguh, berdaya saing, dan aman secara siber.

II. METODE

Kegiatan pengabdian kepada masyarakat ini dilaksanakan di wilayah Provinsi Daerah Istimewa Yogyakarta (DIY) dengan fokus pada pendampingan peningkatan literasi *cyber security awareness* bagi pelaku Usaha Mikro, Kecil, dan Menengah (UMKM). Pelaksanaan kegiatan dilakukan selama bulan Mei hingga November 2024. Kegiatan dilaksanakan secara

tatap muka di lokasi tim pengabdi dan disertai praktik langsung serta secara daring dengan mitra. Kegiatan ini terdiri atas empat tahapan utama, yaitu sosialisasi literasi keamanan siber, pelatihan penggunaan perangkat keamanan digital, simulasi serangan siber dan transaksi aman, serta pendampingan dan evaluasi hasil pelatihan.

Peserta kegiatan adalah 42 pelaku UMKM dari berbagai bidang usaha di wilayah Yogyakarta, seperti kuliner, fesyen, kerajinan, dan jasa kreatif digital. Rekrutmen peserta dilakukan secara terbuka melalui pendaftaran daring (*Google Form*) yang disebarkan melalui grup WhatsApp komunitas UMKM. Peserta yang mendaftar terlebih dahulu dan memenuhi kriteria kelengkapan data usaha diprioritaskan untuk mengikuti kegiatan. Setiap peserta diwajibkan membawa perangkat digital seperti laptop atau ponsel yang digunakan dalam kegiatan usaha mereka, serta memiliki pengalaman menggunakan platform digital seperti e-commerce atau media sosial untuk transaksi daring. Kriteria ini dipilih agar kegiatan pendampingan bersifat aplikatif dan kontekstual terhadap kegiatan usaha peserta.

Desain kegiatan menggabungkan pendekatan partisipatif dan praktik langsung untuk memastikan transfer pengetahuan yang efektif. Tahap pertama berupa sosialisasi keamanan siber, yang berfokus pada peningkatan kesadaran mengenai ancaman digital seperti *phishing*, malware, *social engineering*, dan pencurian data. Pada tahap kedua, peserta mendapatkan pelatihan penggunaan perangkat lunak keamanan digital, meliputi pengenalan fungsi antivirus, *firewall*, *Virtual Private Network* (VPN), dan alat simulasi serangan siber. Selanjutnya dilakukan simulasi transaksi aman menggunakan berbagai platform digital yang umum digunakan pelaku UMKM, seperti Facebook Marketplace, Instagram Business, E-commerce, dan Google Business Profile. Pada tahap akhir, tim pelaksana melakukan pendampingan langsung untuk membantu peserta menerapkan praktik keamanan digital dalam bisnis masing-masing serta memberikan solusi terhadap permasalahan yang muncul selama penerapan. Peserta akan diberikan survei terkait beberapa hal untuk menganalisis pendekatan yang tepat dan pendampingan disesuaikan dengan kriteria peserta. Selain itu, survei kepuasan peserta terkait

metode pelatihan dan efektivitas pendampingan. Metode analisis yang akan dilakukan adalah analisis deskriptif untuk mengukur perubahan tingkat pemahaman peserta terkait *cyber security awareness*.

III. HASIL DAN PEMBAHASAN

Hasil dari kegiatan pendampingan peningkatan *literasi cyber security awareness* bagi UMKM di DIY menunjukkan adanya perubahan signifikan dalam pemahaman peserta terkait pentingnya keamanan siber dalam transaksi digital. Berdasarkan data yang diperoleh dari kuesioner yang sudah diisi oleh peserta, terlihat adanya peningkatan pengetahuan peserta setelah mengikuti pelatihan dan pendampingan ini dengan rata-rata skor 3,14 menjadi 4,54 dengan pengukuran menggunakan skala likert 1-5. Hasil ini menunjukkan bahwa pelatihan literasi digital berbasis praktik mampu meningkatkan kemampuan deteksi ancaman siber hingga lebih dari 30% di kalangan pelaku UMKM (Puspitasari & Pratama, 2022).

Sebanyak 42 peserta mengikuti kegiatan secara penuh dengan antusiasme tinggi, sebagaimana ditunjukkan pada Gambar 1 dan Gambar 2, yang memperlihatkan suasana kegiatan pelatihan dan penyampaian materi. Peserta berpartisipasi aktif dalam diskusi dan simulasi, khususnya ketika diperkenalkan pada contoh serangan siber sederhana yang sering dihadapi dalam transaksi online.

Gambar 1. Peserta Pendampingan *Cyber Security Awareness*

Para peserta yang berjumlah 42 orang mengikuti kegiatan di ruang pelatihan dengan suasana kondusif dan interaktif. Peserta terdiri dari berbagai latar belakang usaha seperti kuliner, fesyen, kerajinan, dan jasa kreatif digital. Kegiatan ini juga menjadi sarana bagi peserta untuk berbagi pengalaman terkait praktik digital yang mereka gunakan, sekaligus sebagai dasar bagi tim pendamping untuk menyesuaikan pendekatan pelatihan pada sesi berikutnya. Dengan komposisi peserta yang didominasi oleh perempuan, kegiatan ini tidak hanya meningkatkan literasi keamanan digital, tetapi juga berperan sebagai bentuk pemberdayaan perempuan di sektor UMKM berbasis teknologi di Provinsi Daerah Istimewa Yogyakarta.

Gambar 2. Penyampaian Materi *Cyber Security Awareness*

Pada sesi ini, Tim pengabdi memaparkan konsep dasar keamanan digital yang meliputi pengenalan jenis-jenis ancaman siber seperti *phishing, malware, social engineering*, serta strategi perlindungan data pribadi dan bisnis di era digital. Serangan *social engineering* menjadi bentuk manipulasi paling sering digunakan untuk mengeksploitasi kelalaian pengguna non-teknis, sehingga pemahaman psikologis pengguna terhadap modus kejahatan digital sangat penting (Hadnagy, 2018). Penyampaian materi dilakukan secara interaktif menggunakan media presentasi dan studi kasus yang relevan dengan aktivitas usaha peserta, seperti keamanan transaksi di platform e-commerce, pengelolaan akun bisnis di media sosial, serta cara mengidentifikasi tautan atau pesan mencurigakan. Tim pengabdi juga menjelaskan praktik terbaik dalam menjaga keamanan perangkat digital, penggunaan kata sandi yang kuat, serta pentingnya pembaruan sistem secara berkala.

Peserta tampak aktif berdiskusi dan memberikan tanggapan terhadap contoh-contoh kasus nyata yang disajikan. Kegiatan ini menjadi fondasi penting sebelum peserta melanjutkan

ke tahap pelatihan praktik dan simulasi keamanan siber. Melalui sesi penyampaian materi ini, peserta tidak hanya memperoleh pengetahuan teoretis, tetapi juga membangun kesadaran kritis terhadap potensi risiko digital yang dapat mengancam keberlangsungan usaha mereka.

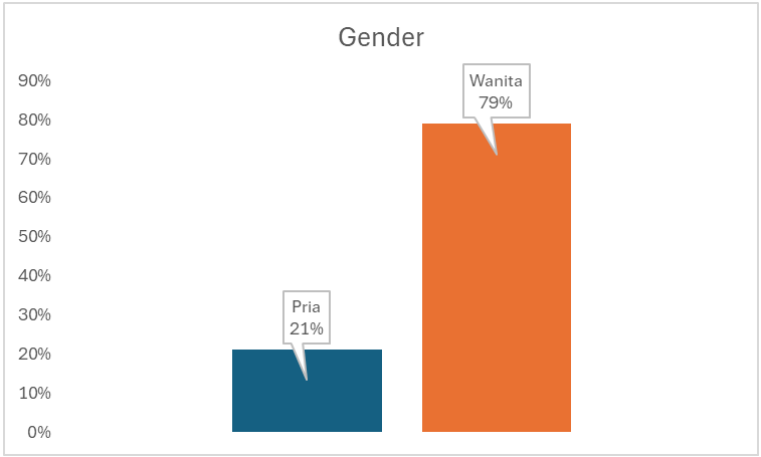
Gambar 3. Pendampingan Transaksi Digital bagi UMKM

Pendampingan juga dilakukan secara langsung melalui praktik penggunaan berbagai aplikasi transaksi digital seperti Facebook Marketplace, Instagram Business, E-commerce, dan *Google Business Profile*. Tahapan ini bertujuan membantu peserta memahami cara mengelola keamanan data pelanggan dan mencegah kebocoran informasi bisnis secara praktis (Gambar 3). Tim pengabdi berperan aktif memberikan bimbingan personal agar setiap peserta dapat menyesuaikan praktik keamanan dengan kebutuhan bisnisnya masing-masing. Kegiatan ini menunjukkan pendekatan berbasis praktik yang efektif, karena peserta tidak hanya menerima pengetahuan teoretis, tetapi juga menguasai keterampilan aplikatif dalam melindungi transaksi

digital mereka. Pendampingan semacam ini penting untuk meningkatkan kepercayaan diri pelaku UMKM dalam mengelola bisnis secara aman di era digital.

Gambar 4. Demontrasi Software *Cybersecurity*

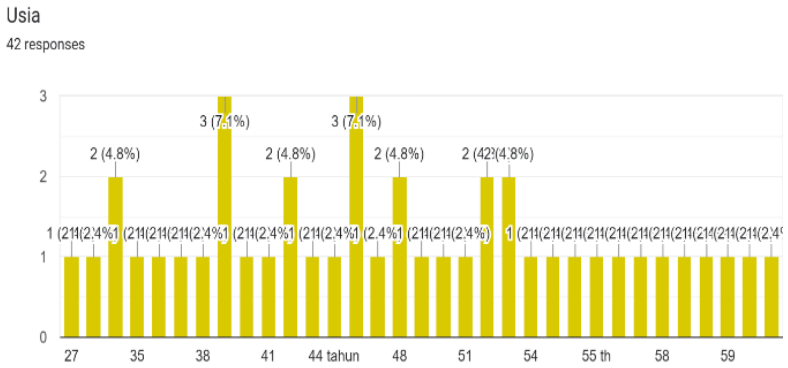
Selain itu, peserta diperkenalkan dengan beberapa perangkat keamanan seperti antivirus, *firewall, Virtual Private Network* (VPN), serta alat simulasi serangan siber (Gambar 4) yang dapat diterapkan sesuai kebutuhan usaha masing-masing. Peningkatan ketahanan digital UMKM perlu dilakukan melalui pelatihan terarah dan berbasis risiko aktual di lapangan (Ajhari et al., 2023). Tim pengabdi memberikan penjelasan tentang cara menginstal, mengonfigurasi,



dan mengoperasikan perangkat tersebut, sekaligus menekankan pentingnya pembaruan sistem keamanan secara berkala. Selain itu, peserta diajak untuk melakukan simulasi mendeteksi tautan berbahaya, memverifikasi keamanan situs web sebelum bertransaksi, dan memanfaatkan fitur keamanan tambahan pada perangkat yang digunakan. Kegiatan ini dirancang agar peserta tidak hanya mengenal istilah teknis keamanan siber, tetapi juga mampu menerapkan secara praktis teknologi pelindung data dalam operasional bisnis mereka.

Gambar 5. Analisis Data Sebaran Peserta berdasarkan Gender

Peserta yang mengikuti kegiatan ini adalah peserta dengan jenis kelamin Perempuan dan laki-laki dengan presentase 79% (33) peserta Perempuan dan 21% (9) peserta laki-laki gambar



5 menunjukkan diagram tersebut. Berdasarkan gambar tersebut kita dapat menganalisis bahwa peserta didominasi dari gender perempuan. Hal ini menunjukkan bahwa program ini menarik perhatian lebih banyak perempuan dibandingkan laki-laki.

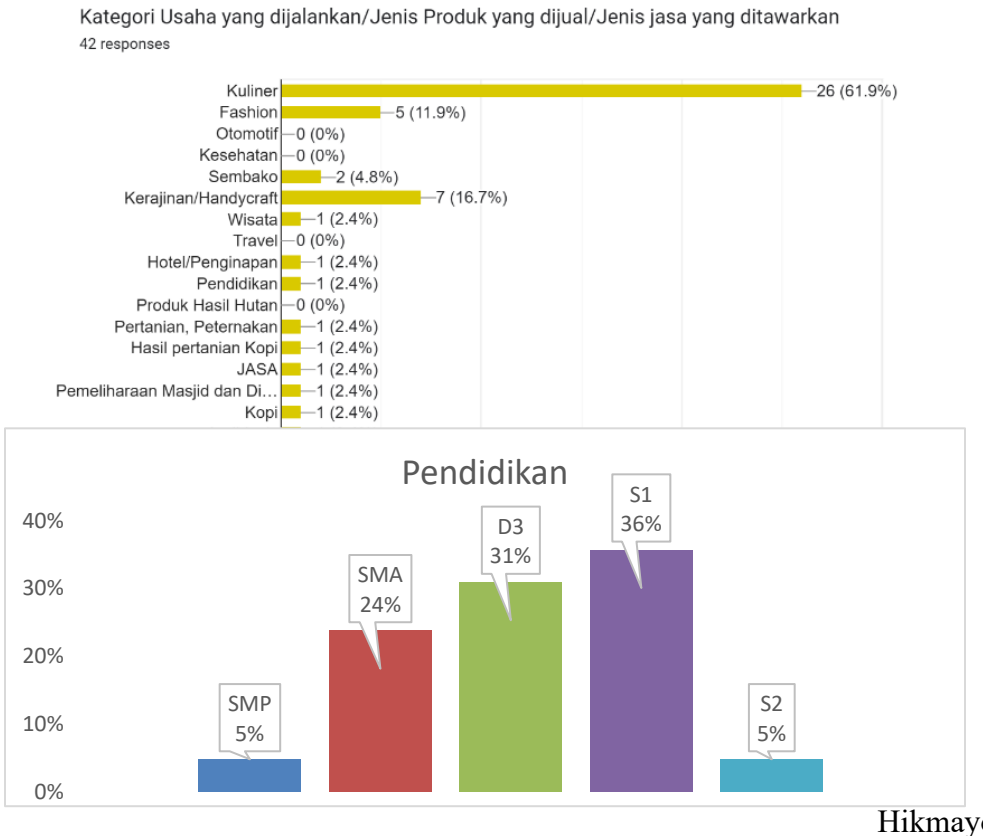
Beberapa kemungkinan alasan terkait fenomena ini, yaitu perempuan mungkin lebih tertarik mengikuti pelatihan ini karena merasa lebih membutuhkan perlindungan digital dalam kegiatan bisnis atau personal mereka, perempuan mungkin memiliki keterlibatan yang lebih tinggi dalam pengelolaan UMKM yang memanfaatkan teknologi digital sehingga lebih peduli terhadap keamanan data, dan informasi terkait pelatihan lebih efektif menjangkau Perempuan dibandingkan laki-laki, misalnya melalui jaringan sosial atau komunitas bisnis yang mayoritas anggotanya perempuan.

Gambar 6. Analisis Data Sebaran Usia Peserta

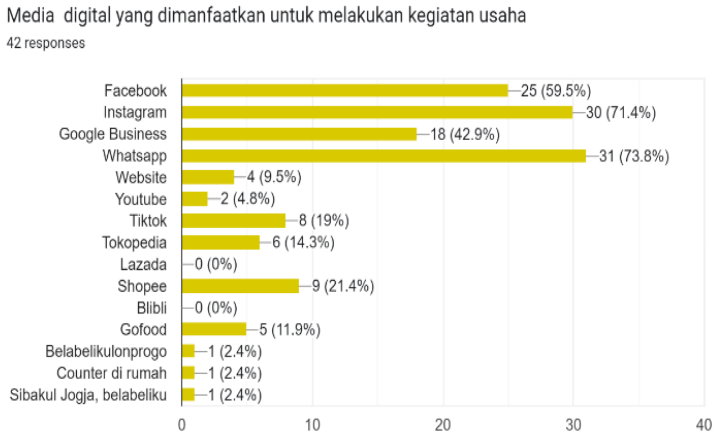
Peserta yang mengikuti pendampingan juga berasal dari beberapa tingkatan usia dari rentang usia 27 – 59 tahun. Gambar 6. menunjukkan grafik usia peserta. Hal ini menunjukkan bahwa program pendampingan dapat menjangkau berbagai kelompok usia, dengan mayoritas peserta berasal dari kelompok usia produktif (27-45 tahun) yang berperan penting dalam ekosistem UMKM digital. Peserta yang lebih tua juga menunjukkan minat yang signifikan, meskipun mereka mungkin menghadapi tantangan yang lebih besar dalam memahami teknologi keamanan siber.

Gambar 7. Analisis Data Distribusi Pendidikan Peserta

Tim pengabdi juga mensurvei terkait tingkat pendidikan peserta sehingga dapat membuat suatu kesimpulan dan pengelompokkan terkait metode yang tepat yang akan dilakukan dalam hal pendampingan. Gambar 7 menunjukan sebaran pendidikan peserta. Sebesar 35% (15)



peserta dengan latar belakang pendidikan S1, sebesar 31% (13) peserta dengan latar belakang pendidikan D3, sebesar 24% (10) peserta dengan latar belakang pendidikan SLTA, sebesar 5%



(2) peserta dengan latar belakang pendidikan S2, dan sebesar 5% (2) dengan latar belakang pendidikan SLTP. Hal ini menunjukkan bahwa mayoritas peserta memiliki latar belakang pendidikan S1 (35%) dan D3 (31%), sebagian besar peserta sudah memiliki pemahaman dasar yang cukup mengenai teknologi, namun masih memerlukan pendalaman lebih lanjut dalam aspek keamanan siber.

Gambar 8. Analisis Data Sebaran Jenis Usaha Peserta

Berdasarkan hasil survei pada Gambar 8 terkait kategori usaha yang dijalankan/jenis produk yang dijual/jenis jasa yang ditawarkan dari peserta pendampingan menunjukkan bahwa sebagian besar 61,9% peserta menjalankan usaha kuliner dan sisanya 38,1 % menjalankan usaha bisnis di sektor lainnya. Sektor kuliner merupakan pelaku paling aktif dalam pemanfaatan platform digital untuk transaksi dan pemasaran daring (Sofiati & Anggraeni, 2021). Sebagian besar peserta yang menjalankan usaha kuliner memerlukan pengetahuan keamanan siber yang relevan dengan aktivitas digital mereka, seperti memproses transaksi online, melindungi data pelanggan, dan menjaga reputasi digital mereka. Usaha di sektor lainnya juga memerlukan pendekatan keamanan siber yang sesuai dengan konteks bisnis mereka, termasuk perlindungan terhadap pencurian data dan penyalahgunaan informasi sensitif.

Gambar 9. Analisi Data Media Digital yang digunakan Peserta

Tim pengabdi juga melakukan survei kepada peserta terkait media digital yang dimanfaatkan untuk melakukan kegiatan usaha pada gambar 9. Hal tersebut menunjukkan bahwa sebagian besar 73,8% peserta menggunakan media W*hatsApp* dalam melakukan kegiatan usaha dan selebihnya 26,2% menggunakan media lainnya ataupun peserta menggunakan beberapa media untuk mendukung kegiatan usaha mereka. Pelaku UMKM di Indonesia lebih banyak mengandalkan aplikasi komunikasi cepat seperti WhatsApp karena kemudahan penggunaan dan jangkauan pelanggan yang luas (Isnaini et al., 2020). Sebagian besar peserta menggunakan *WhatsAp*p sebagai media utama untuk menjalankan usaha mereka. Hal tersebut menunjukkan bahwa kemudahan dalam penggunaan *WhatsAp*p, menyediakan berbagai fitur yang mendukung kebutuhan bisnis, seperti balasan otomatis, katalog produk, serta komunikasi langsung dengan pelanggan secara real-time, dan memungkinkan pelaku usaha untuk menjangkau pelanggan dengan lebih cepat dan efisien, terutama di Indonesia di mana aplikasi ini sangat populer. Dengan pengetahuan yang baik tentang ancaman keamanan siber di berbagai platform digital, UMKM dapat meningkatkan perlindungan bisnis mereka dan mencegah potensi kerugian akibat serangan siber.

Hasil kegiatan ini menunjukkan bahwa pelatihan yang menggabungkan pendekatan edukatif dan partisipatif efektif dalam membangun pemahaman menyeluruh peserta terhadap keamanan digital. Pelaku usaha kecil di negara berkembang cenderung mengabaikan keamanan siber karena keterbatasan sumber daya dan pengetahuan teknis, sehingga diperlukan pendekatan edukatif yang sederhana namun berkelanjutan (Yudhiyati et al., 2021).

Kegiatan pendampingan ini juga memperlihatkan dampak sosial yang positif. Peserta melaporkan peningkatan kepercayaan diri dalam menggunakan teknologi dan rasa aman dalam menjalankan bisnis daring. Pelatihan dasar keamanan digital secara langsung dapat mengurangi risiko pencurian data dan meningkatkan kesadaran pelaku usaha terhadap ancaman dunia maya (Yusnanto et al., 2023).

Secara keseluruhan, kegiatan ini berhasil mencapai tujuannya, yaitu meningkatkan literasi keamanan siber pelaku UMKM melalui pelatihan yang aplikatif, kontekstual, dan

inklusif. Namun demikian, masih terdapat beberapa keterbatasan, antara lain durasi kegiatan yang relatif singkat, jumlah peserta yang terbatas, dan evaluasi berbasis self-report yang memungkinkan adanya bias persepsi. Dibutuhkan program pelatihan berjenjang dan kemitraan dengan lembaga IT untuk memperkuat aspek teknis serta memperluas cakupan peserta (Balafif, 2023). Selain itu, monitoring jangka panjang juga diperlukan untuk memastikan bahwa praktik keamanan siber yang telah diperkenalkan benar-benar diterapkan secara berkelanjutan dalam aktivitas usaha.

IV. KESIMPULAN

Kegiatan pendampingan peningkatan literasi *Cyber Security Awareness* bagi pelaku UMKM di Daerah Istimewa Yogyakarta telah memberikan hasil yang positif dan terukur terhadap peningkatan pemahaman peserta mengenai keamanan digital. Berdasarkan hasil kuesioner sebelum dan sesudah pelatihan, terjadi peningkatan signifikan pada tingkat literasi keamanan siber peserta, yaitu dari rata-rata skor 3,14 menjadi 4,54 pada skala Likert 1–5. Hasil tersebut menunjukkan bahwa metode pelatihan berbasis praktik langsung yang diterapkan dalam kegiatan ini berhasil meningkatkan kemampuan peserta dalam mengenali ancaman siber serta menerapkan praktik keamanan digital yang lebih baik dalam aktivitas usaha sehari-hari.

Sebagian besar peserta kegiatan merupakan perempuan (79%) yang bergerak pada sektor kuliner (61,9%). Temuan ini menunjukkan bahwa kelompok perempuan memiliki antusiasme tinggi dalam meningkatkan kompetensi keamanan digital dan memegang peran strategis dalam transformasi digital UMKM di Yogyakarta. Dominasi peserta dari sektor kuliner juga menunjukkan bahwa pelatihan keamanan siber sangat relevan dengan kebutuhan pelaku usaha yang aktif bertransaksi daring dan mengelola data pelanggan melalui berbagai platform digital.

Hasil survei juga menunjukkan bahwa WhatsApp merupakan platform bisnis yang paling dominan digunakan oleh peserta (73,8%) karena kemudahan akses, kecepatan komunikasi, dan fitur interaktif yang mendukung kegiatan usaha. Namun, kondisi ini juga

menegaskan pentingnya peningkatan kesadaran terhadap risiko keamanan digital pada aplikasi pesan instan, seperti potensi phishing, penipuan daring, dan kebocoran data.

Sebagai tindak lanjut, disarankan agar kegiatan ini dikembangkan menjadi program pelatihan berjenjang yang melibatkan kemitraan dengan lembaga dan praktisi di bidang teknologi informasi serta keamanan siber. Kolaborasi ini diharapkan dapat memperkuat aspek teknis pendampingan, memperluas cakupan peserta, dan memastikan keberlanjutan hasil melalui kegiatan monitoring serta evaluasi jangka panjang. Dengan demikian, program ini tidak hanya meningkatkan literasi keamanan siber dalam jangka pendek, tetapi juga membangun ketahanan digital berkelanjutan bagi pelaku UMKM di Daerah Istimewa Yogyakarta.

UCAPAN TERIMAKASIH

Tim pengabdi mengucapkan terima kasih terutama ditujukan kepada Universitas Negeri Yogyakarta, Direktorat Riset dan Pengabdian Masyarakat (DRPM) UNY, PT Sarana Infotekno Mitra Solusi, dan berbagai UMKM di DIY sebagai peserta kegiatan.

DAFTAR PUSTAKA

Ajhari, A. A., Manaon, M. A., & Dimas. (2023). Security Awareness Framework untuk Usaha Mikro, Kecil dan Menenengah di Indonesia. *Info Kripto*, *17*(3), 85–91. https://doi.org/10.56706/ik.v17i3.80

Balafif, S. (2023). Penyesuaian Model Ketahanan Siber UMKM Di Indonesia Dengan Nist Cybersecurity Framework. *Jurnal Informatika: Jurnal Pengembangan IT*, *8*(3), 291–301. https://doi.org/10.30591/jpit.v8i3.5662

Erdogan, G., Halvorsrud, R., Boletsis, C., Tverdal, S., & Pickering, J. B. (2023). Cybersecurity Awareness and Capacities of SMEs. *International Conference on Information Systems Security and Privacy*, *Icissp*, 296–304. https://doi.org/10.5220/0011609600003405

Hadnagy, C. (2018). Social Engineering "The Science of Human Hacking." *Wiley*, *2*, 2–362. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT%0Ahttp://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52012PC0011:pt:NOT

Isnaini, K. N., Sulistiyani, D. F., & Sutrisno, M. (2020). Data Security Awarenesssebagai Upaya Peningkatan Literasi Tentang Cyber AttacksdanThreats. *Jurnal Pemberdayaan Masyarakat Berkarakter*, *3*(2), 121–132.

Morgan, S. (2020). Cybercrime To Cost The World $10.5 Trillion Annually By 2025. *Cybercrime Magazine*. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

Puspitasari, D., & Pratama, Y. B. D. (2022). Penguatan UMKM melalui Pelatihan Literasi Digital di Dusun Beran, Gemarang, Madiun. *Jurnal Manajemen Dan Pemasaran Jasa*, *3*(1), 1–12.

Ramadhan, R. F. (2024). Peningkatan Pemahaman Penggunaan Marketplace Melalui Sosialisasi Pada Anak Usia Dasar dan Remaja. *Abdinesia: Jurnal Pengabdian Kepada Masyarakat*, *4*(1), 59–63. https://doi.org/10.69503/abdinesia.v4i1.575

Sofiati, S., & Anggraeni, I. S. K. (2021). Strategi Memikat Dan Mempertahankan Pelanggan Melalui Digital Marketing Dan Aplikasi Keuangan Fintech Warung Jamu Tradisional Pada Era Pandemi Covid-19. *Jurnal Ilmiah Padma Sri Kreshna*, *3*(1). https://doi.org/10.37631/psk.v3i1.396

Suartana, I. M., Eka Putra, R., Bisma, R., & Prapanca, A. (2022). Pengenalan Pentingnya Cyber Security Awareness pada UMKM. *Jurnal Abadimas Adi Buana*, *5*(02), 197–204. https://doi.org/10.36456/abadimas.v5.i02.a4560

Wong, L. W., Lee, V. H., Tan, G. W. H., Ooi, K. B., & Sohal, A. (2022). The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities. *International Journal of Information Management*, *66*(May). https://doi.org/10.1016/j.ijinfomgt.2022.102520

Yudhiyati, R., Putritama, A., & Rahmawati, D. (2021). What small businesses in developing country think of cybersecurity risks in the digital age: Indonesian case. *Journal of Information, Communication and Ethics in Society*, *19*(4), 446–462. https://doi.org/10.1108/JICES-03-2021-0035

Yusnanto, T., Fatkhurrochman, F., Muin, M. A., & Waluyo, S. (2023). Pelatihan Dasar Keamanan Digital Untuk Mengurangi Pencurian Data Yang Berdampak Pada UMKM. *Jurnal Pengabdian Masyarakat Bangsa*, *1*(9), 2022–2029. https://doi.org/10.59837/jpmba.v1i9.458