

Peningkatan *Cyber Security Awareness* Melalui Pelatihan Edukatif Kepada Siswa Sekolah Menengah Kejuruan

Khairul Fathan Habie*¹, Aldibangun Pidekso Putro², Herman Yuliansyah³, Imam Riadi⁴

^{1,2,3,4} Universitas Ahmad Dahlan, Yogyakarta, Indonesia

Corresponding Author: 2307048001@webmail.uad.ac.id

Abstrak

Perkembangan teknologi informasi dan komunikasi telah mengalami pertumbuhan yang sangat pesat. Era digital membawa banyak kemudahan dan keuntungan, mulai dari akses informasi yang cepat, komunikasi yang efisien, hingga kemudahan layanan online yang mempermudah kehidupan sehari-hari. Sejalan dengan hal tersebut era digital juga menghadirkan tantangan baru dalam hal keamanan informasi atau cyber security. Keamanan informasi menjadi semakin krusial dengan meningkatnya penggunaan teknologi digital, membuat individu, organisasi, dan institusi rentan terhadap ancaman siber seperti peretasan, pencurian data, malware, dan serangan phishing. Oleh karena itu, diperlukan pelatihan dengan tujuan untuk meningkatkan kesadaran dan pemahaman siswa SMK 1 Sedayu, tentang pentingnya kesadaran dan pemahaman cyber security. Kegiatan program pemberdayaan umat (PRODAMAT) meliputi tahap persiapan, pelaksanaan, dan evaluasi. Kegiatan PRODAMAT dilakukan dengan metode ceramah dan diskusi tanya jawab. Peningkatan pemahaman siswa diukur dengan rangkaian pre-test dan post-test. Hasil yang diperoleh dari program pemberdayaan umat menunjukkan bahwa adanya peningkatan pemahaman pada indikator kesadaran "Sangat Paham" meningkat dari 31% menjadi 52%.

Kata kunci: *Cyber Security, Cyber Security Awareness, Pelatihan Edukatif*

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi dalam beberapa dekade terakhir telah mengalami pertumbuhan yang sangat pesat. Era digital membawa banyak kemudahan dan keuntungan, mulai dari akses informasi yang cepat, komunikasi yang efisien, hingga berbagai layanan *online* yang mempermudah kehidupan sehari-hari (Nurul, Shynta Anggrainy, & Siska Aprelyani, 2022). Selain itu, teknologi digital juga telah membuka peluang baru dalam berbagai bidang seperti pendidikan, kesehatan, bisnis, dan pemerintahan (Mere, 2024) (Verdinandus Lelu Ngono & Taufik Hidayat, 2019). Penggunaan teknologi digital memungkinkan proses pembelajaran yang lebih interaktif, layanan kesehatan yang lebih terjangkau, transaksi bisnis yang lebih cepat, serta pelayanan publik yang lebih efektif dan transparan, namun di balik segala manfaat yang ditawarkan, era digital juga menghadirkan tantangan baru, terutama dalam hal keamanan informasi atau *cyber security*. Keamanan informasi menjadi isu yang semakin krusial seiring dengan meningkatnya penggunaan teknologi digital (Lallie et al., 2021). Setiap individu, organisasi, dan institusi kini sangat bergantung pada sistem informasi dan jaringan internet. Ketergantungan ini menciptakan kerentanan terhadap berbagai ancaman siber seperti peretasan, pencurian data, malware, dan serangan phishing (Alkhalil, Hewage, Nawaf, & Khan, 2021). Misalnya, peretasan dapat menyebabkan kerugian finansial yang besar bagi perusahaan, sementara pencurian data pribadi dapat mengakibatkan penyalahgunaan identitas yang merugikan individu.

Kasus-kasus seperti kebocoran data pribadi, penipuan *online*, dan serangan siber pada institusi penting seringkali menghiiasi berita, menunjukkan bahwa ancaman ini nyata dan dapat terjadi kapan saja (Mediana, 2024). Beberapa insiden besar, seperti serangan ransomware pada sistem kesehatan dan kebocoran data pengguna media sosial, menunjukkan betapa seriusnya ancaman siber ini (Wisanggenis, 2020). Bahkan, serangan siber dapat mengganggu stabilitas nasional jika menargetkan infrastruktur kritis seperti jaringan listrik atau sistem perbankan. Hal

ini menggarisbawahi betapa pentingnya langkah-langkah perlindungan yang tepat dan kesadaran yang tinggi mengenai keamanan siber.

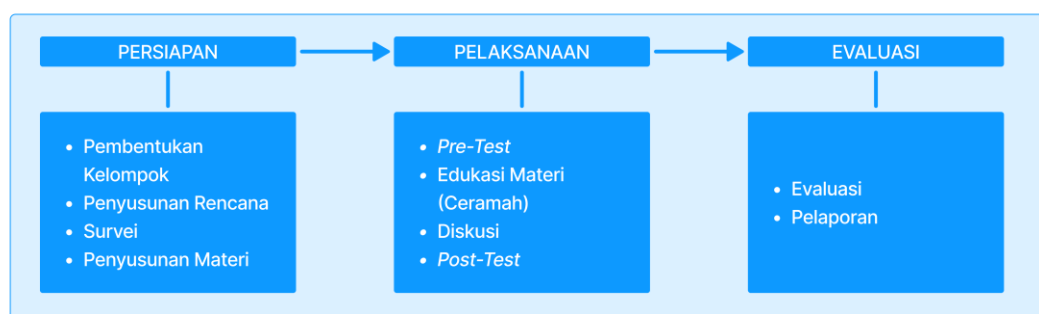
Kesadaran masyarakat terhadap pentingnya keamanan siber saat ini masih relatif rendah. Banyak individu yang belum memahami cara melindungi informasi pribadi mereka secara efektif (Sadeli & Irawati, 2023), tidak menyadari risiko yang terkait dengan penggunaan teknologi digital, atau tidak mengetahui tindakan yang harus diambil saat menghadapi ancaman siber (Suartana, Eka Putra, Bisma, & Prapanca, 2022). Kurangnya edukasi dan pemahaman mengenai cyber security ini dapat berdampak buruk, baik bagi individu maupun masyarakat baik secara fisik maupun mental secara keseluruhan (Ramadhan & Nurnawati, 2023). Dampak yang ditimbulkan tidak hanya bersifat finansial tetapi juga dapat mempengaruhi aspek psikologis dan emosional. Misalnya, korban penipuan online mungkin mengalami stres dan kecemasan yang berkepanjangan (Kiling & Kiling-Bunga, 2019).

Pelatihan merupakan metode yang sangat efektif untuk memberikan edukasi terkait pentingnya keamanan siber. Melalui pelatihan, peserta dapat menerima informasi secara langsung dan interaktif (Sudarsono, Nafiati, et al., 2023) (Sudarsono, Tentama, et al., 2023), yang membantu mereka dalam memahami konsep-konsep dasar serta aplikasi praktis dalam menjaga keamanan siber. Penelitian sebelumnya menunjukkan bahwa pelatihan yang terstruktur dan melibatkan ceramah interaktif, diskusi, serta simulasi praktik nyata dapat secara signifikan meningkatkan kesadaran dan keterampilan peserta dalam mengidentifikasi serta mengatasi ancaman siber (Sulistyawati et al., 2022) (Sukei et al., 2022). Hal ini menjadikan pelatihan sebagai alat yang penting dalam upaya meningkatkan keamanan siber.

Program Pemberdayaan Umat (PRODAMAT) ini bertujuan untuk meningkatkan kesadaran dan pemahaman masyarakat mengenai pentingnya *cyber security* di era digital. Melalui berbagai kegiatan edukatif, pelatihan, dan sosialisasi, diharapkan masyarakat dapat lebih memahami risiko-risiko siber dan langkah-langkah yang perlu diambil untuk melindungi diri siswa sendiri dan data pribadinya. Program ini juga membekali peserta dengan pengetahuan praktis dan keterampilan dasar dalam mengamankan informasi digital, sehingga peserta dapat lebih percaya diri dan aman dalam memanfaatkan teknologi digital dalam kehidupan sehari-hari. Dengan meningkatnya kesadaran dan pemahaman mengenai *cyber security*, diharapkan masyarakat dapat lebih waspada terhadap ancaman siber, lebih bijak dalam menggunakan teknologi, dan pada akhirnya dapat berkontribusi dalam menciptakan lingkungan digital yang lebih aman dan terlindungi.

2. METODE PELAKSANAAN

Pelatihan ini dilaksanakan pada tanggal 10 Juni 2024 bertempat di SMK 1 Sedayu, Kabupaten Bantul, DI. Yogyakarta. Kegiatan ini mengangkat tema terkait peningkatan *cyber security awareness*. Peserta yang menjadi sasaran utama pada kegiatan ini adalah siswa SMK 1 Sedayu. Pelaksanaan kegiatan ini terdiri dari beberapa tahap, dimulai dari persiapan, pelaksanaan, dan evaluasi. Secara umum metode pelaksanaan dapat dilihat pada Gambar 1.



Gambar 1 Metode Pelaksanaan

Tahapan persiapan merupakan langkah awal yang sangat krusial untuk memastikan keberhasilan program secara keseluruhan. Proses ini dirancang agar setiap aspek program dapat direncanakan secara sistematis, menyeluruh, dan terkoordinasi dengan baik. Tahapan ini diawali dengan pembentukan tim yang terdiri dari anggota yang memiliki kompetensi, pengalaman, dan pemahaman yang relevan terhadap tujuan dari program. Tim ini tidak hanya bertanggung jawab dalam menyusun rencana kegiatan, tetapi juga memastikan bahwa setiap detail program, seperti jadwal, materi, dan metode pelaksanaan, dirancang dengan baik. Selain itu, survei lokasi kegiatan dilakukan untuk memastikan tempat yang dipilih memiliki fasilitas yang memadai, seperti aksesibilitas, ketersediaan perangkat pendukung, serta kenyamanan peserta. Materi yang relevan dan menarik juga disiapkan dengan seksama, mencakup berbagai topik penting terkait keamanan siber. Persiapan yang matang juga mencakup antisipasi terhadap berbagai risiko yang mungkin dapat terjadi selama pelaksanaan kegiatan. Tujuan utama dari tahapan persiapan ini adalah untuk meminimalkan risiko yang mungkin terjadi dan memastikan bahwa program dapat berjalan dengan lancar, efektif, dan sesuai dengan yang telah direncanakan.

Tahapan pelaksanaan merupakan inti dari seluruh rangkaian kegiatan, di mana program yang telah direncanakan sebelumnya dijalankan dengan mengacu pada rencana yang telah disusun secara detail. Pada tahap ini, interaksi langsung dengan peserta menjadi fokus utama, menggunakan metode ceramah interaktif yang dirancang agar materi disampaikan secara terstruktur, menarik, dan mudah dipahami oleh peserta. Peserta diajak untuk berpartisipasi aktif melalui diskusi dan sesi tanya jawab, sehingga pembelajaran menjadi lebih dinamis dan efektif. Untuk mengukur efektivitas pelatihan, dilakukan *pre-test* sebelum kegiatan dimulai, yang bertujuan mengetahui tingkat pemahaman awal peserta terhadap topik yang akan dibahas. Setelah pelatihan selesai, *post-test* dilaksanakan untuk mengevaluasi sejauh mana peningkatan pengetahuan dan pemahaman peserta terhadap materi yang telah disampaikan. Pendekatan ini dirancang untuk memastikan bahwa pelatihan memberikan dampak nyata terhadap peningkatan kesadaran dan kemampuan peserta, khususnya dalam hal keamanan siber, sehingga tujuan program dapat tercapai secara maksimal.

Tahapan evaluasi merupakan tahapan terakhir yang dilakukan setelah seluruh kegiatan pelatihan selesai dilaksanakan. Tujuan utama dari tahapan ini untuk mengidentifikasi segala kendala yang muncul selama pelaksanaan serta merumuskan solusi yang tepat untuk mengatasinya. Pada tahap ini, tim melakukan pengumpulan dan analisis data secara menyeluruh, mencakup hasil *pre-test* dan *post-test* untuk mengevaluasi tingkat peningkatan pemahaman peserta, serta umpan balik yang diberikan oleh peserta mengenai kualitas pelatihan yang telah diikuti. Data yang diperoleh tersebut kemudian dianalisis secara mendalam untuk menilai efektivitas metode yang digunakan, relevansi materi yang disampaikan, serta tingkat kepuasan peserta terhadap pelatihan. Berdasarkan hasil analisis tersebut, tim kemudian menyusun laporan evaluasi yang mendokumentasikan seluruh tahapan kegiatan, kendala yang dihadapi, solusi yang diterapkan, serta pencapaian yang diraih. Laporan ini tidak hanya berfungsi sebagai alat untuk menilai keberhasilan kegiatan yang telah dilaksanakan, tetapi juga menjadi referensi penting bagi pengembangan dan perbaikan program serupa di masa mendatang. Dengan adanya evaluasi yang terstruktur dan komprehensif, diharapkan pelatihan berikutnya dapat dirancang dengan lebih baik, memberikan manfaat yang lebih besar bagi peserta, dan mencapai hasil yang lebih optimal.

3. HASIL DAN PEMBAHASAN

Persiapan

Pada tahapan persiapan ini dimulai dengan pembentukan Kelompok Program Pemberdayaan Umat (PRODAMAT) yang terdiri dari dua Mahasiswa Magister Informatika UAD dan dua dosen Pembimbing Kelompok. Setelah kelompok terbentuk, langkah selanjutnya adalah anggota kelompok menyusun rencana kegiatan dan pelaksanaan survei lokasi kegiatan.

Kegiatan survei menunjukkan lokasi kegiatan yakni SMK 1 Sedayu memiliki fasilitas yang memadai untuk pelaksanaan program kegiatan pemberdayaan umat secara optimal. Selain itu, diskusi mendalam dengan pihak sekolah juga dilakukan untuk memastikan bahwa materi yang akan disampaikan selaras dengan kurikulum yang sudah ada serta relevan dengan kebutuhan para siswa.

Materi presentasi disusun dan mencakup topik-topik penting tentang *cyber security*, jenis-jenis kejahatan *cyber*, panduan penggunaan *password* yang kuat, dan praktik serta kebiasaan *cyber* yang aman. Materi disusun dalam bentuk presentasi *power-point* yang menarik, dapat dilihat pada Gambar 2.



Gambar 2 Materi Presentasi *PowerPoint*

Pelaksanaan

Pelaksanaan kegiatan ini dilakukan dengan interaksi langsung dengan peserta melalui metode ceramah yang interaktif, sebagaimana dapat dilihat pada Gambar 3. Topik yang dibahas mencakup definisi dan pentingnya keamanan siber, pengenalan berbagai jenis serangan siber, panduan untuk penggunaan kata sandi yang baik dan kuat, serta praktik dan kebiasaan siber yang aman. Selain penyampaian materi secara langsung, juga diadakan sesi diskusi tanya jawab dengan peserta pelatihan. Melalui sesi tanya jawab ini, peserta memiliki kesempatan untuk mengajukan pertanyaan dan mendapatkan penjelasan lebih mendalam, sehingga pemahaman siswa tentang materi yang disampaikan dapat lebih optimal. Kegiatan ini dirancang sedemikian rupa untuk memastikan bahwa peserta tidak hanya menerima informasi secara pasif, tetapi juga terlibat secara aktif dalam proses pembelajaran.



Gambar 3 Penyampaian Materi *Cyber Security*

Evaluasi

Evaluasi pelatihan dilakukan dengan menggunakan *pre-test* yang diberikan sebelum pelatihan dimulai dan *post-test* yang dilakukan setelah pelatihan selesai. Hasil dari *pre-test* dan *post-test* tersebut digunakan untuk mengukur tingkat efektivitas pembelajaran yang telah dilakukan. Jumlah sampel yang dikumpulkan dari *pre-test* dan *post-test* masing-masing adalah sebanyak 26 responden. Instrumen yang digunakan dalam *pre-test* dan *post-test* mencakup tiga indikator penilaian, yaitu pengetahuan, tindakan, dan kesadaran terhadap keamanan siber. Masing-masing indikator penilaian tersebut dapat dilihat pada Tabel 1. Setiap indikator penilaian memiliki berbagai aspek pemahaman yang berbeda-beda. Indikator penilaian serta aspek-aspek penilaian yang digunakan untuk mengukur tingkat pemahaman siswa dapat dilihat secara rinci pada Tabel 2. Metode yang digunakan untuk menghitung hasil kuesioner adalah skala likert, yang memungkinkan pengukuran melalui tingkat persetujuan atau ketidaksetujuan peserta terhadap pernyataan-pernyataan yang berkaitan dengan indikator penilaian.

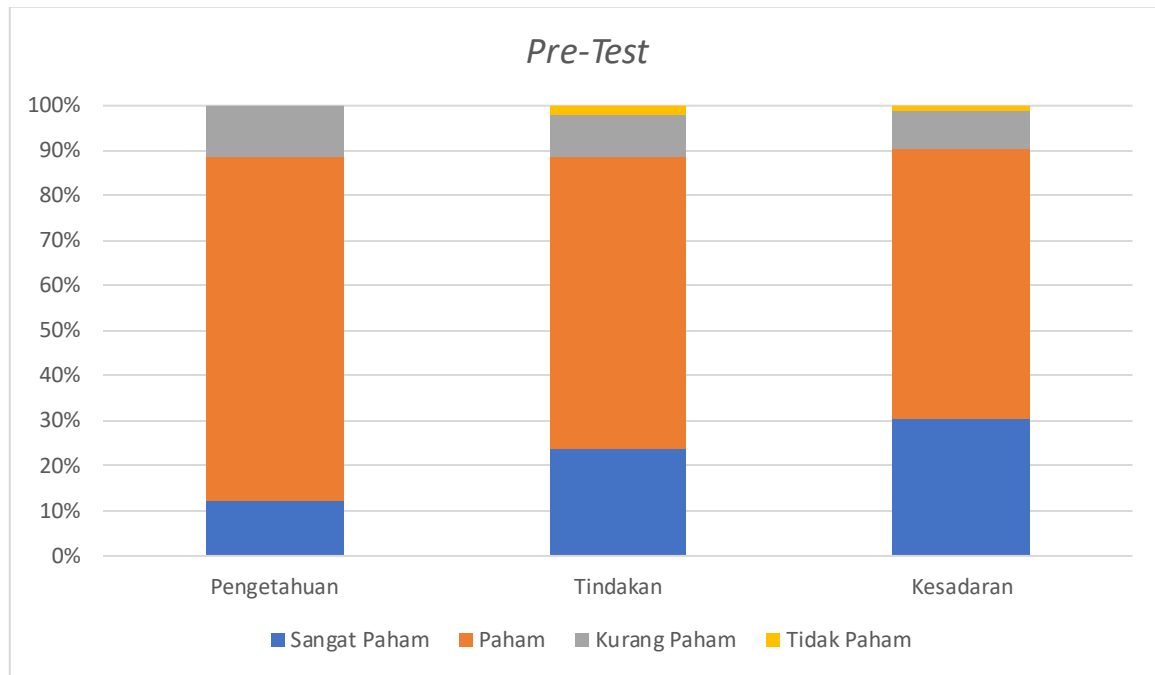
Tabel 1 Indikator Penilaian

No	Indikator	Deskripsi
1	Pengetahuan	Mengukur pemahaman pengetahuan individu terkait definisi dan pentingnya <i>cyber security</i> .
2	Tindakan	Mengukur sejauh mana individu menerapkan praktik-praktik <i>cyber security</i> dalam keseharian.
3	Kesadaran	Mengukur tingkat kewaspadaan individu terkait potensi ancaman <i>cyber security</i> dalam keseharian.

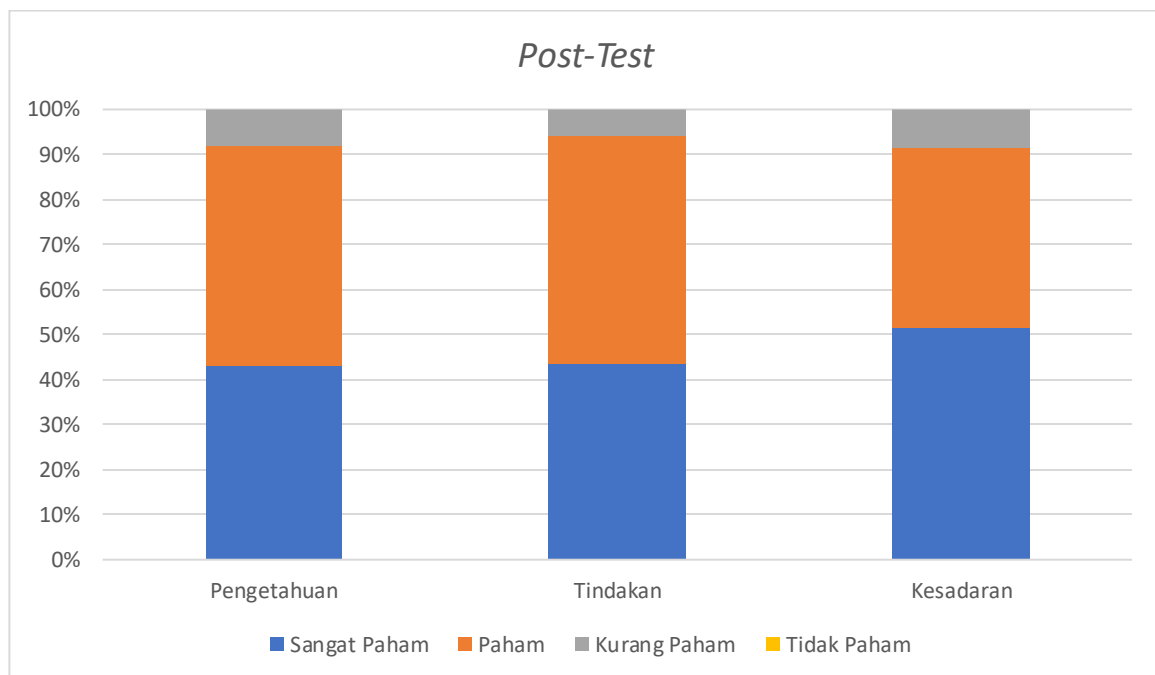
Tabel 2 Indikator Penilaian dan Aspek Penilaian

Indikator	Aspek	Bobot
Pengetahuan	Sangat Paham	4
	Paham	3
	Kurang Paham	2
	Tidak Paham	1
Tindakan	Sangat Paham	4
	Paham	3
	Kurang Paham	2
	Tidak Paham	1
Kesadaran	Sangat Paham	4
	Paham	3
	Kurang Paham	2
	Tidak Paham	1

Tabel 2 menjelaskan penilaian untuk tiga indikator utama, yaitu pengetahuan, tindakan, dan kesadaran terkait keamanan siber. Setiap indikator dinilai berdasarkan tingkatan pemahaman yang telah ditentukan. Tingkatan tersebut adalah sangat paham dengan bobot 4, paham dengan bobot 3, kurang paham dengan bobot 2, dan tidak paham dengan bobot 1. Hasil dari *pre-test* dan *post-test* yang dilakukan untuk mengevaluasi tingkat pemahaman siswa terhadap materi yang diberikan dapat dilihat secara rinci pada Gambar 4 dan 5.



Gambar 4 Hasil *Pre-Test* Pemahaman Terkait *Cyber Security*



Gambar 5 Hasil *Post-Test* Pemahaman Terkait *Cyber Security*

Pada Gambar 4 dan Gambar 5, diperlihatkan secara jelas perbandingan hasil *pre-test* dan *post-test* terkait pemahaman siswa tentang keamanan siber. Dari data tersebut, kita dapat melihat adanya peningkatan yang signifikan dalam pemahaman siswa pada setiap indikator penilaian yang telah ditetapkan. Pada indikator Pengetahuan, terlihat bahwa jumlah siswa yang “Sangat Paham” meningkat dari 12% pada saat *pre-test* menjadi 43% pada saat *post-test*. Ini menunjukkan bahwa pelatihan yang diberikan telah berhasil meningkatkan pengetahuan siswa secara substansial. Sementara itu, jumlah siswa yang “Kurang Paham” menurun dari 11% menjadi 8%, yang mengindikasikan bahwa sebagian besar siswa telah meningkatkan pemahaman mereka setelah mengikuti pelatihan.

Pada indikator Tindakan, peningkatan pemahaman juga terlihat jelas. Jumlah siswa yang “Sangat Paham” meningkat dari 24% sebelum pelatihan menjadi 41% setelah pelatihan. Selain itu, jumlah siswa yang “Kurang Paham” menurun dari 9% menjadi 6%, dan tidak ada lagi peserta yang “Tidak Paham” setelah pelatihan selesai. Hal ini menunjukkan bahwa pelatihan tidak hanya meningkatkan pengetahuan, tetapi juga kemampuan siswa dalam menerapkan tindakan yang tepat terkait keamanan siber. Pada indikator Kesadaran, peningkatan pemahaman siswa juga sangat signifikan. Jumlah siswa yang “Sangat Paham” meningkat dari 31% pada saat pre-test menjadi 52% pada saat post-test. Lebih lanjut, tidak ada lagi peserta pelatihan yang “Tidak Paham” setelah pelatihan selesai. Ini menunjukkan bahwa pelatihan yang diberikan telah berhasil meningkatkan kesadaran siswa tentang pentingnya keamanan siber dalam kehidupan sehari-hari.

Secara keseluruhan, hasil dari *pre-test* dan *post-test* ini menunjukkan bahwa pelatihan yang diberikan telah berhasil secara signifikan meningkatkan pemahaman, tindakan, dan kesadaran siswa terhadap keamanan siber. Peningkatan yang konsisten pada setiap indikator penilaian mengindikasikan bahwa metode dan materi yang digunakan dalam pelatihan sangat efektif dan relevan dengan kebutuhan siswa.

4. KESIMPULAN

Kegiatan program pemberdayaan umat dengan tema “Peningkatan *Cyber Security Awareness* Melalui Pelatihan Edukatif Kepada Siswa Sekolah Menengah Kejuruan” yang dilakukan di SMK 1 Sedayu, berhasil terlaksana dengan baik dan sesuai harapan. Kegiatan ini dilakukan dengan tujuan untuk meningkatkan kesadaran akan *cyber security* di lingkungan sekolah menengah kejuruan. Pada pelatihan ini siswa diberikan pengetahuan tentang definisi dan pentingnya *cyber security*, pengenalan jenis-jenis serangan *cyber*, panduan penggunaan password yang baik, serta praktik dan kebiasaan *cyber* yang aman. Hasil pengujian menunjukkan bahwa adanya peningkatan pemahaman pada indikator kesadaran “Sangat Paham” meningkat dari 31% menjadi 52%.

UCAPAN TERIMA KASIH

Terima kasih diucapkan kepada kepala sekolah, guru, dan siswa SMK 1 Sedayu, Bantul, DI Yogyakarta yang telah menerima dengan baik untuk melaksanakan program ini. Penulis juga sangat berterima kasih kepada program studi Magister Informatika Universitas Ahmad Dahlan (MTI UAD) yang telah mendukung selama proses kegiatan program pemberdayaan umat (PRODAMAT).

DAFTAR PUSTAKA

- Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. *Frontiers in Computer Science*, 3(March), 1–23.
- Kiling, I. Y., & Kiling-Bunga, B. N. (2019). Motif, Dampak Psikologis, Dan Dukungan Pada Korban Perdagangan Manusia Di Nusa Tenggara Timur. *Jurnal Psikologi Ulayat*, 6, 83–101.
- Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, 105(January), 102248. Retrieved from <https://linkinghub.elsevier.com/retrieve/pii/S0167404821000729>
- Mediana. (2024). Kemenkominfo Tangani 111 Kasus Kebocoran Data Pribadi Sepanjang 2019-2024. *kompas.id*. Retrieved July 13, 2024, from <https://www.kompas.id>
- Mere, K. (2024). Dampak Penggunaan Digital Learning pada Pendidikan Dasar. *Al-Madrasah: Jurnal Pendidikan Madrasah Ibtidaiyah*, 8(1), 264.
- Nurul, S., Shynta Anggrainy, & Siska Aprelyani. (2022). Faktor-Faktor Yang Mempengaruhi Keamanan Sistem Informasi: Keamanan Informasi, Teknologi Informasi Dan Network

- (Literature Review Sim). *Jurnal Ekonomi Manajemen Sistem Informasi*, 3(5), 564–573.
- Ramadhan, I. H., & Nurnawati, E. K. (2023). Analisis Kesadaran Mahasiswa Terhadap Bahaya Cybercrime Di Media Sosial. *JTKSI (Jurnal Teknologi Komputer dan Sistem Informasi)*, 6(1), 38.
- Sadeli, A. F., & Irawati, I. (2023). Awareness of Personal Data Protection Law in concern to literacy. *Jurnal Kajian Informasi & Perpustakaan*, 11(2), 241.
- 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.
- Sudarsono, B., Nafiati, L., Tentama, F., Arief Ghozali, F., Sulistyawati, Mulasari, S. A., Sukes, T. W., et al. (2023). Pelatihan Berbasis Industri Sebagai Upaya Peningkatan Pemahaman Budaya Kerja Industri Siswa SMK Muhammadiyah 2 Tempel. *Seminar Nasional Penelitian dan Pengabdian kepada Masyarakat*, 5, 232–239.
- Sudarsono, B., Tentama, F., Arief Ghozali, F., Asti Mulasari, S., Wahyuni Sukes, T., Yuliansyah, H., Sulistyawati, et al. (2023). Implementasi Pelatihan Berbasis Industri Untuk Peningkatan Budaya Kerja Industri Siswa SMK Muhammadiyah 2 Tempel. *BERNAS: Jurnal Pengabdian Kepada Masyarakat*, 4(4), 2523–2528. Retrieved from <https://doi.org/10.31949/jb.v4i4.6272>
- Sukes, T. W., Yuliansyah, H., Mulasari, S. A., Sulistyawati, Tentama, F., Ghazali, A. F., Sudarsono, B., et al. (2022). Pelatihan Ketahanan Keluarga dan Konseling Keluarga pada Konselor Keluarga dan Masyarakat di Kalurahan Ngalang, Gedangsari, Gunungkidul. *Seminar Nasional Pengabdian Kepada Masyarakat*, 4, 634–639. Retrieved from <https://ojs.unm.ac.id/semnaslpm/article/view/18284>
- Sulistyawati, Arief Ghozali, F., Asti Mulasari, S., Wahyuni Sukes, T., Yuliansyah, H., Tentama, F., Sudarsono, B., et al. (2022). Pelatihan Pengelolaan Sampah di Kalurahan Murtigading Kecamatan Saden Kabupaten Bantul Daerah Istimewa Yogyakarta. *Seminar Nasional Pengabdian Kepada Masyarakat*, 4, 1282–1290. Retrieved from <https://ojs.unm.ac.id/semnaslpm/article/view/18284>
- Verdinandus Lelu Ngono, & Taufik Hidayat, W. (2019). Pendidikan Di Era Digital. *Jurnal Seminar Nasional Pendidikan*, 628–638. Retrieved from <https://jurnal.univpgri-palembang.ac.id/index.php/prosidingpps/article/view/3093>
- Wisanggenis, S. P. (2020). Ancaman Serius "Ransomware" di Fasilitas Kesehatan. *kompas.id*. Retrieved July 13, 2024, from <https://www.kompas.id>