Efektivitas Edukasi *Cybersecurity* dalam Meningkatkan Pengetahuan Siswa tentang Ancaman Digital pada Siswa Menengah Atas

Hamzah Agung[1*]
[1]*Politeknik Semen Indonesia*
Coresponding: hamzah.agung@polteksi.ac.id*
Submitted: 17-06-2025; Accepted: 07-07-2025; Published: 07-07-2025

ABSTRACT

The rapid development of information and communication technology has increased adolescents' exposure to various digital risks, such as phishing, data misuse, and the risks associated with artificial intelligence (AI) usage. The core issue lies in students' low digital literacy, particularly in recognizing and anticipating these threats. This study aims to examine the effectiveness of cybersecurity education in enhancing the digital knowledge and awareness of students at SMA Muhammadiyah 9 Surabaya within the context of digitalization, social media, and AI. A quantitative approach was employed using a quasi-experimental design (one-group pretest-posttest), involving 30 eleventh- and twelfth-grade students as participants. Data were collected through pretests and posttests and analyzed using SPSS. The results showed statistically significant improvements in all measured aspects: internet knowledge (+4.5), data security (+8.33), phishing link identification (+10), and understanding of AI-related risks (+10.17). These findings suggest that cybersecurity education not only enhances technical understanding but also fosters critical awareness of digital risks previously unrecognized by students. The implications of this study highlight the importance of systematically integrating cybersecurity content into the school curriculum as a long-term strategic measure to develop a digitally literate, critical, and responsible generation in the technological era.

Keywords: Cybersecurity, digital literacy, phishing, data security, artificial intelligence, high school students

ABSTRAK

Pesatnya perkembangan teknologi informasi dan komunikasi telah meningkatkan paparan remaja terhadap berbagai risiko digital, seperti phishing, penyalahgunaan data pribadi, serta risiko penggunaan kecerdasan buatan (AI). Permasalahan utamanya adalah rendahnya literasi digital siswa dalam mengenali dan mengantisipasi ancaman tersebut. Penelitian ini bertujuan untuk mengkaji efektivitas edukasi cybersecurity dalam meningkatkan pengetahuan dan kesadaran digital siswa SMA Muhammadiyah 9 Surabaya dalam konteks digitalisasi, media sosial, dan AI. Pendekatan kuantitatif dengan desain quasi-experiment (one-group pretest-posttest) digunakan dalam penelitian ini, melibatkan 30 siswa kelas XI dan XII sebagai responden. Data diperoleh melalui pretest dan posttest, kemudian dianalisis menggunakan SPSS. Hasil menunjukkan peningkatan yang signifikan secara statistik pada seluruh aspek yang diukur: pengetahuan internet (+4,5), keamanan data (+8,33), identifikasi tautan phishing (+10), dan pemahaman risiko penggunaan AI (+10,17). Temuan ini menunjukkan bahwa edukasi cybersecurity mampu meningkatkan pemahaman teknis sekaligus membentuk kesadaran kritis terhadap risiko digital yang sebelumnya belum disadari siswa. Implikasi dari penelitian ini menunjukkan pentingnya integrasi sistematis materi keamanan siber dalam kurikulum sekolah sebagai langkah strategis jangka panjang untuk membentuk generasi yang cerdas digital, berpikir kritis, dan bertanggung jawab dalam era teknologi.

Kata kunci: Cybersecurity, literasi digital, phishing, keamanan data, kecerdasan buatan, siswa SMA

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi (TIK) yang sangat pesat telah membawa perubahan besar dalam berbagai aspek kehidupan, termasuk pendidikan, sosial, dan ekonomi [1]. Teknologi digital seperti media sosial, kecerdasan buatan (AI), dan internet of things (IoT) kini semakin mudah diakses oleh masyarakat luas, termasuk oleh kalangan remaja [2]. Di Indonesia, menurut laporan Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) tahun 2023, tingkat penetrasi internet telah mencapai lebih dari 77% dari total populasi [3]. Meskipun kemajuan ini memberikan berbagai manfaat, di sisi lain, masyarakat juga dihadapkan pada tantangan serius berupa meningkatnya ancaman keamanan siber, seperti phishing, data breach, peretasan akun, penyebaran malware, dan bentuk-bentuk kejahatan digital lainnya yang semakin kompleks [4].

Fenomena ini sangat relevan dengan kondisi pelajar di tingkat sekolah menengah atas (SMA), yang merupakan kelompok pengguna internet paling aktif [5]. Berdasarkan hasil Survei Sosial Ekonomi Nasional

(Susenas) oleh Badan Pusat Statistik (BPS) pada Maret 2023, sebanyak 94,16% anak muda Indonesia usia 16–30 tahun pernah mengakses internet dalam tiga bulan terakhir, dengan 84,37% di antaranya menggunakan internet untuk mengakses media sosial .Di samping itu, laporan *State of Mobile 2023* oleh data.ai menunjukkan bahwa rata-rata masyarakat Indonesia menghabiskan sekitar 5,7 jam per hari menggunakan internet pada tahun 2022 [6]. Namun demikian, tingginya intensitas penggunaan ini tidak diiringi dengan pemahaman yang memadai mengenai praktik keamanan digital [7]. Banyak siswa masih belum menyadari bahaya membagikan informasi pribadi secara sembarangan, jarang menggunakan autentikasi dua faktor, dan mudah terjebak oleh tautan palsu atau konten menyesatkan [8], [9], [10] . Hal ini membuat mereka sangat rentan terhadap berbagai bentuk kejahatan digital [11]. Beberapa bentuk kejahatan digital yang sering menimpa pelajar antara lain peretasan akun media sosial, penyebaran konten pribadi tanpa izin, serta pencurian identitas digital [12]. Data dari Badan Siber dan Sandi Negara (BSSN) menunjukkan bahwa sepanjang tahun 2022, terjadi lebih dari 403 juta serangan siber di Indonesia [13]. Dari jumlah tersebut, lebih dari 20% korbannya adalah remaja dan pelajar [14]. Selain itu, laporan UNICEF mengungkapkan bahwa 45% remaja di Indonesia pernah mengalami perundungan siber *(cyberbullying)* [15]. Fakta-fakta ini menegaskan bahwa pelajar merupakan kelompok yang sangat rentan terhadap bahaya di ruang digital [16].

Untuk menjawab tantangan tersebut, edukasi keamanan siber atau *cybersecurity* menjadi elemen penting dalam literasi digital abad ke-21 [17]. Edukasi ini tidak hanya bertujuan untuk meningkatkan pemahaman teknis, tetapi juga membentuk kesadaran kritis serta sikap bertanggung jawab dalam berinteraksi di dunia maya [18]. Melalui pembelajaran formal di sekolah maupun pendekatan non-formal seperti pelatihan dan kampanye digital, siswa dapat dibekali dengan kemampuan untuk mengenali ancaman digital, melindungi informasi pribadi, dan menyaring informasi secara bijak [19]. Oleh karena itu, edukasi *cybersecurity* berperan sebagai langkah preventif yang penting dalam melindungi siswa dari risiko dunia digital [20].

Dalam konteks ini, sekolah memiliki tanggung jawab yang besar dalam membekali siswanya dengan keterampilan digital yang aman dan etis [21]. Peran sekolah tidak hanya terbatas pada penyampaian materi akademis, tetapi juga mencakup pembentukan karakter dan pengembangan keterampilan hidup yang sesuai dengan tuntutan zaman [22]. Kurikulum yang mengintegrasikan materi tentang keamanan akun, perlindungan data pribadi, etika digital, serta pemahaman terhadap modus-modus kejahatan siber akan sangat membantu siswa dalam membentuk kesadaran digital yang kuat [23]. Kolaborasi antara pihak sekolah, orang tua, dan instansi teknologi juga menjadi elemen penting dalam menciptakan lingkungan belajar yang aman secara digital [24].

SMA Muhammadiyah 9 Surabaya merupakan salah satu institusi pendidikan yang menunjukkan kepedulian terhadap isu keamanan digital melalui berbagai program edukatif dan penerapan teknologi dalam kegiatan belajar mengajar. Meskipun demikian, efektivitas edukasi *cyber security* yang telah diberikan kepada siswa masih perlu dikaji lebih dalam. Penelitian ini diarahkan untuk mengidentifikasi sejauh mana peran edukasi tersebut dalam membentuk perilaku aman digital siswa, khususnya dalam konteks penggunaan internet dan media sosial secara bijak dan bertanggung jawab. Hal ini penting untuk memahami dampak nyata dari intervensi pendidikan yang telah dilakukan oleh pihak sekolah.

Berdasarkan penelitian sebelumnya, penulis tertarik dengan topic ini, jadi penelitian ini bertujuan untuk mengetahui kontribusi konkret dari edukasi cybersecurity terhadap peningkatan kesadaran dan perilaku aman digital di kalangan siswa SMA Muhammadiyah 9 Surabaya. Melalui pendekatan kualitatif dan kuantitatif, diharapkan penelitian ini dapat mengungkap keterkaitan antara tingkat pemahaman siswa mengenai keamanan digital dengan tindakan nyata yang mereka lakukan dalam aktivitas daring sehari-hari. Temuan penelitian ini juga dapat menjadi dasar evaluasi terhadap strategi pembelajaran yang sudah diterapkan, serta memberikan masukan untuk perbaikan di masa mendatang.

Penelitian ini juga diharapkan dapat memberikan kontribusi ilmiah dalam pengembangan literasi digital di bidang keamanan siber, khususnya di tingkat pendidikan menengah. Hasil dari studi ini dapat dijadikan landasan dalam perumusan kurikulum atau program literasi digital yang lebih relevan, sistematis, dan kontekstual. Selain itu, penelitian ini juga diharapkan dapat meningkatkan kesadaran akan pentingnya perlindungan data dan

etika digital, sehingga siswa tidak hanya menjadi pengguna teknologi yang aktif, tetapi juga cerdas, kritis, dan bertanggung jawab dalam menghadapi tantangan dunia digital yang terus berkembang.

2. METODE PENELITIAN

Desain Penelitian

Penelitian ini menggunakan pendekatan kuantitatif dengan jenis eksperimen semu (quasi experiment) dalam bentuk desain one-group pretest-posttest desain [25]. Pendekatan ini dipilih karena bertujuan untuk mengetahui pengaruh suatu perlakuan, yaitu edukasi cybersecurity, terhadap perubahan tingkat pengetahuan siswa sebelum dan sesudah diberikan perlakuan tersebut [26]. Dalam desain ini, satu kelompok siswa akan diberikan tes awal (pretest), kemudian diberikan intervensi berupa materi edukasi cybersecurity, dan selanjutnya dilakukan tes akhir (posttest) untuk melihat perubahannya. Metode kuantitatif digunakan karena penelitian ini bersifat objektif, sistematis, dan terukur. Dengan menggunakan pendekatan ini, peneliti dapat memperoleh data numerik yang dapat diolah secara statistik untuk mengetahui signifikansi perubahan tingkat pengetahuan siswa terhadap tiga aspek utama yang menjadi variabel dependen dalam penelitian ini, yaitu: Digitalisasi (Y1) Media Sosial (Y2) Kecerdasan Buatan (Artificial Intelligence / AI) (Y3) Sedangkan variabel independennya adalah edukasi cybersecurity (X) yang diberikan melalui materi pembelajaran interaktif yang dirancang untuk membekali siswa dengan pemahaman terkait keamanan digital, perlindungan data pribadi, ancaman siber, dan etika penggunaan teknologi.

Populasi dan Sampel

Populasi dalam penelitian ini adalah seluruh siswa kelas X dan XI di SMA Muhammadiyah 9 Surabaya yang berada dalam rentang usia 15 hingga 17 tahun. Populasi ini dipilih karena sesuai dengan karakteristik pengguna aktif internet dan media sosial di kalangan remaja, serta rentan terhadap ancaman dunia digital, sebagaimana telah dijelaskan pada bab sebelumnya. Sampel penelitian terdiri dari 30 siswa, yang terdiri atas: 15 siswa laki-laki, dan 15 siswa perempuan. Teknik pengambilan sampel menggunakan purposive sampling, yaitu teknik penentuan sampel berdasarkan kriteria tertentu yang relevan dengan tujuan penelitian [27]. Adapun kriteria pemilihan sampel meliputi: Siswa kelas XI dan XII, Usia antara 15–17 tahun, Bersedia mengikuti seluruh rangkaian kegiatan penelitian (pretest, pemberian materi, dan posttest), Mewakili perbandingan jenis kelamin secara seimbang. Pemilihan sampel secara purposive ini dimaksudkan agar hasil penelitian dapat merepresentasikan kelompok remaja usia sekolah yang aktif menggunakan teknologi digital dan media sosial dalam kehidupan sehari-hari.

Teknik Pengumpulan Data

Data penelitian dikumpulkan melalui tes tertulis, yang terdiri dari dua tahap: Pretest dilakukan sebelum penyampaian materi edukasi cybersecurity untuk mengukur pengetahuan awal siswa. Posttest dilakukan setelah kegiatan edukasi untuk melihat peningkatan pemahaman setelah intervensi dilakukan. Soal pretest dan posttest disusun berdasarkan indikator dari tiga variabel dependen (digitalisasi, media sosial, dan AI) yang dikaitkan dengan konsep-konsep dasar dalam edukasi cybersecurity

Teknik Analisis Data

Teknik analisis data dalam penelitian ini bertujuan untuk mengukur perbedaan tingkat pengetahuan siswa sebelum dan sesudah diberikan edukasi mengenai cybersecurity, serta menganalisis peningkatan pemahaman terhadap tiga variabel dependen yaitu digitalisasi, media sosial, dan kecerdasan buatan (AI). Data yang diperoleh dari hasil pretest dan posttest dianalisis menggunakan bantuan perangkat lunak dengan metode uji t berpasangan dan analisa regresi linar berganda untuk menilai dampak pelatihan pada peningkatan pengetahuan dan pemahaman terhadap cybersecurity.

3. HASIL DAN PEMBAHASAN

Hasil

Karakteristik Responden

Karakteristik responden di SMA Muhammadiyah 9 Surabaya dirinci pada Tabel 1, dengan rentang usia 16 sampai 18 tahun, duduk di kelas XI dan XII, terdiri dari siswa berjumlah 15 orang, siswi 15 orang

Tabel 1 karakteristik Responden *(Karakteristik Responden (n = 30)*

Karakteristik	N	%
Jenis Kelamin		
Laki - Laki	15	50
Perempuan	15	50
Kelas		
X	15	50
XI	15	50
Usia		
16	13	43
17	15	50
18	2	7
Total	30	100

Tabel 1 menunjukkan bahwa 50% karakteristik responden laki-laki dan petempuan, kelas X dan XI, sedangkan untuk kelompok usia diwakili oleh kelompok usia 17 tahun. Selain itu, terdapat kelompok usia 16 tahun dan 18 tahun, yang masing-masing mencakup 43% dan 7 % dari total responden.

Pengetahuan internet

Hasil pre-test dan post-test untuk mengukur perubahan pengetahuan internet, dan peningkatan pemahaman internet responden yang mencakup digitalisasi, media sosial, dan kecerdasan buatan (AI) terhadap cybersecurity, Hasil statistic yang diperoleh dari data pra-tes dan pasca-tes disajikan dalam tabel 2.

Tabel 2 Pengetahuan internet

Paired Samples Statistics

		Mean	N	Std. Deviation	Std. Error Mean
Pair 1	Pre-test	17.5000	30	3.41144	.62284
	Post-test	22.0000	30	2.81621	.51417

Data diatas menunjukkan data perbandingan pengetahuan internet. Nilai rata-rata (mean) antara pretest dan posttest dari 30 siswa yang menjadi responden. Nilai rata-rata pretest sebelum diberikan edukasi cybersecurity adalah 17,5 dengan standar deviasi sebesar 3,41. Setelah pelaksanaan edukasi, nilai rata-rata posttest meningkat menjadi 22,0 dengan standar deviasi 2,82. Peningkatan sebesar 4,5 poin ini menunjukkan adanya perbedaan dalam pemahaman siswa setelah mengikuti kegiatan edukasi. Dari sisi statistik, standar deviasi yang lebih kecil pada posttest (2,82) dibandingkan pre-test (3,41) menunjukkan bahwa hasil posttest siswa lebih seragam atau konsisten. Selain itu, nilai standard error mean yang kecil pada post-test (0,51417) juga menunjukkan bahwa nilai rata-rata tersebut cukup representatif terhadap populasi siswa yang diteliti.

Tabel 3 Keamanan data

Paired Samples Statistics

		Mean	N	Std. Deviation	Std. Error Mean
Pair 1	pretest	11.5000	30	3.97188	.72516
	posttest	19.8333	30	2.78027	.50760

Berdasarkan hasil pretest dan posttest terhadap 30 siswa SMA Muhammadiyah 9 Surabaya pada aspek keamanan data, terjadi peningkatan nilai rata-rata yang cukup signifikan. Nilai rata-rata pretest berada pada angka 11,5, sedangkan nilai rata-rata posttest meningkat menjadi 19,83. Peningkatan sebesar 8,33 poin ini menunjukkan bahwa pemahaman siswa terhadap isu-isu keamanan data meningkat setelah mengikuti sesi edukasi cybersecurity. Selain itu, standar deviasi menurun dari 3,97 pada pretest menjadi 2,78 pada posttest, yang berarti variasi nilai siswa semakin kecil dan pemahaman mereka menjadi lebih merata. Nilai standard error mean juga menurun dari 0,72 menjadi 0,50, mengindikasikan bahwa hasil posttest lebih representatif terhadap populasi siswa.

Tabel 4 Link Phising

Paired Samples Statistics

		Mean	N	Std. Deviation	Std. Error Mean
Pair 1	pretest	10.0000	30	7.19195	1.31306
	posttest	20.0000	30	3.93919	.71919

Hasil analisis pretest dan posttest pada aspek pengetahuan tentang link phishing menunjukkan adanya peningkatan yang sangat signifikan. Nilai rata-rata pretest berada pada angka 10,00, sementara nilai rata-rata posttest meningkat menjadi 20,00. Artinya, terdapat kenaikan sebesar 10 poin setelah siswa mengikuti sesi edukasi cybersecurity. Selain itu, standar deviasi menurun dari 7,19 pada pretest menjadi 3,93 pada posttest, yang menunjukkan bahwa hasil posttest siswa lebih terpusat dan seragam. Nilai Standard Error Mean juga berkurang dari 1,31 menjadi 0,71, menandakan bahwa nilai posttest lebih stabil dan representatif terhadap populasi siswa.

Tabel 5 Bahaya AI

Paired Samples Statistics

		Mean	N	Std. Deviation	Std. Error Mean
Pair 1	pretest	10.6667	30	5.97889	1.09159
	posttest	20.8333	30	3.73320	.68159

Data hasil pretest dan posttest pada aspek pemahaman tentang bahaya kecerdasan buatan (AI) menunjukkan peningkatan yang signifikan. Nilai rata-rata pretest berada pada angka 10,67, sedangkan nilai rata-rata posttest meningkat menjadi 20,83. Artinya, terjadi kenaikan sebesar 10,17 poin setelah siswa mendapatkan edukasi cybersecurity. Selain itu, standar deviasi menurun dari 5,97 menjadi 3,73, menandakan bahwa hasil posttest siswa lebih homogen. Penurunan nilai Standard Error Mean dari 1,09 menjadi 0,68 memperkuat bahwa hasil posttest lebih stabil dan representatif terhadap populasi.Keterangan pada tabel diberikan di atas tabel.

Pembahasan

Era digitalisasi yang berkembang pesat saat ini tidak dapat dipisahkan dari keberadaan sosial media dan kecerdasan buatan (Artificial Intelligence/AI). Dalam konteks pendidikan dan literasi digital, terdapat empat komponen penting yang menjadi fokus utama dalam edukasi cybersecurity, yaitu: Pengetahuan Internet: Pemahaman dasar tentang cara kerja internet, penggunaan layanan daring secara aman, serta etika digital. Keamanan Data: Kesadaran akan pentingnya menjaga privasi dan perlindungan data pribadi dari penyalahgunaan. Link Phising: Pengetahuan tentang modus penipuan daring melalui tautan palsu yang bertujuan mencuri data pengguna. Bahaya AI: Pemahaman akan potensi risiko penggunaan AI, seperti penyebaran hoaks melalui deepfake, manipulasi data, dan pelanggaran etika digital. Keempat komponen tersebut menjadi landasan penting dalam membangun kesadaran cybersecurity bagi para siswa, terutama di jenjang SMA.

Dimulai dari yang pertama adalah pengetahuan internet. Berdasarkan hasil pretest dan posttest yang dilakukan terhadap 30 siswa, terdapat peningkatan nilai rata-rata dari 17,5 menjadi 22,0 dalam aspek pengetahuan internet. Peningkatan ini mencerminkan bahwa edukasi cybersecurity memberikan kontribusi terhadap peningkatan pemahaman siswa mengenai penggunaan internet yang aman. Namun, jika dilihat lebih dalam, selisih skor sebesar 4,5 poin tidak terlalu besar dan dapat dikatakan bahwa peningkatannya tidak terlalu signifikan secara substansial. Hal ini disebabkan oleh fakta bahwa sebagian besar siswa sudah memiliki pengetahuan dasar tentang internet sebelum mengikuti pelatihan. Dalam era digital saat ini, siswa pada umumnya telah terbiasa menggunakan internet, baik untuk keperluan belajar, hiburan, maupun komunikasi. Mereka telah akrab dengan layanan digital seperti mesin pencari, media sosial, dan aplikasi pembelajaran daring, sehingga materi dasar tentang pengetahuan internet tidak sepenuhnya baru bagi mereka. Dari pembahasan ini sejalan dengan penelitian [28], di tingkat sekolah menengah atas banyak siswa telah mengenal dasar penggunaan perangkat dan aplikasi digital, dan penggunaan internet, meskipun kemampuan pemahaman keamanan digital masih sangat terbatas

Setelah itu di aspek kemanan data, peningkatan rata-rata skor sebesar 8,33 poin dari pretest ke posttest menunjukkan bahwa edukasi mengenai keamanan data berdampak besar terhadap pemahaman siswa. Kenaikan ini tidak hanya menunjukkan efektivitas materi yang disampaikan, tetapi juga mencerminkan bahwa sebagian besar siswa sebelumnya belum memiliki pengetahuan yang memadai tentang cara melindungi data pribadi mereka di dunia digital. Dibandingkan dengan aspek pengetahuan internet yang hanya meningkat sebesar 4,5 poin, peningkatan dalam aspek keamanan data terlihat lebih signifikan, baik secara kuantitatif maupun secara substansial. Hal ini mengindikasikan bahwa materi keamanan data membuka wawasan baru bagi siswa terhadap ancaman digital yang sebelumnya belum mereka sadari secara utuh. Dalam aspek ini pembahasanya sejalan dengan penelitian dari [29], menjelaskan bahwa setelah penyisipan topik keamanan digital ke dalam kurikulum formal, ditemukan peningkatan signifikan untuk 11 dari 14 topik literasi siber, yang menunjukkan bahwa peserta sebelumnya tidak memiliki pemahaman utuh terhadap ancaman digital tertentu. Penelitian ini menunjukkan bahwa strategi integrasi materi keamanan tidak hanya sebagai topik tambahan tetapi sebagai bagian kurikulum rutin efektif membuka kesadaran siswa terhadap risiko-risiko yang sebelumnya tidak mereka kenali atau pahami sepenuhnya.

Materi yang diberikan mencakup konsep-konsep mendasar seperti Single Sign-On (SSO), yang memperkenalkan cara mengakses berbagai layanan digital hanya dengan satu akun. Siswa memahami bahwa meskipun SSO praktis, ia menyimpan risiko besar apabila akun utama diretas. Selain itu, mereka mempelajari pentingnya Two-Factor Authentication (2FA) sebagai lapisan keamanan tambahan yang dapat melindungi akun dari akses tidak sah, terutama saat sandi berhasil ditebak atau dicuri. Pengelolaan kata sandi juga menjadi sorotan utama; siswa dibimbing untuk membuat password yang kuat dan unik serta disarankan menggunakan password manager agar tidak lupa dan tetap aman.

Salah satu poin yang paling membuka kesadaran siswa adalah topik mengenai oversharing di media sosial. Sebagian besar dari mereka terbiasa membagikan informasi pribadi seperti tanggal lahir, lokasi, hingga aktivitas harian tanpa menyadari potensi bahayanya. Melalui diskusi dan simulasi, siswa memahami bahwa informasi-informasi tersebut dapat dimanfaatkan untuk keperluan phising, social engineering, atau bahkan

pencurian identitas. Edukasi ini membantu mereka lebih kritis dan bijak dalam membagikan informasi secara daring.

Dalam aspek link phising, Peningkatan pengetahuan siswa terhadap link phishing tergolong sangat signifikan, yang ditunjukkan oleh kenaikan rata-rata skor dari 10,00 pada pretest menjadi 20,00 pada posttest. Selisih nilai sebesar 10 poin penuh mencerminkan adanya lonjakan pemahaman yang kuat setelah siswa mengikuti edukasi cybersecurity. Pada tahap awal (pretest), nilai rata-rata yang rendah menunjukkan bahwa sebagian besar siswa belum memahami sama sekali apa itu link phishing. Banyak dari mereka belum dapat membedakan antara tautan resmi dan tautan palsu, serta tidak menyadari bahwa kejahatan digital bisa datang dalam bentuk pesan atau email yang tampak terpercaya. Hasil penelitian ini sejalan dengan temuan dari [30], yang menyatakan bahwa tingkat literasi keamanan digital di kalangan pelajar SMA masih tergolong rendah, terutama dalam hal mengenali ancaman seperti phishing dan pengelolaan data pribadi.

Edukasi yang diberikan mencakup penjelasan menyeluruh tentang definisi link phishing, karakteristik umum tautan berbahaya, serta teknik yang biasa digunakan oleh pelaku kejahatan siber, seperti peniruan domain, pesan mendesak, dan rekayasa sosial (social engineering). Para siswa diberi contoh-contoh nyata dari bentuk phishing yang biasa ditemui dalam kehidupan sehari-hari, seperti tautan hadiah palsu, notifikasi akun yang dinonaktifkan, atau halaman login cybercampus/Siakad. Selain itu, penurunan standar deviasi dari 7,19 menjadi 3,93 menunjukkan bahwa setelah pelatihan, jawaban siswa menjadi lebih seragam dan konsisten menandakan bahwa materi telah dipahami secara merata oleh sebagian besar peserta.

Hal ini juga didukung oleh penurunan standard error mean dari 1,31 ke 0,72, yang memperkuat kesimpulan bahwa nilai rata-rata posttest lebih representatif terhadap keseluruhan populasi siswa. Dengan latar belakang bahwa pada awalnya siswa sangat minim pengetahuan tentang phishing, peningkatan drastis ini menegaskan keberhasilan program edukasi dalam menjawab kesenjangan pengetahuan yang ada. Materi tidak hanya menambah informasi, tetapi juga memberikan kesadaran baru kepada siswa agar lebih berhati-hati dan kritis dalam berinteraksi dengan tautan digital. Hal ini sangat penting mengingat mereka adalah generasi digital yang rentan menjadi target serangan siber jika tidak memiliki literasi keamanan yang memadai.

Pada pembahasan terakhir yaitu bahaya penggunaan AI. Peningkatan nilai rata-rata dari 10,67 menjadi 20,83 mencerminkan bahwa pemahaman siswa terhadap potensi bahaya AI meningkat secara sangat signifikan. Hal ini dapat dimaklumi karena pada tahap awal (pretest), sebagian besar siswa belum menyadari bahwa AI dapat menjadi ancaman serius, terutama dalam hal pengumpulan dan penyalahgunaan data pribadi. Mereka umumnya melihat AI hanya sebagai alat bantu teknologi seperti chatbot, aplikasi edit gambar, atau rekomendasi konten, tanpa memahami bagaimana teknologi ini bekerja di balik layar. Materi edukasi yang disampaikan dalam sesi ini membuka wawasan siswa mengenai bagaimana AI dapat mengumpulkan, menyimpan, dan menggunakan ulang data pribadi mereka, terutama data yang dibagikan secara sukarela di internet. Salah satu contoh yang ditekankan dalam pelatihan adalah bahaya mengunggah foto ke platform berbasis AI tanpa mengetahui ketentuan penggunaan data. Sama halnya dengan penelitian [31], menegaskan bahwa banyak pengguna, termasuk generasi muda, tidak memahami sepenuhnya cara kerja algoritma AI, terutama dalam proses pengambilan dan penyimpanan data personal, sehingga menimbulkan risiko terhadap privasi dan etika digital.

Banyak platform AI menyimpan foto atau informasi yang diunggah dan menggunakannya kembali dalam pelatihan model tanpa persetujuan jelas dari pengguna. Hal ini dapat menyebabkan risiko privasi yang besar, terutama jika data tersebut dapat dicari atau dimanfaatkan oleh pihak yang tidak bertanggung jawab. Peningkatan yang signifikan ini terjadi karena siswa sebelumnya tidak memiliki pemahaman yang cukup mengenai sisi gelap AI. Mereka baru menyadari bahwa teknologi ini, jika tidak digunakan dengan bijak, justru bisa menjadi alat yang membahayakan keamanan data pribadi mereka sendiri. Edukasi ini berhasil menanamkan kesadaran baru bahwa teknologi canggih seperti AI tidak hanya membawa manfaat, tetapi juga harus diimbangi dengan literasi keamanan dan etika digital yang kuat, khususnya dalam hal perlindungan data dan privasi. Hal serupa juga disetujui oleh penelitian dari [32], menyoroti bahwa banyak pengguna muda merasa minimnya kontrol terhadap data pribadi mereka dan takut terhadap potensi penyalahgunaan oleh sistem AI, terutama terkait pengumpulan data tanpa transparansi yang memadai.

Setelah melihat dari ke empat pembahasan yang telah dipaparkan, dapat disimpulkan bahwa edukasi cybersecurity memberikan dampak positif dalam meningkatkan pengetahuan siswa di SMA Muhammadiyah 9 Surabaya mengenai empat komponen utama literasi digital, yaitu pengetahuan internet, keamanan data, link phishing, dan bahaya AI. Dari keempat aspek tersebut, peningkatan yang paling signifikan terjadi pada aspek link phishing, dengan selisih rata-rata nilai sebesar 10 poin. Hal ini menunjukkan bahwa siswa sebelumnya tidak familiar dengan konsep phishing dan belum memahami bahwa tautan mencurigakan dapat menjadi sarana utama serangan siber. Peningkatan signifikan kedua terjadi pada aspek bahaya AI, karena pada awalnya siswa tidak menyadari bahwa teknologi AI dapat menyimpan, menggunakan ulang, bahkan menyalahgunakan data pribadi mereka, termasuk foto atau informasi yang mereka unggah. Mereka cenderung menggunakan AI hanya sebagai alat bantu tanpa mempertimbangkan sisi keamanannya. Kedua hasil ini menunjukkan bahwa edukasi cybersecurity tidak hanya menambah pengetahuan teknis, tetapi juga membentuk kesadaran baru akan risiko digital yang selama ini luput dari perhatian siswa. Dengan demikian, kegiatan edukasi ini sangat penting untuk diterapkan secara berkelanjutan dalam membangun generasi yang melek digital dan sadar akan keamanan siber.

KESIMPULAN

Berdasarkan hasil penelitian, dapat disimpulkan bahwa edukasi cybersecurity berperan penting dalam meningkatkan pengetahuan dan kesadaran siswa terhadap berbagai aspek keamanan digital di era modern. Keempat komponen utama yang menjadi fokus, yaitu pengetahuan internet, keamanan data, link phishing, dan bahaya AI, semuanya menunjukkan adanya peningkatan pemahaman setelah siswa mengikuti sesi edukasi. Peningkatan tertinggi terjadi pada aspek link phishing, yang naik sebesar 10 poin, dan bahaya AI yang meningkat sebesar 10,17 poin. Hal ini menunjukkan bahwa siswa sebelumnya tidak familiar dengan konsep phishing dan tidak menyadari risiko serius yang ditimbulkan oleh penggunaan teknologi AI tanpa pemahaman yang memadai. Edukasi yang diberikan berhasil menjembatani kesenjangan pengetahuan ini dengan memberikan wawasan yang jelas dan aplikatif. Dengan meningkatnya kesadaran siswa terhadap risiko digital, termasuk pentingnya menjaga data pribadi, menghindari tautan palsu, serta berhati-hati dalam menggunakan teknologi berbasis AI, maka kegiatan edukasi seperti ini perlu dilakukan secara rutin dan terstruktur. Pengetahuan teknis saja tidak cukup; siswa juga perlu dibekali dengan sikap kritis dan etika digital agar dapat menjadi pengguna teknologi yang bertanggung jawab. Hasil penelitian ini menjadi dasar kuat bagi sekolah untuk mengintegrasikan materi keamanan digital dalam kurikulum, sekaligus menjadi rekomendasi bagi institusi pendidikan lainnya agar lebih proaktif dalam menghadapi tantangan dunia digital yang semakin kompleks dan berisiko tinggi.

DAFTAR PUSTAKA

[1] G. M. Fricticarani, A., Hayati, A., Hoirunisa, I., & Rosdalina, "Strategi pendidikan untuk sukses di era teknologi 5.0," *J. Inov. Pendidik. Dan Teknol. Inf.*, vol. 4, no. 1, pp. 56–68, 2023, doi: 10.52060/pti.v4i1.1173.

[2] A. Nawanti, R. D., Santoso, W. T., Sumardjoko, B., & Fathoni, "Transformasi Kepemimpinan Pendidikan Era Disrupsi," *Didakt. J. Kependidikan*, vol. 13, no. 2, pp. 2599–2606, 2024, doi: 10.58230/27454312.618.

[3] S. Muhafilah, I., & Suwarningsih, "Durasi penggunaan media sosial dan tingkat stres dengan kualitas tidur pada remaja," *J. Ilmu Kesehat. Masy.*, vol. 12, no. 5, pp. 346–351, 2023, doi: 10.33221/jikm.v12i05.2076.

[4] H. Kurniarullah, M. R., Nabila, T., Khalidy, A., Tan, V. J., & Widiyani, "Tinjauan kriminologi terhadap penyalahgunaan artificial intelligence: Deepfake pornografi dan pencurian data pribadi," *J. Ilm. Wahana Pendidik.*, vol. 10, no. 10, pp. 534–547, 2024, doi: 10.5281/zenodo.11448814.

[5] M. F. Zein, *Panduan Menggunakan Media Sosial untuk Generasi Emas Milenial*. 2019.

[6] D. T. Hunaifi, "Analisis Tren Penggunaan Filter Digital pada Pengguna Media Sosial Instagram di Indonesia," *Al Qalam J. Ilm. Keagamaan dan Kemasyarakatan*, vol. 17, no. 6, pp. 4541–4558, 2023, doi: 10.35931/aq.v17i6.2831.

[7] M. Hanifah, R., Fuadi, F., Wigati, M., Wilantika, R., Agustina, F. F., Syaifussalam, M. L., ... & Ardiyansah, "Sosialisasi Bina Medsos (Bijak Gunakan Media Sosial) Pada Siswa SMK," *J. Pengabdi. Kpd. Masy. Nusant.*, vol. 5, no. 2, pp. 1810–1816, 2024, doi: 10.55338/jpkmn.v5i2.3092.

[8] M. Tahir, M. A., & Safrin, "Peningkatan Kesadaran Hukum dalam Transaksi Online di MAN 2 Palu melalui Penyuluhan Hukum," *J. Abdi Masy. Indones.*, vol. 5, no. 2, pp. 695–702, 2025, doi: 10.54082/jamsi.1537.
[9] O. P. Nisa, K., & Handayani, "Peningkatan Literasi Digital: Edukasi Kejahatan Siber Dan Pinjaman Online Illegal MAN 2 Cilacap," *J. Pengabdi. Masyarakat-PIMAS*, vol. 4, no. 2, pp. 61–68, 2025, doi: 10.35960/pimas.v4i2.1831.
[10] A. Ananta, K. D., Ambodo, T., & Tohawi, "Pengaruh Media Sosial terhadap Peningkatan Kejahatan Siber di Indonesia," *Islam. Law J. Siyasah*, vol. 9, no. 2, pp. 118–131, 2024, doi: 10.53429/iljs.v9i2.858.
[11] S. Laksana, T. G., & Mulyani, "Pengetahuan dasar identifikasi dini deteksi serangan kejahatan siber untuk mencegah pembobolan data perusahaan," *J. Ilm. Multidisiplin*, vol. 3, no. 1, pp. 109–122, 2024, doi: 10.56127/jukim.v3i01.1143.
[12] K. Rizkiyanto, E., Sudewo, F. A., & Rizkianto, *Penegakan Hukum Terhadap Tindak Pidana Cyberbullying melalui Media Elektronik*. Penerbit NEM, 2024.
[13] B. A. Indradjaja, M. A. P., Suseno, S., & Atmaja, "Implementasi Penyidikan Terhadap Tindak Pidana Siber Dalam Perspektif Perbandingan Hukum: Indonesia dan Inggris Raya," *J. Ilm. Penegakan Huk.*, vol. 11, no. 2, pp. 162–172, 2024, doi: 10.31289/jiph.v11i2.12931.
[14] R. Rastati, *Bentuk perundungan siber di media sosial dan pencegahannya bagi korban dan pelaku*. Bandung Institute of Technology, 2016.
[15] N. Rahmadani, T. A., & Harahap, "Dampak Cyberbullying di Media Sosial pada Perilaku Reaktif Remaja di Desa Sei Rotan," *J. Noken Ilmu-Ilmu Sos.*, vol. 8, no. 2, pp. 214–227, 2023, doi: 10.33506/jn.v8i2.2372.
[16] R. F. Ruimassa, A. A., & Nanuru, "Gereja dan cyberbullying remaja: Pendampingan pastoral bagi remaja korban cyberbullying," *KURIOS*, vol. 9, no. 3, pp. 702–714, 2023, doi: 10.30995/kur.v9i3.843.
[17] M. S. Waliulu, Y. S., Sos, S., Kom, M. I., Arif, H. M., Mokoginta, D., Novita, R., ... & Iswahyudi, *Pendidikan Dalam Transformasi Digital*. Cendikia Mulia Mandiri, 2023.
[18] W. D. Melina, M., Admiral, A., & Sari, "Penguatan Literasi Digital Remaja melalui Program Penyuluhan Dampak Media Sosial di SMK Multi Mekanik Masmur," *Room Civ. Soc. Dev.*, vol. 4, no. 2, pp. 351–358, 2025, doi: 10.59110/rcsd.534.
[19] A. Moeins, I. H. A., Alhempi, R. R., & Lukas, *Strategi Penguatan Kinerja Generasi Z Dalam Menghadapi Indonesia Emas 2045*. Takaza Innovatix Labs, 2024.
[20] A. Novita, D., Mulyono, M., & Retnowati, "Perkembangan Hukum Siber di Indonesia: Studi Literatur tentang Tantangan dan Solusi Keamanan Nasional," *Innov. J. Soc. Sci. Res.*, vol. 4, no. 6, pp. 1179–1186, 2024, doi: 10.31004/innovative.v4i6.16144.
[21] A. A. B. Muslimin, T. P., & Fatimah, "Kompetensi dan kesiapan guru sekolah dasar terhadap tantangan pendidikan di Era Society 5.0," *Cokroaminoto J. Prim. Educ.*, vol. 7, no. 1, pp. 55–72, 2024, doi: 10.30605/cjpe.712024.3589.
[22] D. P. S. Gumilar, G., & Rosid, "PERANAN SUPERVISI DALAM MENINGKATKAN KUALITAS PEMBELAJARAN BERKELANJUTAN," *J. Ilm. Pendidik. Citra Bakti*, vol. 11, no. 3, pp. 651–661, 2024, doi: 10.38048/jipcb.v11i3.3189.
[23] K. Iskandar, I., Putra, D. D., Yasin, A. I., & Khairan, *Cyber Smart Campus: Cakap Digital & Aman Siber*. PT. Sonpedia Publishing Indonesia, 2025.
[24] N. W. Oktaviana, M., Prasetya, D. D., & Siswijayanti, "PENCEGAHAN PERUNDUNGAN DARING BAGI PESERTA DIDIK TINGKAT SEKOLAH MENENGAH PERTAMA (SMP)," *J. Ekon. Bisnis dan Pendidik.*, vol. 4, no. 1, pp. 2–8, 2024, doi: 10.17977/um066v4i12024p2.
[25] J. W. Creswell, *Research design: pendekatan kualitatif, kuantitatif, dan mixed*. 2012.
[26] A. H. Aini, N., Fatmaningrum, W., & Yusuf, "Upaya meningkatkan perilaku pasien dalam tatalaksana diabetes mellitus dengan pendekatan teori model behavioral system Dorothy E. Johnson," *J. Ners*, vol. 6, no. 1, pp. 1–10, 2011.
[27] A. Nayazik, "Pembentukan keterampilan pemecahan masalah melalui model IDEAL problem solving dengan teori pemrosesan informasi," *Kreano, J. Mat. Kreat.*, vol. 8, no. 2, pp. 182–190, 2017, doi: 10.15294/kreano.v8i2.7163.
[28] H. Hermansyah *et al.*, "Transformasi Administrasi Perkantoran melalui Literasi Digital: Pelatihan dan Penerapan Teknologi untuk Siswa SMK Muhammadiyah Kadungora," *Badranaya J. Pengabdi. Kpd. Masy.*, vol. 2, no. 02, pp. 54–62, Dec. 2024, doi: 10.31980/badranaya.v2i02.1895.
[29] M. A. Azzeh, M., Altamimi, A. M., Albashayreh, M., \& Al-Oudat, "Adopting the Cybersecurity Concepts into Curriculum The Potential Effects on Students Cybersecurity Knowledge," *arXiv Prepr. arXiv*, vol. 1, no. 1, 2022, doi: 10.48550/arXiv.2209.10407.
[30] R. P. Rista *et al.*, "Sosialisasi Pentingnya Etika Dalam Penggunaan Sosial Media Pada SDN Medokan Semampir 1 Surabaya," *J. Pengabdi. Masy. Bangsa*, vol. 2, no. 6, pp. 2167–2173, Aug. 2024, doi: 10.59837/jpmba.v2i6.1185.

[31] L. Floridi *et al.*, "AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations," *Minds Mach.*, vol. 28, no. 4, pp. 689–707, Dec. 2018, doi: 10.1007/s11023-018-9482-5.
[32] A. Shrestha *et al.*, "Navigating AI to Unpack Youth Privacy Concerns: An In-Depth Exploration and Systematic Review," 2024. doi: 10.48550/arXiv.2412.16369.