TECHNE: JOURNAL OF TECHNOLOGY DEVELOPMENT
Vol. 02, No 01, June 2025, Hal. 15 - 21
P-ISSN: - E-ISSN: -
Open Access: https://dx.doi.org

PELATIHAN KEAMANAN SIBER DASAR BAGI GURU DAN TENAGA KEPENDIDIKAN DALAM MENGHADAPI ERA DIGITAL SMA NEGERI 1 PASIR PENYU

Feri Saputra[1], Iriene Putri Mulyadi [2], Dianda Rifaldi[3], Heri Hermanto[4], Guslila Sari Nasution [5], Nia Mardiana[6], Fauzan Purma Ramadhan[7], Juli Yandra[8], Mahardika Feidiantara[9]

[1,2,3,5,7,8,9] Fakultas Teknologi Informasi, Universitas Riau Indonesia, Rengat, Indonesia
[4,6] Fakultas Ilmu Administrasi, Universitas Riau Indonesia, Rengat, Indonesia
*Corresponding E-mail: ferisaputra5@gmail.com

ARTICLE INFO

Article history:
Received: 15 Mey 2025
Revised: 16 June 2025
Accepted: 25 June 2025

ABSTRACT

This study aims to design, implement, and evaluate basic cybersecurity training for teachers and educational staff at SMA Negeri 1 Pasir Penyu in facing the digital era. The method used was a quasi-experimental design with pre-test and post-test. A total of 35 participants attended a two-day training program covering both theoretical and practical materials, including data protection, phishing awareness, password management, and the safe use of digital platforms. The results showed an average knowledge increase of 65% from pre-test to post-test. In addition, participants expressed high satisfaction with the training and expected further advanced modules. The conclusion of this study is that basic cybersecurity training significantly improves the awareness and readiness of teachers and educational staff. It is recommended that such training be conducted regularly and supported by school policies.

Keywords: Cybersecurity; Digital Literacy; Educational Staff; Teacher Training

1. PENDAHULUAN

Transformasi digital di bidang pendidikan membawa peluang sekaligus tantangan yang besar. Hampir seluruh aspek pendidikan, mulai dari proses pembelajaran, administrasi, manajemen data siswa, hingga komunikasi antar guru, peserta didik, dan orang tua, kini sangat bergantung pada teknologi informasi [1]. Penerapan e-learning, sistem manajemen sekolah berbasis digital, serta pemanfaatan media sosial dan aplikasi komunikasi mempercepat proses pendidikan sekaligus meningkatkan efisiensi. Namun, di sisi lain, pemanfaatan teknologi digital ini juga membuka peluang terjadinya berbagai ancaman keamanan siber yang semakin kompleks, seperti serangan phishing, pencurian data pribadi, penyalahgunaan media sosial, hingga serangan malware yang dapat melumpuhkan sistem sekolah [2].

Dalam konteks pendidikan menengah, guru dan tenaga kependidikan memiliki peran yang sangat penting, tidak hanya sebagai pendidik yang mentransfer ilmu pengetahuan, tetapi juga sebagai pengelola data yang harus menjaga kerahasiaan serta keamanan informasi peserta didik [3]. Tanggung jawab tersebut mencakup perlindungan terhadap data akademik, informasi pribadi siswa, hingga dokumen administrasi sekolah. Namun, kenyataannya, pemahaman mengenai keamanan siber di kalangan guru dan tenaga kependidikan masih relatif rendah [4]. Banyak dari mereka yang belum terbiasa menggunakan praktik keamanan digital dasar, seperti penggunaan kata sandi yang kuat, autentikasi dua faktor, atau kewaspadaan terhadap pesan dan

tautan mencurigakan. Kondisi ini meningkatkan risiko kebocoran data serta potensi terjadinya serangan siber yang dapat mengganggu kelancaran proses pembelajaran.

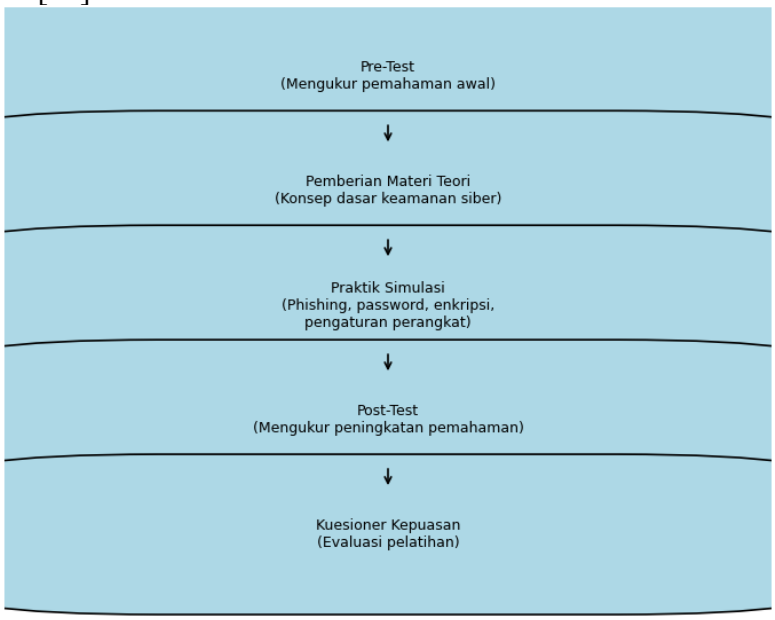
Beberapa penelitian menunjukkan bahwa kelemahan utama dalam keamanan siber bukan hanya pada teknologi, tetapi pada aspek manusia sebagai pengguna [5]. Oleh karena itu, penguatan literasi digital dan kesadaran keamanan siber melalui pendidikan dan pelatihan menjadi sangat penting. Pelatihan keamanan siber dasar terbukti dapat meningkatkan keterampilan guru dalam mengenali ancaman, mengelola data dengan lebih aman, serta mendorong terciptanya budaya keamanan digital di lingkungan sekolah [6]. Selain itu, pelatihan yang dirancang dengan pendekatan praktis, seperti simulasi serangan phishing atau studi kasus kebocoran data, akan lebih efektif dibanding hanya melalui penyampaian teori [7].

Urgensi pelatihan ini semakin tinggi karena dunia pendidikan Indonesia tengah mendorong percepatan transformasi digital pasca-pandemi COVID-19. Sekolah tidak hanya dituntut untuk menguasai teknologi pembelajaran daring, tetapi juga harus mampu memastikan bahwa sistem dan data yang digunakan tetap terlindungi dari ancaman siber [8]. Jika aspek keamanan diabaikan, maka keberhasilan transformasi digital di sekolah dapat terganggu oleh risiko penyalahgunaan data maupun serangan digital yang merugikan banyak pihak.

Berdasarkan latar belakang tersebut, penelitian ini dilakukan di SMA Negeri 1 Pasir Penyu dengan tujuan: (1) mengukur pemahaman awal guru dan tenaga kependidikan mengenai keamanan siber, (2) memberikan pelatihan keamanan siber dasar yang mencakup aspek teori dan praktik, serta (3) mengevaluasi efektivitas pelatihan dalam meningkatkan pengetahuan dan keterampilan peserta. Hasil dari penelitian ini diharapkan dapat memberikan kontribusi nyata dalam meningkatkan literasi digital dan budaya keamanan siber di lingkungan sekolah menengah, serta menjadi model bagi sekolah lain di Indonesia dalam menghadapi tantangan era digital.

2. METODE

Penelitian ini menggunakan pendekatan quasi-eksperimen dengan desain *one group pre-test and post-test* [9]. Desain ini dipilih karena sesuai untuk mengukur efektivitas suatu program pelatihan dengan cara membandingkan tingkat pemahaman peserta sebelum dan sesudah intervensi. Model ini telah banyak digunakan dalam penelitian pendidikan dan pelatihan, terutama untuk menguji dampak intervensi non-randomized terhadap peningkatan kompetensi peserta [10].



Gambar 1. Alur Metode Penelitian Pelatihan Keamanan Siber

Subjek Penelitian

Subjek penelitian terdiri dari 35 guru dan tenaga kependidikan SMA Negeri 1 Pasir Penyu. Pemilihan responden dilakukan dengan teknik purposive sampling, karena seluruh peserta memiliki keterkaitan langsung dengan proses pembelajaran maupun pengelolaan data sekolah [11]. Pemilihan guru dan tenaga kependidikan sebagai sasaran pelatihan didasarkan pada hasil studi sebelumnya yang menegaskan bahwa sektor pendidikan merupakan salah satu target rawan serangan siber, terutama karena kurangnya pemahaman pengguna terhadap praktik keamanan digital [12].

Instrumen penelitian meliputi:

1. Tes pengetahuan (pre-test dan post-test): berupa soal pilihan ganda yang disusun berdasarkan indikator pemahaman keamanan siber dasar.
2. Lembar observasi: digunakan untuk mencatat keterlibatan peserta selama pelatihan, termasuk partisipasi dalam simulasi dan diskusi.
3. Kuesioner kepuasan: diisi setelah pelatihan untuk mengetahui tingkat kepuasan peserta terkait materi, metode, dan pemateri [13].

Validitas instrumen diuji melalui *expert judgment* dengan melibatkan pakar keamanan siber dan pendidikan teknologi, sedangkan reliabilitas instrumen diuji menggunakan koefisien Cronbach Alpha.

Materi yang diberikan dalam pelatihan mencakup:

- Literasi digital: pemahaman dasar mengenai etika digital, privasi, dan perlindungan data pribadi.
- Keamanan kata sandi: praktik penggunaan kata sandi yang kuat dan manajemen kata sandi yang aman.
- Simulasi phishing: peserta diberikan contoh pesan email dan tautan berbahaya untuk melatih kewaspadaan.
- Enkripsi data sederhana: pengenalan konsep enkripsi untuk melindungi file penting.
- Pengaturan keamanan perangkat: praktik konfigurasi pada laptop, smartphone, dan jaringan Wi-Fi [14].

Materi ini disusun berdasarkan panduan internasional mengenai *cybersecurity awareness training* yang menekankan pada keterampilan praktis dan relevan dengan kehidupan sehari-hari [15].

Prosedur Penelitian

Pelatihan dilaksanakan selama dua hari dalam bentuk workshop intensif. Hari pertama berfokus pada sesi teori, meliputi pengenalan konsep dasar keamanan siber, studi kasus kebocoran data, serta pembahasan kebijakan perlindungan data di sekolah. Hari kedua diarahkan pada sesi praktik, berupa simulasi serangan phishing, praktik pengaturan kata sandi, hingga konfigurasi keamanan perangkat.

Langkah penelitian dapat dirinci sebagai berikut:

1. Peserta mengisi pre-test untuk mengukur pemahaman awal.
2. Pemberian materi teori melalui ceramah interaktif.
3. Praktik simulasi berupa studi kasus nyata ancaman siber di sektor pendidikan.
4. Peserta mengisi post-test untuk mengukur peningkatan pemahaman.

5. Peserta mengisi kuesioner kepuasan sebagai bahan evaluasi program.

Analisis Data

Data yang diperoleh dianalisis menggunakan statistik deskriptif untuk menggambarkan rata-rata skor pengetahuan, serta uji t berpasangan (paired t-test) untuk mengetahui signifikansi perbedaan antara hasil pre-test dan post-test [16]. Analisis tambahan berupa evaluasi kualitatif terhadap hasil observasi dan kuesioner kepuasan digunakan untuk memberikan gambaran komprehensif mengenai efektivitas pelatihan.

Pendekatan analisis kombinasi kuantitatif dan kualitatif ini digunakan karena terbukti efektif dalam mengevaluasi program pelatihan berbasis literasi digital dan keamanan siber [17].

3. HASIL DAN PEMBAHASAN

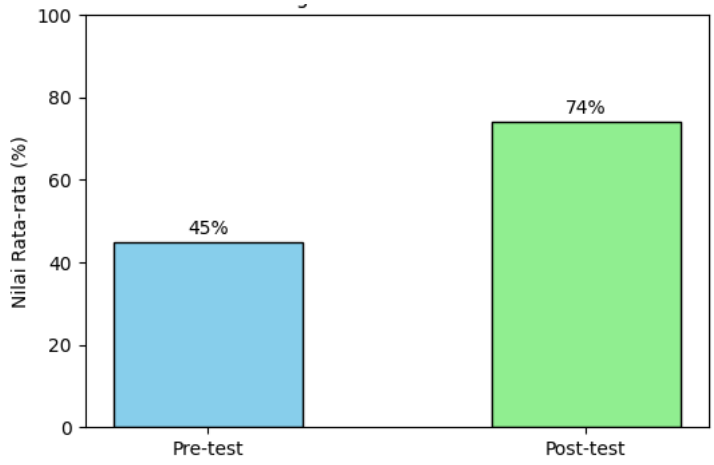
Hasil

Pelaksanaan pelatihan keamanan siber dasar di SMA Negeri 1 Pasir Penyu memberikan gambaran yang jelas mengenai peningkatan pemahaman peserta setelah mengikuti kegiatan. Hasil pre-test menunjukkan bahwa mayoritas guru dan tenaga kependidikan masih belum memahami konsep dasar keamanan digital. Beberapa kesalahan yang sering muncul adalah dalam mengenali tanda-tanda pesan phishing, penggunaan kata sandi yang sama pada berbagai akun, serta kurangnya perhatian terhadap pengaturan keamanan pada perangkat pribadi. Nilai rata-rata yang diperoleh pada tahap pre-test adalah 45%, yang menandakan bahwa sebagian besar peserta berada pada kategori rendah dalam hal literasi keamanan siber.

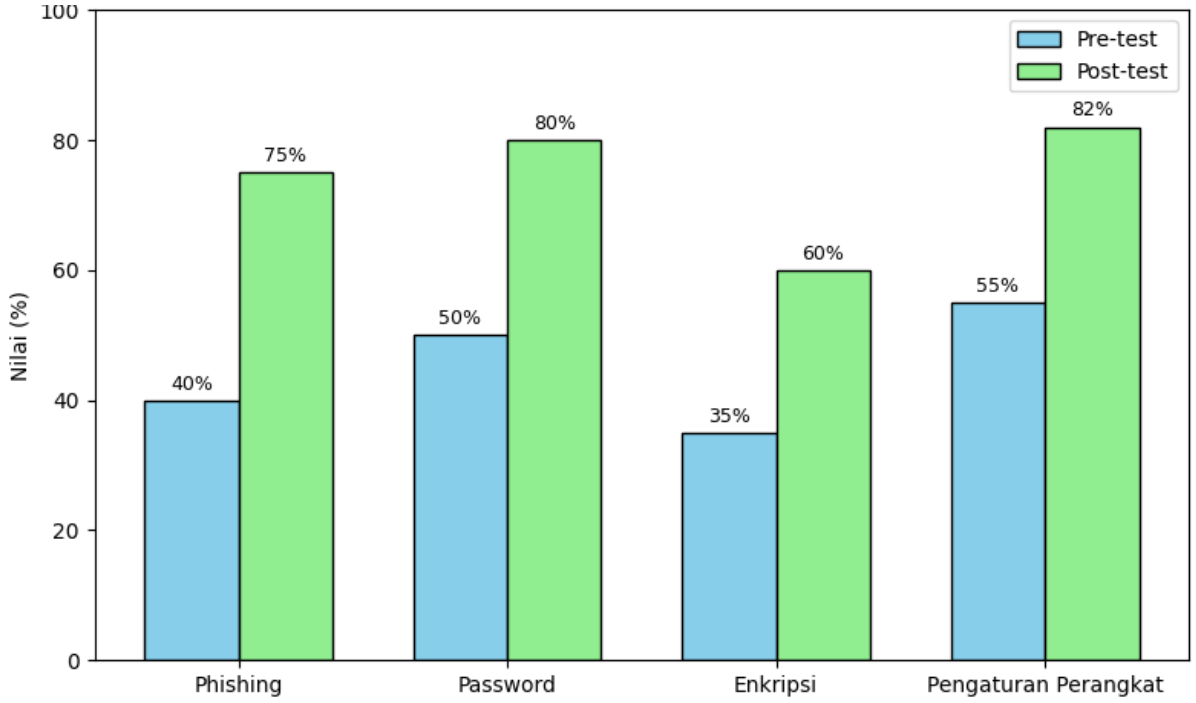
Setelah dilakukan pelatihan selama dua hari, hasil post-test menunjukkan peningkatan signifikan. Nilai rata-rata peserta meningkat menjadi 74%, dengan sebagian besar peserta mampu menjawab benar soal-soal terkait keamanan kata sandi, pengaturan privasi akun, serta tindakan pencegahan terhadap tautan mencurigakan. Secara kuantitatif, peningkatan pemahaman mencapai 65% dari kondisi awal.

Tabel 1. berikut menggambarkan perbandingan nilai rata-rata pre-test dan post-test

Tahap Tes	Nilai Rata-rata	Peningkatan
Pre-test	45%	-
Post-test	74%	+65%



Gambar 2. memperlihatkan hasil tersebut dalam bentuk diagram batang, yang menunjukkan adanya perbedaan mencolok antara nilai rata-rata sebelum dan sesudah pelatihan



Gambar 3. Perbandingan Nilai Pre-test dan Post-test per Indikator

Pembahasan

Peningkatan nilai rata-rata dari 45% menjadi 74% membuktikan bahwa pelatihan yang dilakukan efektif dalam meningkatkan kesadaran dan keterampilan guru serta tenaga kependidikan dalam menghadapi ancaman digital. Peningkatan paling signifikan terjadi pada aspek pengenalan *phishing* dan manajemen kata sandi. Hal ini menunjukkan bahwa metode pelatihan berbasis praktik seperti simulasi serangan digital memiliki dampak yang kuat dalam membangun pemahaman peserta [9].

Hasil ini sejalan dengan penelitian yang menekankan pentingnya kombinasi antara teori dan praktik dalam pendidikan keamanan siber [12], [14]. Materi berupa studi kasus nyata memudahkan peserta untuk mengaitkan pengetahuan baru dengan pengalaman sehari-hari, sehingga meningkatkan kemampuan analisis kritis terhadap ancaman digital.

Dari hasil kuesioner kepuasan, sebagian besar peserta (87%) menyatakan bahwa pelatihan sangat bermanfaat dan relevan dengan kebutuhan mereka. Sebagian besar guru juga mengusulkan agar pelatihan tidak hanya dilakukan sekali, melainkan menjadi program rutin dengan topik lanjutan seperti keamanan jaringan, penggunaan *firewall*, dan perlindungan data sekolah secara lebih mendalam. Hal ini konsisten dengan temuan [15], yang menyatakan bahwa pembelajaran berkelanjutan sangat diperlukan agar budaya keamanan digital dapat melekat dalam lingkungan kerja.

Meskipun hasilnya positif, pelatihan ini juga menghadapi hambatan, seperti keterbatasan sarana komputer di sekolah, ketergantungan pada jaringan internet yang belum stabil, serta keterbatasan waktu karena jadwal mengajar guru yang padat. Kendala tersebut perlu diantisipasi dengan penyediaan infrastruktur yang lebih baik serta dukungan kebijakan sekolah yang mendorong pelaksanaan pelatihan secara berkala.

Secara keseluruhan, penelitian ini menegaskan bahwa keberhasilan transformasi digital di sekolah tidak hanya ditentukan oleh ketersediaan perangkat teknologi, tetapi juga oleh kesiapan sumber daya manusia dalam memahami aspek keamanan siber. Oleh karena itu, pelatihan keamanan siber dasar harus menjadi bagian integral dari pengembangan kompetensi

guru dan tenaga kependidikan, sehingga risiko ancaman digital dapat diminimalisasi dan tercipta lingkungan pembelajaran yang aman.

4. KESIMPULAN

Berdasarkan hasil penelitian dan analisis yang telah dilakukan, dapat disimpulkan bahwa:

1. Pelatihan keamanan siber dasar efektif meningkatkan pemahaman guru dan tenaga kependidikan. Rata-rata nilai pre-test sebesar 45% meningkat menjadi 74% pada post-test, atau terjadi peningkatan pemahaman sebesar 65%. Hal ini membuktikan bahwa pelatihan berbasis teori dan praktik memberikan dampak signifikan terhadap literasi keamanan digital peserta [9], [12].
2. Peningkatan terbesar terjadi pada aspek pengenalan phishing dan manajemen kata sandi. Peserta menjadi lebih mampu mengenali email mencurigakan, menggunakan kata sandi yang lebih kuat, serta memahami pentingnya autentikasi ganda. Namun, pemahaman terkait enkripsi data dan pengamanan jaringan masih memerlukan pendalaman lebih lanjut [14].
3. Peserta memberikan respon positif terhadap pelatihan. Sebanyak 87% menyatakan puas dengan materi dan metode, serta mengusulkan agar kegiatan serupa dilakukan secara berkala. Temuan ini mendukung literatur sebelumnya yang menekankan pentingnya pelatihan berkelanjutan untuk menumbuhkan budaya keamanan digital [15].
4. Hambatan yang dihadapi meliputi keterbatasan infrastruktur dan waktu guru. Keterbatasan perangkat komputer dan jaringan internet yang kurang stabil menjadi tantangan utama. Oleh karena itu, dukungan kebijakan sekolah dan penyediaan infrastruktur menjadi faktor penting untuk menjamin keberlanjutan program pelatihan [16].

Dengan demikian, dapat disimpulkan bahwa pelatihan keamanan siber dasar merupakan langkah strategis untuk memperkuat kesiapan sekolah dalam menghadapi ancaman digital. Rekomendasi dari penelitian ini adalah:

1. Sekolah perlu menyusun kebijakan keamanan digital yang mengatur perlindungan data siswa dan tenaga kependidikan.
2. Pelatihan keamanan siber sebaiknya dilaksanakan secara berkelanjutan dan bertingkat, dimulai dari dasar hingga modul lanjutan.

Kolaborasi dengan pakar keamanan siber atau institusi terkait diperlukan untuk memperkuat kompetensi pendidik dan mendukung transformasi digital yang aman.

5. UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada SMA Negeri 1 Pasir Penyu yang telah memberikan izin dan dukungan dalam pelaksanaan kegiatan pelatihan keamanan siber dasar. Ucapan terima kasih juga disampaikan kepada Universitas Riau Indonesia (UNRIDA) atas dukungan akademik dan fasilitasi penelitian ini.

Selain itu, apresiasi diberikan kepada seluruh guru dan tenaga kependidikan yang telah berpartisipasi aktif dalam pelatihan serta memberikan masukan berharga untuk pengembangan materi. Penulis juga berterima kasih kepada rekan-rekan sejawat dan pihak-pihak lain yang telah membantu dalam proses perencanaan, pelaksanaan, hingga penyusunan laporan penelitian ini.

6. REFERENCES

[1] S. Watini, G. Davies, and N. Andersen, “Cybersecurity in Learning Systems: Data Protection and Privacy in Educational Information Systems and Digital Learning Environments,” Journal ITEE, vol. 3, no. 1, 2024.

[2] R. Saleh, M. Nasution, and A. Pratama, "Indonesia's Cyber Security Strategy: Problems and Challenges," Atlantis Press, pp. 45–53, 2023.
[3] M. Subni, A. Puspitasari, and R. A. Putri, "Peran Guru dalam Meningkatkan Kesadaran Keamanan Data Digital," Jurnal Pengabdian Kepada Masyarakat (JPKPM), vol. 4, no. 1, pp. 38–46, 2024.
[4] UNMAHA, "Pentingnya Kesadaran Keamanan Cyber bagi Guru dan Dosen," UNMAHA Blog, 2023. [Online]. Available: https://blog.unmaha.ac.id
[5] S. C. Khoironi, "Pengaruh Analisis Kebutuhan Pelatihan Budaya Keamanan Siber sebagai Upaya Pengembangan Kompetensi bagi Aparatur Sipil Negara di Era Digital," Jurnal Studi Komunikasi dan Media, vol. 24, no. 1, pp. 37–56, 2020.
[6] T. Triwiyanto, M. A. Ma'arif, and D. R. Nuryana, "Design, Development, and Implementation of Information Security Education for Teachers and Educational Personnel," ResearchGate, Dec. 2020.
[7] S. Djusar, "E-Training of the Cybersecurity for the Senior High School Teachers," Neliti, 2022. [Online]. Available: https://www.neliti.com/publications/457235
[8] SidikCyberMedia, "Kurikulum Keamanan Siber di Sekolah," SidikCyberMedia, 2023. [Online]. Available: https://sidikcybermedia.com
[9] J. Satrio, "Peningkatan Keterampilan Keamanan Siber bagi Pengelola Situs dan Media Sosial Desa Baros," Jurnal Inovasi dan Pemberdayaan Masyarakat (JIPPm), vol. 1, no. 2, pp. 15–22, 2022.
[10] D. Ary, L. C. Jacobs, and C. K. Sorensen, Introduction to Research in Education, 10th ed. Boston, MA: Cengage Learning, 2018.
[11] Sugiyono, Metode Penelitian Kuantitatif, Kualitatif, dan R&D. Bandung: Alfabeta, 2019.
[12] H. Susanto, "Cybersecurity Awareness in Indonesian Education Sector," International Journal of Cyber and IT Service Management, vol. 2, no. 1, pp. 12–20, 2021.
[13] S. A. Sukardi, Evaluasi Program Pendidikan dan Pelatihan. Jakarta: Bumi Aksara, 2020.
[14] A. K. Singh and P. Kumar, "Teaching Data Encryption Concepts in Digital Literacy Programs," Journal of Information Security Education, vol. 5, no. 2, pp. 55–64, 2021.
[15] P. F. Thomas, "Continuous Cybersecurity Training: Building Digital Security Culture in Schools," Education and Information Technologies, vol. 27, pp. 5523–5539, 2022.
[16] D. F. Yuliana and M. R. Prasetyo, "Tantangan Pelatihan Literasi Digital di Sekolah Menengah Indonesia," Jurnal Teknologi Pendidikan Indonesia, vol. 12, no. 3, pp. 220–229, 2022.
[17] H. Y. Kim, "Mixed-Methods Approaches in Evaluating Cybersecurity Training Programs," Computers & Security, vol. 114, p. 102584, 2022.