



## EDUKASI KEAMANAN SIBER BAGI REMAJA SEKOLAH MENENGAH DALAM MENGHADAPI ANCAMAN HOAKS DAN CYBERBULLYING

Rahmawati<sup>1</sup>, Abdul Rahman<sup>2</sup>, Muhammad Nur Iman<sup>3</sup>

<sup>1</sup>Universitas Halu Oleo

<sup>2</sup>STAI DDI Maros

<sup>3</sup>Universitas Hasanuddin

\*Correspondence E-mail: [rahmawati.fib@uho.ac.id](mailto:rahmawati.fib@uho.ac.id)<sup>1</sup>, [abdulrahmannu26@gmail.com](mailto:abdulrahmannu26@gmail.com)<sup>2</sup>, [iman.sindo@unhas.ac.id](mailto:iman.sindo@unhas.ac.id)<sup>3</sup>

### ABSTRACT

This study aims to enhance cybersecurity awareness among secondary school students through an educational program focused on the prevention of hoaxes and cyberbullying. The initiative was implemented in response to the growing exposure of adolescents to misinformation, online harassment, and privacy risks in digital environments. Using a participatory approach, the program involved 30 students from two secondary schools who participated in workshops, simulations, and interactive discussions. Data were collected through pre-test and post-test questionnaires, observations, and semi-structured interviews to assess knowledge, attitudes, and behavioral changes. The results revealed a significant improvement in participants' understanding of online safety concepts, including critical evaluation of digital information, ethical communication, and privacy management. Statistical analysis using a paired sample t-test ( $p < 0.05$ ) indicated an increase in cybersecurity literacy after the intervention. Qualitative findings supported this, showing enhanced awareness, empathy, and responsibility in digital interactions. Overall, the program successfully empowered students to identify and respond effectively to hoaxes and cyberbullying, fostering a safer and more ethical online culture among youth. These findings highlight the importance of continuous cybersecurity education in schools as a strategic effort to build digital resilience and promote responsible digital citizenship.

### ARTICLE INFO

#### Article History:

Received: 12 Nov 2025

Accepted: 17 Dec 2025

Published: 19 Jan 2026

Pages: 76-82

#### Keyword:

Cybersecurity education;  
digital literacy; hoax  
prevention; cyberbullying;  
youth empowerment

## 1. PENDAHULUAN

Perkembangan teknologi digital di abad ke-21 telah mengubah secara fundamental cara manusia berkomunikasi, belajar, dan berinteraksi social (Aser et al., 2022). Generasi remaja, yang dikenal sebagai digital natives, menjadi kelompok yang paling aktif dalam memanfaatkan teknologi informasi, terutama media sosial, sebagai sarana utama dalam kehidupan sehari-hari (Dono et al., 2022). Berdasarkan laporan We Are Social (2024), sekitar 95% remaja Indonesia terhubung ke internet setiap hari dengan durasi penggunaan rata-rata

lebih dari lima jam. Akses luas ini memberi peluang besar bagi peningkatan literasi digital, kreativitas, dan inovasi. Namun, di sisi lain, ketergantungan yang tinggi terhadap teknologi juga memunculkan risiko baru, seperti penyebaran hoaks, penipuan daring, serta tindakan perundungan digital (*cyberbullying*), yang dapat berdampak negatif terhadap perkembangan psikologis dan sosial remaja (Ardyah Rahmadani & Harahap, 2023).

Fenomena penyebaran hoaks di kalangan remaja kini menjadi isu krusial yang memerlukan perhatian serius (Ihsan Suri & Arsenius Wisnu Aji Patria Perkasa, 2023). Hoaks atau informasi palsu sering kali disebarakan melalui media sosial yang menjadi sumber utama berita bagi kalangan muda. Minimnya kemampuan remaja dalam melakukan verifikasi informasi menyebabkan mereka mudah terpengaruh oleh berita palsu yang bersifat provokatif, emosional, atau sensasional (Putri et al., 2023). Kondisi ini diperburuk oleh algoritma media sosial yang menampilkan konten serupa dengan preferensi pengguna, sehingga mempersempit wawasan dan menciptakan filter bubble yang menghambat objektivitas berpikir. Akibatnya, banyak remaja yang tanpa sadar ikut menyebarkan informasi yang salah dan memperkuat rantai disinformasi di dunia maya.

Di sisi lain, *cyberbullying* atau perundungan di dunia maya juga meningkat secara signifikan seiring dengan masifnya penggunaan media digital oleh remaja. Bentuk *cyberbullying* dapat berupa penghinaan, pelecehan, penyebaran foto pribadi tanpa izin, hingga pengucilan sosial di dunia maya. Dampak yang ditimbulkan tidak hanya bersifat psikologis, seperti stres, depresi, dan rasa rendah diri, tetapi juga dapat mempengaruhi performa akademik serta hubungan sosial korban di dunia nyata (Hanika et al., 2021). Studi Kementerian Komunikasi dan Informatika (Kominfo, 2023) menunjukkan bahwa sekitar 46% remaja Indonesia pernah mengalami bentuk *cyberbullying* baik sebagai korban maupun pelaku. Fenomena ini menunjukkan pentingnya intervensi edukatif untuk membangun kesadaran akan etika berinteraksi di ruang digital.

Dalam konteks ini, edukasi keamanan siber memiliki peran vital dalam membekali remaja dengan pengetahuan dan keterampilan untuk menghadapi tantangan dunia digital secara bijak (Chariroh & Ningdiyah, 2023). Edukasi ini tidak sekadar mengajarkan aspek teknis seperti menjaga kerahasiaan kata sandi atau mengenali situs berbahaya, tetapi juga menanamkan nilai moral, tanggung jawab, dan empati dalam berinteraksi secara daring (Fadhilah, 2019). Melalui pendidikan keamanan siber, remaja diharapkan mampu menjadi pengguna teknologi yang cerdas (*smart users*), bertanggung jawab (*responsible users*), dan beretika (*ethical users*). Selain itu, peningkatan kesadaran terhadap ancaman digital dapat membantu mereka lebih selektif dalam mengonsumsi informasi serta menghindari perilaku yang dapat merugikan diri sendiri dan orang lain (Ummah, 2019).

Pelaksanaan program edukasi keamanan siber di sekolah menengah menjadi langkah strategis untuk membangun budaya digital yang sehat di kalangan remaja. Sekolah memiliki posisi penting sebagai lembaga formal yang tidak hanya menekankan pencapaian akademik, tetapi juga pembentukan karakter dan literasi digital siswa (Miranti & Putri, 2021). Dengan metode pelatihan interaktif seperti simulasi kasus, permainan edukatif, dan diskusi berbasis pengalaman nyata, siswa dapat belajar mengenali bentuk-bentuk ancaman siber serta memahami cara melindungi diri mereka dari bahaya hoaks dan *cyberbullying*. Melalui pembelajaran yang menyenangkan dan kontekstual, remaja lebih mudah menerima pesan edukatif yang disampaikan dan termotivasi untuk menerapkannya dalam kehidupan digital sehari-hari.

Selain dukungan dari pihak sekolah, kolaborasi antara lembaga pemerintah, komunitas digital, dan organisasi masyarakat sipil juga menjadi faktor penting dalam

memperluas dampak program edukasi keamanan siber. Sinergi lintas sektor ini dapat memperkuat upaya penyediaan materi pembelajaran yang relevan, mengadakan kampanye literasi digital, serta menyediakan layanan konseling bagi korban cyberbullying. Pemerintah melalui Kominfo dan Badan Siber dan Sandi Negara (BSSN) telah mendorong program literasi digital nasional, namun peran masyarakat lokal, guru, dan orang tua tetap menjadi elemen kunci dalam menjaga kesinambungan program di tingkat sekolah dan komunitas.

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk menganalisis efektivitas program edukasi keamanan siber dalam meningkatkan kesadaran dan pemahaman remaja sekolah menengah terhadap ancaman hoaks dan cyberbullying. Melalui pendekatan partisipatif dan edukatif, diharapkan hasil penelitian ini dapat memberikan kontribusi nyata terhadap pengembangan model pembelajaran keamanan siber yang adaptif dan berkelanjutan. Selain itu, penelitian ini diharapkan mampu menghasilkan rekomendasi kebijakan dan praktik pendidikan yang mendorong terbentuknya generasi digital yang cerdas, kritis, dan beretika dalam menghadapi tantangan dunia maya yang semakin kompleks.

## **2. METODE PELAKSANAAN**

Metode pelaksanaan dalam kegiatan ini menggunakan pendekatan partisipatif dan edukatif dengan rancangan kegiatan berupa pelatihan dan sosialisasi interaktif mengenai keamanan siber bagi remaja sekolah menengah (Hadita et al., 2021). Rancangan kegiatan meliputi tiga tahapan utama, yaitu: (1) tahap persiapan, yang mencakup observasi awal dan penyusunan modul pelatihan keamanan siber; (2) tahap pelaksanaan, berupa penyuluhan dan praktik interaktif terkait pencegahan hoaks dan cyberbullying; serta (3) tahap evaluasi, yang dilakukan untuk mengukur peningkatan pemahaman dan perubahan perilaku digital peserta setelah mengikuti pelatihan (Elian & Ilyas, 2020).

Khalayak sasaran dalam kegiatan ini adalah remaja sekolah di SMA 12 Kendari, Sulawesi Tenggara yang memiliki tingkat penggunaan internet tinggi. Sebanyak 50 peserta dipilih melalui teknik purposive sampling, dengan kriteria remaja yang aktif menggunakan media sosial dan menunjukkan ketertarikan terhadap isu literasi digital. Pemilihan responden dilakukan berdasarkan rekomendasi dari pihak sekolah dan konselor bimbingan, dengan tujuan memastikan bahwa peserta yang terlibat dapat menjadi agen perubahan (peer educator) bagi teman sebayanya setelah pelatihan selesai.

Bahan dan alat yang digunakan dalam kegiatan ini mencakup modul pelatihan keamanan siber, materi presentasi digital, video edukatif mengenai hoaks dan cyberbullying, serta lembar kerja siswa yang berisi studi kasus untuk diskusi kelompok. Selain itu, perangkat pendukung seperti laptop, proyektor LCD, dan koneksi internet digunakan untuk mendukung kegiatan pembelajaran interaktif. Aplikasi digital seperti Kahoot! dan Google Form dimanfaatkan untuk mengukur tingkat pengetahuan peserta melalui pre-test dan post-test secara daring, sedangkan forum diskusi daring menggunakan platform Google Classroom sebagai sarana tindak lanjut pembelajaran.

Desain kegiatan pelatihan dirancang dengan prinsip interaktif dan kolaboratif. Peserta diajak untuk berpartisipasi aktif dalam sesi berbagi pengalaman mengenai keamanan digital, bermain peran (role play) dalam simulasi kasus cyberbullying, serta melakukan analisis kritis terhadap konten hoaks di media sosial. Dalam setiap sesi, fasilitator berperan sebagai pendamping yang memandu peserta untuk memahami konsep keamanan siber secara aplikatif, bukan sekadar teoritis. Pendekatan ini dinilai efektif untuk meningkatkan keterlibatan emosional dan kognitif peserta, sehingga pembelajaran menjadi lebih bermakna.

Teknik pengumpulan data dilakukan melalui beberapa cara. Pertama, observasi langsung dilakukan selama kegiatan berlangsung untuk melihat tingkat partisipasi dan interaksi peserta. Kedua, kuesioner pre-test dan post-test digunakan untuk mengukur peningkatan pengetahuan dan pemahaman peserta sebelum dan sesudah pelatihan. Ketiga, wawancara mendalam dilakukan terhadap sejumlah peserta terpilih untuk memperoleh gambaran kualitatif tentang perubahan sikap dan perilaku digital setelah mengikuti program.

Analisis data dilakukan dengan dua pendekatan. Data kuantitatif dari hasil pre-test dan post-test dianalisis menggunakan statistik deskriptif (mean, standar deviasi, nilai minimum dan maksimum) serta uji Paired Sample t-Test untuk mengetahui signifikansi peningkatan pemahaman peserta. Sementara itu, data kualitatif hasil wawancara dianalisis dengan analisis tematik, yaitu mengelompokkan kutipan responden berdasarkan tema seperti peningkatan literasi digital, kesadaran terhadap ancaman hoaks, dan pencegahan cyberbullying. Hasil analisis dari kedua pendekatan tersebut kemudian disintesis untuk memberikan gambaran menyeluruh tentang efektivitas program pelatihan dalam meningkatkan kesadaran keamanan siber di kalangan remaja sekolah menengah.

### 3. HASIL DAN PEMBAHASAN

Kegiatan edukasi keamanan siber bagi remaja sekolah menengah ini dilaksanakan selama dua hari dengan total durasi 8 jam pelatihan, mencakup materi tentang pengenalan ancaman digital, hoaks, dan cyberbullying, serta strategi pencegahan melalui praktik literasi digital. Sebanyak 30 peserta berpartisipasi aktif dalam seluruh rangkaian kegiatan. Pelaksanaan pre-test dan post-test dilakukan untuk mengukur tingkat pemahaman peserta sebelum dan sesudah mengikuti program. Secara umum, hasil menunjukkan adanya peningkatan signifikan dalam pemahaman remaja terhadap konsep keamanan siber dan perilaku digital yang bertanggung jawab. Data kuantitatif dari hasil pre-test dan post-test disajikan dalam bentuk statistik deskriptif untuk menggambarkan distribusi nilai peserta sebelum dan sesudah pelatihan.

**Tabel 1. Statistik Deskriptif Pre-test dan Post-test Pemahaman Keamanan Siber**

Variabel	N	Min	Max	Mean	Std. Deviation
Skor Pre-test	30	45	75	60.23	7.12
Skor Post-test	30	70	95	84.67	6.35

Berdasarkan Tabel 1, nilai rata-rata (mean) peserta meningkat dari 60.23 pada pre-test menjadi 84.67 pada post-test, menunjukkan peningkatan pemahaman yang cukup signifikan. Nilai standar deviasi yang relatif kecil (7.12 dan 6.35) menunjukkan bahwa persebaran nilai antar peserta cukup seragam. Hal ini mengindikasikan bahwa sebagian besar peserta memperoleh manfaat yang merata dari pelatihan yang diberikan. Untuk menguji secara statistik apakah peningkatan pemahaman peserta setelah pelatihan signifikan secara ilmiah, dilakukan uji Paired Sample t-Test.

**Tabel 2. Hasil Uji Paired Sample t-Test Pre-test dan Post-test**

Pasangan Variabel	Mean Difference	t-value	df	Sig. (2-tailed)
Pre-test – Post-test	-24.44	-12.371	29	0.000

Hasil uji menunjukkan bahwa nilai Sig. (2-tailed) = 0.000 < 0.05, yang berarti terdapat perbedaan signifikan antara hasil pre-test dan post-test. Dengan demikian, pelatihan keamanan siber terbukti efektif dalam meningkatkan pengetahuan dan kesadaran peserta terhadap ancaman digital, hoaks, dan cyberbullying. Selain data kuantitatif, hasil wawancara mendalam terhadap beberapa peserta juga memberikan gambaran kualitatif mengenai perubahan sikap dan perilaku setelah mengikuti pelatihan.

**Tabel 3. Hasil Wawancara Peserta Pelatihan Keamanan Siber**

Inisial Responden	Kutipan Wawancara
R-02	<i>“Dulu saya sering percaya begitu saja dengan berita di media sosial, tapi sekarang saya lebih berhati-hati dan selalu cek sumbernya.”</i>
R-10	<i>“Setelah pelatihan, saya lebih sadar pentingnya menjaga privasi akun dan tidak sembarangan klik tautan yang mencurigakan.”</i>
R-15	<i>“Saya jadi tahu kalau komentar di dunia maya juga bisa melukai orang lain. Sekarang saya lebih bijak saat berpendapat di internet.”</i>
R-21	<i>“Pelatihannya seru karena banyak contoh nyata dan simulasi. Saya bisa langsung praktik cara mengenali hoaks.”</i>
R-28	<i>“Saya jadi lebih percaya diri untuk mengingatkan teman-teman kalau mereka menyebarkan berita bohong atau melakukan cyberbullying.”</i>

Hasil penelitian menunjukkan bahwa program edukasi keamanan siber berhasil meningkatkan literasi digital dan kesadaran kritis peserta terhadap ancaman dunia maya. Peningkatan signifikan pada skor post-test mengindikasikan efektivitas pendekatan pelatihan berbasis interaktif, yang memungkinkan peserta tidak hanya memahami teori, tetapi juga mengaplikasikannya dalam konteks nyata. Hasil ini sejalan dengan penelitian terdahulu yang menyatakan bahwa metode pembelajaran partisipatif dan berbasis pengalaman lebih efektif dalam meningkatkan kesadaran digital pada remaja (Nasrullah, 2023).



**Gambar 1** .Sosialisasi Ancaman Hoaks Dan Cyberbullying

Temuan kualitatif melalui wawancara memperkuat hasil kuantitatif dengan menunjukkan adanya perubahan perilaku nyata di kalangan peserta. Para remaja mulai menerapkan prinsip kehati-hatian dalam menggunakan media sosial, lebih sadar akan dampak komentar negatif, dan memiliki keberanian untuk menegur teman sebaya yang melakukan tindakan cyberbullying. Hal ini menunjukkan bahwa pelatihan tidak hanya berdampak pada pengetahuan, tetapi juga pada pembentukan karakter digital yang etis.

Selain itu, hasil pelatihan juga memperlihatkan bahwa penyajian materi yang kontekstual dan relevan dengan kehidupan remaja, seperti studi kasus hoaks viral dan simulasi perundungan daring, dapat meningkatkan keterlibatan emosional peserta. Dampaknya, pelatihan menjadi lebih bermakna dan berpotensi menciptakan peer influence positif di lingkungan sekolah. Dengan demikian, kegiatan edukasi keamanan siber seperti ini dapat dijadikan model pengabdian masyarakat yang berkelanjutan, khususnya dalam membangun budaya digital yang aman dan beretika di kalangan generasi muda.

#### 4. KESIMPULAN

Pelaksanaan program edukasi keamanan siber bagi remaja sekolah menengah di SMA 12 Kendari menunjukkan bahwa pemahaman peserta terhadap ancaman digital seperti hoaks dan cyberbullying meningkat secara signifikan setelah kegiatan dilakukan. Sebelum pelatihan, sebagian besar peserta belum mampu membedakan antara informasi valid dan hoaks, serta belum memahami dampak hukum maupun psikologis dari perilaku perundungan daring. Melalui kegiatan sosialisasi, simulasi kasus, dan diskusi interaktif, peserta menjadi lebih kritis dalam menyaring informasi serta lebih bijak dalam menggunakan media sosial.

Hasil evaluasi menunjukkan adanya peningkatan yang nyata pada aspek pengetahuan dan kesadaran digital. Para remaja tidak hanya memahami konsep keamanan siber secara teoritis, tetapi juga mampu menerapkan langkah-langkah praktis seperti penggunaan kata sandi yang kuat, pengaturan privasi akun, serta pelaporan konten yang berpotensi berbahaya. Selain itu, peningkatan empati dan kesadaran etika digital juga terlihat dari hasil wawancara dan observasi pasca-pelatihan, di mana peserta menunjukkan perubahan sikap terhadap perilaku online yang lebih bertanggung jawab.

Secara keseluruhan, kegiatan edukasi ini berperan penting dalam membangun literasi digital dan ketahanan siber generasi muda di era informasi. Upaya ini membuktikan bahwa pendekatan edukatif berbasis pelatihan interaktif efektif dalam menanamkan nilai tanggung jawab, empati, dan kesadaran kritis terhadap konten digital. Program semacam ini diharapkan dapat terus dikembangkan secara berkelanjutan dengan melibatkan sekolah, lembaga pemerintah, dan komunitas digital agar dapat menciptakan ekosistem daring yang aman, sehat, dan beretika bagi remaja Indonesia.

#### DAFTAR PUSTAKA

- Ardyah Rahmadani, T., & Harahap, N. (2023). Dampak Cyberbullying di Media Sosial pada Perilaku Reaktif Remaja di Desa Sei Rotan. *Jurnal Noken: Ilmu-Ilmu Sosial*, 8(2).  
<https://doi.org/10.33506/jn.v8i2.2372>
- Aser, F. G., Paramita, S., & Sudarto. (2022). Fenomena Cyberbullying di Media Sosial TikTok. *Kiwari*, 1(3). <https://doi.org/10.24912/ki.v1i3.15763>
- Chariroh, L., & Ningdiyah, A. E. M. (2023). Cyberbullying pada remaja pengguna tik tok: Bagaimana peranan tipe kepribadian ekstrovert? *Jurnal of Psychological Research*, 2(4).
- Dono, D., Setyaningsih, E. R., & Pickerling, P. (2022). Penyaring Komentar Cyberbullying Pada Konten Blog. *Journal of Intelligent System and Computation*, 4(2).  
<https://doi.org/10.52985/insyst.v4i2.271>

- Elian, A. F., & Ilyas, I. (2020). Pelaksanaan Metode Pembelajaran Partisipatif Pada Kursus Mahacoustic Music Management Di Kota Semarang. *Aksara: Jurnal Ilmu Pendidikan Nonformal*, 6(2). <https://doi.org/10.37905/aksara.6.2.111-120.2020>
- Fadhilah, S. (2019). Cyberbullying Di Kalangan Remaja Pada Jejaring Sosial. *Media Nusantara*, 15(1).
- Hadita, A., Yusuf, R., & Darmawan, E. D. (2021). METODE PARTISIPATIF PADA PELATIHAN FINANCIAL LIFE SKILLS UNTUK MENINGKATKAN LITERASI KEUANGAN PENGAJAR TRIDAYA GROUP BANDUNG. *Sebatik*, 25(1). <https://doi.org/10.46984/sebatik.v25i1.1266>
- Hanika, I. M., Witjaksono, A. A., & Pratiwi, S. I. (2021). Fenomena Cyberbullying pada Mahasiswa di Jakarta Selatan. *Jurnal Ilmiah Media, Public Relations, Dan Komunikasi (IMPRESI)*, 2(1). <https://doi.org/10.20961/impresi.v2i1.53136>
- Ihsan Suri, & Arsenius Wisnu Aji Patria Perkasa. (2023). Media Sosial dan Citra Diri: Peran Akun Kedua dalam Melindungi Identitas dan Privasi Anak serta Remaja. *Innovative: Journal of Social Science Research*, 3(5).
- Miranti, P., & Putri, L. D. (2021). Waspada Dampak Penggunaan Gadget Terhadap Perkembangan Sosial Anak Usia Dini. *Jendela PLS*, 6(1). <https://doi.org/10.37058/jpls.v6i1.3205>
- Putri, S. N., Fiandra, Y., & Ramdhan, Z. (2023). PERANCANGAN DALAM IKLAN I AM ENOUGH PADA PLATFORM TIKTOK BERTEMAKAN CYBERBULLYING. *E-Proceeding of Art & Design*, 10(2).
- Ummah, M. S. (2019). Bullying di Kalangan Remaja. *Sustainability (Switzerland)*, 11(1).