

PENGUATAN KESADARAN KEAMANAN SIBER REMAJA MELALUI SOSIALISASI TERSTRUKTUR DI
SMAN 10 KOTA JAMBIFriska Ameliana Putri¹, Audia Zahara², Nini Alvita³¹²³Fakultas Sains dan Teknologi, UIN Sultan Thaha Saifuddin Jambifriskaaputri250123@gmail.com¹, audiazaharaa@gmail.com², ninialvita59@gmail.com³**Abstrak**

Perkembangan teknologi digital memberikan dampak positif bagi generasi muda dalam bidang pendidikan dan komunikasi, namun juga meningkatkan risiko ancaman keamanan siber. Rendahnya literasi dan kesadaran keamanan digital menjadi faktor utama meningkatnya kerentanan remaja terhadap berbagai serangan siber. Kegiatan Pengabdian Kepada Masyarakat ini bertujuan untuk meningkatkan kesadaran dan pemahaman keamanan siber bagi siswa SMAN 10 Kota Jambi melalui kegiatan sosialisasi terstruktur. Metode pelaksanaan dilakukan melalui presentasi interaktif menggunakan media laptop dan proyektor, dilengkapi dengan kuis serta pembagian kuesioner evaluasi. Peserta kegiatan berjumlah 30 siswa kelas XI F-8 yang mengikuti kegiatan secara sukarela. Materi yang disampaikan meliputi pengertian keamanan siber, jenis-jenis serangan siber, pentingnya perlindungan data pribadi, serta langkah-langkah pencegahan risiko digital. Hasil kegiatan menunjukkan adanya peningkatan kesadaran siswa terhadap pentingnya menggunakan kata sandi yang kuat, kehati-hatian terhadap tautan mencurigakan, serta kewaspadaan terhadap penipuan daring. Siswa juga menunjukkan antusiasme tinggi terhadap materi yang disampaikan. Dengan demikian, sosialisasi keamanan siber dinilai cukup efektif dalam meningkatkan pemahaman awal siswa, namun perlu dilakukan secara berkelanjutan dan lebih aplikatif untuk membentuk perilaku digital yang aman dan bertanggung jawab.

Kata Kunci : Keamanan Siber, Kejahatan Siber, SMAN 10 Kota Jambi**Abstract**

The development of digital technology has had a positive impact on the younger generation in the fields of education and communication, but it has also increased the risk of cybersecurity threats. Low digital literacy and awareness are major factors in increasing adolescent vulnerability to various cyberattacks. This Community Service activity aims to increase cybersecurity awareness and understanding among students of SMAN 10 Jambi City through structured outreach activities. The implementation method was carried out through interactive presentations using laptops and projectors, complemented by quizzes and the distribution of evaluation questionnaires. The activity participated in 30 students of grade XI F-8 who participated voluntarily. The material presented included the definition of cybersecurity, types of cyberattacks, the importance of personal data protection, and steps to prevent digital risks. The results of the activity showed an increase in student awareness of the importance of using strong passwords, caution against suspicious links, and vigilance against online fraud. Students also showed high enthusiasm for the material presented. Thus, cybersecurity outreach is considered quite effective in improving students' initial understanding, but it needs to be carried out continuously and more applicable to shape safe and responsible digital behavior.

Keywords: Cyber Security, Cybercrime, SMAN 10 Jambi**Article History**

Received: Desember 2025

Reviewed: Desember 2025

Published: Desember 2025

Plagiarism Checker No 483

Prefix DOI : Prefix DOI :

10.8734/krepa.v1i2.365

Copyright : Krepa



This work is licensed under
a [Creative Commons
Attribution-NonCommercial
4.0 International License](https://creativecommons.org/licenses/by-nc/4.0/)

Pendahuluan

Dalam beberapa tahun terakhir, perkembangan teknologi informasi dan komunikasi telah mengubah cara masyarakat, khususnya generasi muda, dalam berinteraksi, belajar, dan mengakses informasi. Penelitian Yusuf dan Kamariah (2025) menunjukkan bahwa pemanfaatan teknologi digital mampu memperluas akses pendidikan, meningkatkan partisipasi siswa, serta memperkuat kreativitas dan kemampuan berpikir kritis dalam proses belajar mengajar. Namun, dibalik semua kemajuan tersebut, tentu ada ancaman terhadap dunia digital yang juga ikut berkembang pesat. Kristianti & Kurniasi (2024) menegaskan bahwa tantangan keamanan siber kini semakin kompleks, dinamis, dan sulit diprediksi. Oleh karena itu, peningkatan kesadaran keamanan siber di kalangan generasi muda menjadi sangat penting untuk melindungi diri mereka.

Data nasional memperlihatkan urgensi persoalan ini. Pada semester pertama tahun 2025, terdapat sekitar 133,4 juta serangan siber yang terdeteksi di Indonesia, dan mayoritas memanfaatkan celah perilaku pengguna melalui jenis serangan *Generic Protocol Command Decode* (Kompas.com, 2025). Selain itu, skor keamanan siber Indonesia dalam *National Cyber Security Index* (NCSI) berada pada angka 63,64 dari skala 100, menempatkan Indonesia di peringkat 49 dari 176 negara (E, 2025). Angka ini menunjukkan bahwa keamanan digital tidak hanya berkaitan dengan kemampuan infrastruktur, tetapi juga menyangkut kesiapan individu dalam memahami, mengantisipasi, dan merespons ancaman yang ada. Budiyanto & Mabruri (2025) mengemukakan bahwa rendahnya literasi siber masyarakat menjadi salah satu faktor utama yang meningkatkan kerentanan terhadap berbagai bentuk serangan digital.

Badan Siber dan Sandi Negara (BSSN) melaporkan 12.691 insiden siber pada 2023, termasuk serangan yang menargetkan pengguna muda (Zein, 2025). Remaja merupakan kelompok yang paling rentan karena intensitas penggunaan internet yang tinggi tidak selalu diiringi pengetahuan yang memadai mengenai risiko digital. Menteri Komunikasi dan Digital, Meutya Hafid, menyebutkan bahwa 48 persen pengguna internet di Indonesia merupakan remaja di bawah 18 tahun, dengan rata-rata penggunaan lebih dari lima jam per hari (Sihombing, 2025). Kondisi ini membuat remaja rentan terhadap pencurian data, perundungan digital, penyebaran *malware*, serta manipulasi informasi. Berbagai penelitian internasional menyarankan perlunya strategi edukasi partisipatif dan relevan dengan pengalaman remaja untuk meningkatkan kesadaran serta kemampuan remaja dalam menjaga keamanan diri di ruang siber (Cuhanazriansyah, 2025). Pelatihan kesadaran keamanan siber terbukti meningkatkan pengetahuan dan kemampuan siswa dalam keamanan siber dan antisipasi kejahatan siber setelah pelatihan diberikan (Pasha et al., 2024).

SMAN 10 Kota Jambi merupakan salah satu institusi pendidikan yang mayoritas siswanya adalah remaja dengan tingkat akses internet yang tinggi, namun sejauh ini belum pernah dilaksanakan sosialisasi yang terarah terkait keamanan siber. Padahal, sosialisasi yang terstruktur sangat diperlukan untuk mengenalkan konsep dasar keamanan digital, membentuk kebiasaan penggunaan teknologi yang aman, serta meningkatkan kemampuan deteksi dini terhadap potensi ancaman. Oleh karena itu, penguatan kesadaran keamanan siber remaja melalui sosialisasi terstruktur di SMAN 10 Jambi menjadi langkah strategis untuk meminimalkan kerentanan digital sekaligus menanamkan budaya literasi siber sejak dini. Kegiatan sosialisasi ini diharapkan tidak hanya meningkatkan pengetahuan, tetapi juga menumbuhkan sikap tanggap, kritis, dan bertanggung jawab dalam memanfaatkan teknologi secara aman dan produktif.

Metode Pelaksanaan

Metode kegiatan Pengabdian Kepada Masyarakat ini dilakukan melalui sosialisasi mengenai keamanan siber secara efektif di lingkungan SMAN 10 Kota Jambi. Lokasi kegiatan sosialisasi ini adalah SMAN 10 Kota Jambi. Secara administratif, SMAN 10 Kota Jambi berada di Kota Jambi, Kecamatan Telanai Pura, Kota Jambi, Jambi. Kegiatan ini ditujukan untuk siswa Sekolah Menengah Atas kelas 11 F-8 yang direkomendasikan oleh pihak sekolah dan berpartisipasi secara sukarela. Sebanyak 30 siswa terlibat dalam kegiatan sosialisasi ini. Pemilihan peserta tidak didasarkan pada kriteria inklusi atau eksklusi tertentu agar semua siswa memiliki kesempatan

yang sama untuk mengikuti kegiatan edukasi ini.

Dalam pelaksanaan kegiatan, penyampaian materi disajikan langsung oleh Tim Pelaksana dengan menggunakan media laptop dan proyektor disertai kuis berhadiah untuk mengetahui seberapa besar tingkat pemahaman siswa dalam memahami materi yang telah disampaikan. Kegiatan sosialisasi ini dilakukan dengan presentasi interaktif yang mencakup pengenalan keamanan siber, berbagai bentuk serangan dan ancaman internal, cara menjaga keamanan informasi, serta contoh kasus beserta dampaknya dalam kehidupan modern. Adapun tahapan pelaksanaan sosialisasi di SMAN 10 Kota Jambi adalah sebagai berikut.

1. Tahap Persiapan

Tahap persiapan kegiatan sosialisasi ini meliputi :

a. Kunjungan awal

Kunjungan dilakukan ke SMAN 11 Kota Jambi di Jalan Depati Parbo, Pematang Sulur, Kecamatan Telanaipura, Kota Jambi. Tahapan ini bertujuan untuk bertukar informasi antara pihak sekolah dan tim pelaksana, seperti penentuan lokasi kegiatan, penjadwalan, **perkiraan jumlah peserta, serta kebutuhan sarana dan prasarana.**

b. Penyusunan materi

Pada tahap ini, tim pelaksana menyiapkan bahan penyuluhan yang sistematis dan relevan dengan kondisi siswa SMA. Penyusunan materi dilakukan dengan langkah-langkah berikut:

- 1) Menentukan topik utama yang akan dibahas, seperti pengertian keamanan siber, macam-macam serangan siber, ancaman internal, serta praktik pencegahan sederhana yang dapat diterapkan oleh siswa.
- 2) Pengumpulan data, contoh kasus terbaru, dan informasi valid dari sumber terpercaya agar materi akurat dan tidak bersifat sekadar teori umum.
- 3) Penyusunan alur penyampaian materi secara bertahap, mulai dari penjelasan konsep dasar hingga pembahasan kasus nyata agar peserta mudah memahami konteksnya.
- 4) Penambahan ilustrasi, visual, atau simulasi sederhana untuk meminimalkan risiko miskonsepsi dan meningkatkan keterlibatan peserta saat presentasi berlangsung.
- 5) Menyiapkan pertanyaan kuis yang selaras dengan materi dan dapat menjadi alat evaluasi sederhana untuk mengukur tingkat pemahaman siswa.

2. Tahap Penyuluhan

a. Pembukaan dan pengenalan

Pelaksana melakukan pengenalan singkat dan dilanjutkan dengan pertanyaan pemantik sederhana agar muncul rasa ingin tahu dan kesiapan untuk mengikuti materi.

b. Penyampaian materi inti

Materi disampaikan secara interaktif melalui presentasi.

- 1) Pengertian keamanan siber dan ruang lingkupnya.
- 2) Macam-macam serangan digital yang sering terjadi, seperti *phishing*, *malware*, *hacking*, dan pencurian data.
- 3) Ancaman internal yang berasal dari kelalaian pengguna, perilaku berbagi kata sandi, maupun kurangnya kesadaran terhadap privasi digital.
- 4) Strategi praktis menjaga keamanan akun, penggunaan kata sandi yang kuat, verifikasi dua langkah, serta etika bermedia digital.

5) Studi kasus nyata yang relevan dengan lingkungan remaja, seperti penyebaran tautan berbahaya di grup sekolah, penipuan media sosial, atau peretasan akun *game*.

c. Simulasi sederhana

Untuk meningkatkan pemahaman praktis, peserta diajak mengikuti simulasi singkat, misalnya mengenali ciri-ciri pesan mencurigakan, membedakan tautan aman dan berbahaya, atau membuat kata sandi yang kuat dan mudah diingat. Pendekatan ini tidak hanya bersifat teoritis, tetapi melatih keterampilan nyata yang dapat langsung diterapkan.

d. Kuis evaluasi

Tahap penyuluhan diakhiri dengan kuis singkat berhadiah sebagai bentuk evaluasi cepat terhadap materi yang telah disampaikan. Kuis ini berfungsi mengukur pemahaman peserta secara langsung sekaligus menjaga suasana kegiatan tetap menarik dan partisipatif.

Landasan Teori

1. Konsep dan Definisi Keamanan Siber

Cisco mendefinisikan keamanan siber sebagai praktik melindungi berbagai sistem, jaringan, dan program dari serangan digital. Kaspersky (2020) juga mendefinisikan keamanan siber sebagai praktik perlindungan sistem, jaringan, dan program dari serangan digital yang bertujuan untuk mengakses, mengubah, atau menghancurkan informasi sensitif, memeras uang dari pengguna, atau mengganggu operasi bisnis. Serangan siber dapat berasal dari berbagai sumber, termasuk individu, kelompok kriminal terorganisir, atau bahkan negara yang terlibat dalam spionase siber atau perang dunia maya (Budiyanto & Mabruri, 2025).

NIST (2018) menyebutkan bahwa perlindungan data dalam keamanan siber bertumpu pada tiga aspek utama yang dikenal sebagai CIA Triad (*Confidentiality*, *Integrity*, dan *Availability*) (Budiyanto & Mabruri, 2025). Kerangka ini memuat elemen inti keamanan informasi yang memastikan data tetap terlindungi, akurat, dan dapat diakses oleh pihak yang berwenang. *Confidentiality* (Kerahasiaan) berfokus pada pencegahan akses tidak sah terhadap informasi sensitif. Hanya pengguna atau sistem yang berwenang yang seharusnya dapat melihat, menggunakan, atau memproses data tersebut. Selain menjaga kerahasiaan, keamanan siber juga menuntut aspek *Integrity* (Integritas), yaitu memastikan data tetap akurat, konsisten, dan tidak mengalami perubahan tanpa otorisasi, baik selama penyimpanan maupun transmisi. Ancaman seperti kerusakan data, serangan *man-in-the-middle*, atau modifikasi yang dilakukan pihak tidak berwenang dapat mengganggu integritas ini. Di samping itu, *Availability* (ketersediaan) memastikan bahwa informasi serta sistem pendukungnya dapat diakses oleh pihak yang berwenang kapan pun dibutuhkan. Serangan siber, kerusakan perangkat keras, atau bencana alam dapat menghambat ketersediaan data, sehingga sistem perlu dirancang agar tangguh dan mampu pulih dari gangguan (Abidde et al., 2025).

Dalam upaya memperkuat keamanan siber, pemerintah Indonesia telah menerbitkan berbagai regulasi dan kebijakan yang bertujuan untuk melindungi infrastruktur digital nasional. Salah satu kebijakan yang penting adalah Peraturan Presiden No. 53 Tahun 2017 yang mengatur tentang pembentukan BSSN (Badan Siber dan Sandi Negara) sebagai lembaga yang bertanggung jawab atas keamanan siber di Indonesia. Secara regulatif, strategi keamanan nasional Indonesia telah diperkuat melalui sejumlah peraturan seperti Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, serta Undang - Undang Perlindungan Data Pribadi (UU PDP). Regulasi ini bertujuan untuk memberikan kepastian hukum dan perlindungan terhadap data serta transaksi digital warga negara. Selain itu, Indonesia juga telah meratifikasi berbagai perjanjian internasional yang terkait dengan keamanan siber, seperti *Budapest Convention on Cybercrime*.

2. *Cybercrime*

Cybercrime adalah suatu kegiatan atau peristiwa yang melibatkan teknologi komputer dimana seseorang memperoleh keuntungan dengan menimbulkan kerugian pada pihak lain. *Cybercrime* juga merupakan kejahatan komputer yang dilakukan oleh individu atau sekelompok orang yang menyerang sistem keamanan komputer atau data yang terkandung di dalamnya. Kejahatan-kejahatan ini dilakukan karena berbagai alasan, mulai dari kepuasan diri sendiri hingga kejahatan yang dapat menimbulkan kerugian ekonomi atau politik (Muslim et al., 2024).

Berikut adalah beberapa macam *cybercrime* yang sering ditemui dalam kehidupan sehari-hari.

a) *Phising*

Phishing adalah bentuk kejahatan dunia maya yang memanfaatkan teknik rekayasa sosial. Pelaku *phishing*, yang dikenal sebagai *phisher*, berusaha mendapatkan informasi pribadi yang bersifat sensitif, seperti *username*, *password*, dan data penting lainnya. Serangan *phishing* dapat terjadi pada berbagai sektor dan platform *online*, termasuk media sosial, *e-commerce*, layanan jejaring sosial, hingga perbankan. *WhatsApp* menjadi salah satu media sosial yang kerap disalahgunakan sebagai sarana penipuan. Modus *phishing* di *WhatsApp* biasanya dilakukan dengan berpura-pura sebagai pihak resmi suatu instansi, seperti bank atau lembaga kepolisian, untuk menipu korban yang kurang teliti dan memiliki kesadaran keamanan yang rendah (Erdiyanto, 2023).

b) *Malware*

Malware merupakan kependekan dari *malicious software*, yaitu perangkat lunak berbahaya yang dirancang untuk menyusup ke dalam sistem tanpa diketahui oleh pemiliknya dan dapat bertahan dalam jangka waktu tertentu. *Malware* biasanya masuk melalui email, file unduhan, atau program yang sudah terinfeksi. Sebagian besar kejahatan komputer terjadi dalam bentuk pencurian data pribadi atau pembuatan *backdoor* yang memungkinkan pelaku mengakses komputer tanpa izin. Setiap perangkat lunak yang menjalankan tindakan tersebut tanpa persetujuan pemilik perangkat dapat dikategorikan sebagai *malware* (Sari, 2024).

c) *Ransomware*

Ransomware merupakan jenis malware atau program berbahaya yang digunakan oleh pelaku kejahatan siber untuk mengunci, merusak, atau mengancam akan menyebarkan data penting milik korban, kecuali korban membayar sejumlah uang tebusan (Microsoft Security, 2025).

d) *Hacking*

Peretasan (*Hacking*) adalah upaya masuk ke sistem komputer atau jaringan tanpa izin dengan tujuan mencuri, mengubah, atau merusak data. Aksi ini biasanya memanfaatkan kelemahan keamanan pada perangkat atau sistem.

e) *Cyberbullying*

Cyberbullying didefinisikan sebagai bentuk intimidasi yang melibatkan penggunaan sarana elektronik, seperti situs media sosial, email, forum, dan pesan instan, untuk membuat seseorang mengalami perilaku mengancam. Hal ini sering kali mencakup ancaman online berulang, media sosial dan posting forum yang memalukan, dan pesan langsung pribadi yang mengancam (Ray et al., 2024).

f) DDoS (*Distributed Denial of Service*)

DDoS adalah serangan yang membanjiri situs atau layanan dengan lalu lintas internet yang tidak wajar untuk menghentikan operasional (Budiyanto & Maburi, 2025).

Cyber crime memiliki dampak yang luas dan serius, baik bagi individu, bisnis, maupun masyarakat secara keseluruhan. Berikut adalah beberapa dampak utama dari kejahatan *cyber* (Sovina et al., 2024).

a) Kehilangan Data Pribadi

Serangan siber seperti pencurian identitas atau pelanggaran data dapat mengakibatkan kebocoran informasi pribadi seperti nomor kartu kredit, informasi bank, atau data pribadi lainnya. Ini dapat digunakan untuk pencurian identitas, penipuan, atau kejahatan finansial lainnya.

b) Kerugian Finansial

Kejahatan siber sering kali berdampak langsung pada kerugian finansial bagi individu dan bisnis. Ini bisa berupa pencurian uang dari rekening bank, pembelian yang tidak sah menggunakan informasi kartu kredit yang dicuri, atau kerugian finansial lainnya akibat penipuan *online*.

c) Gangguan pada Layanan

Serangan siber seperti serangan DDoS (*Distributed Denial of Service*) dapat menyebabkan gangguan pada layanan *online* seperti situs web, layanan perbankan, atau infrastruktur kritis seperti listrik atau transportasi. Hal ini dapat mengganggu aktivitas sehari-hari dan bahkan mengancam keamanan publik.

d) Kerusakan Reputasi

Untuk bisnis, serangan siber dapat merusak reputasi perusahaan dan kehilangan kepercayaan pelanggan. Pelanggaran data yang besar atau sering dapat menyebabkan hilangnya pelanggan dan kerugian finansial jangka panjang.

e) Ancaman Keamanan Nasional

Serangan siber juga dapat menjadi ancaman terhadap keamanan nasional, dengan negara-negara dan kelompok-kelompok yang menggunakan teknik *hacking* untuk memata-matai negara lain, merusak infrastruktur kritis, atau bahkan meluncurkan serangan terhadap sistem militer atau pemerintah.

f) Gangguan pada Kehidupan Pribadi

Kejahatan siber juga dapat memiliki dampak emosional dan psikologis pada individu yang menjadi korban. Pencurian identitas atau pelecehan *online* dapat menyebabkan stres, kecemasan, atau bahkan depresi pada korban.

3. Ancaman Internal

Ancaman internal (*insider threat*) merupakan salah satu bentuk serangan siber yang paling sulit dideteksi dan berpotensi menimbulkan kerugian finansial serta reputasional yang besar. Hal ini dikarenakan pelaku ancaman internal adalah individu yang memiliki akses sah ke dalam sistem organisasi, memahami struktur jaringan, serta prosedur keamanan yang berlaku, sehingga aktivitas berbahaya yang mereka lakukan sering kali tersamarkan sebagai perilaku normal. Deteksi tradisional yang mengandalkan audit perilaku (*behavioral auditing*) menjadi kurang efektif karena pelaku dapat dengan sengaja menghindari pola-pola yang telah diketahui (Yi & Tian, 2024).

Pureti (2022) membagi penyebab ancaman internal menjadi 2 kategori, yaitu *malicious insider* atau *negligent insider*. *Malicious insider* yaitu individu yang dengan sengaja mengeksploitasi akses mereka untuk keuntungan pribadi atau untuk membahayakan

organisasi. Motivasi mereka dapat bervariasi dari insentif keuangan dan spionase hingga keluhan pribadi. Sedangkan *negligent insider* merupakan individu yang tidak memiliki niat jahat tetapi menimbulkan risiko keamanan karena tindakan ceroboh atau tidak terinformasi yang secara tidak sengaja membahayakan keamanan. Yi dan Tian (2024) menekankan bahwa kategori *negligent insider* adalah faktor utama penyebab ancaman internal akibat dari rendahnya pemahaman keamanan siber dan kebiasaan digital yang tidak aman.

Dampak dari ancaman yang berasal dari dalam sangat besar, mencakup mulai dari pencurian data, kerusakan pada sistem, gangguan dalam operasional, sampai dengan menurunnya kepercayaan terhadap layanan berbasis digital. Ancaman yang muncul dari dalam tidak hanya mengincar perusahaan besar, tetapi juga lembaga pendidikan, seperti sekolah, yang mana para penggunanya yang masih muda memiliki akses yang luas namun minim pengetahuan mengenai keamanan. Memahami ancaman internal sangat penting untuk membangun perilaku digital yang aman, meningkatkan pemahaman tentang keamanan siber, serta mendorong penerapan kontrol akses, autentikasi, dan kebiasaan penggunaan perangkat yang lebih bertanggung jawab.

4. Tips Mencegah Peretasan

Berikut beberapa tips yang dapat dilakukan siswa untuk mencegah terjadinya peretasan.

- Penggunaan Enkripsi data *End-To-End*.
- Menggunakan password yang kuat dan penerapan autentikasi multi faktor (MFA). Penelitian oleh Badeges & Fauzi (2023) menunjukkan bahwa penerapan MFA secara signifikan mengurangi risiko akses tidak sah ke sistem informasi.
- Waspada Phising.
- Backup* data secara rutin.
- Batasi informasi pribadi di media sosial.
- Pasang Antivirus dan *Firewall*.

Hasil dan Pembahasan

Sosialisasi kesadaran keamanan siber dalam kehidupan sehari-hari bagi siswa SMAN 10 Kota Jambi merupakan kegiatan yang penting untuk meningkatkan kesadaran siswa tentang keamanan siber dan membekali mereka dengan pengetahuan dan keterampilan untuk melindungi diri dari ancaman siber. Kegiatan ini diharapkan dapat membantu siswa untuk menggunakan internet dengan aman dan bertanggung jawab. Tujuan dari adanya kegiatan sosialisasi ini, antara lain:

- Meningkatkan kesadaran siswa tentang keamanan siber dalam kehidupan sehari-hari dan antisipasi kejahatan siber.
- Memberikan pengetahuan dan keterampilan kepada siswa untuk melindungi diri dari ancaman siber.
- Mendorong siswa untuk menggunakan internet dengan aman dan bertanggung jawab.

Kegiatan sosialisasi ini dilaksanakan pada hari Kamis, tanggal 18 September 2025. Adapun susunan acaranya dapat dilihat pada tabel berikut.

Tabel 1. Susunan Acara Kegiatan Sosialisasi Keamanan Siber

Waktu	Kegiatan
09:00-09:10	Pembukaan
09:10-09:40	Penyampaian Materi
09:40-09:55	Sesi Kuis Berhadiah
09:55-10:00	Sesi Foto
10:00-10:10	Penutup



Gambar 1. Dokumentasi Kegiatan Sosialisasi Keamanan Siber di SMAN 10 Kota Jambi

Semua siswa menunjukkan antusiasme terhadap materi yang dipaparkan, terutama ketika mempelajari contoh kasus nyata terkait serangan siber yang sering terjadi di kalangan pengguna remaja, seperti penipuan tautan, pembobolan akun media sosial, dan penyebaran perangkat lunak berbahaya. Materi yang disampaikan meliputi pentingnya menjaga data pribadi, jenis-jenis serangan siber yang sering ditemukan di kehidupan sehari-hari, potensi ancaman dari kelalaian pengguna, serta langkah-langkah sederhana untuk mencegah risiko kebocoran data dan penyalahgunaan akun. Seluruh materi tersebut disusun secara sistematis dan dijelaskan melalui presentasi interaktif agar mudah dipahami oleh siswa.

Sebelum penutup kegiatan, tim pelaksana membagikan kuesioner kepada siswa untuk menilai tingkat pemahaman siswa terhadap materi yang disampaikan. Berdasarkan hasil kuesioner, sosialisasi keamanan siber di SMAN 10 Jambi dapat dinilai cukup efektif karena mayoritas siswa menunjukkan peningkatan kesadaran akan risiko digital, seperti penggunaan kata sandi kuat dan kehati-hatian terhadap penipuan *online*. Metode sosialisasi yang interaktif dan praktis terbukti efektif dalam meningkatkan pemahaman dan kesadaran keamanan siber siswa. Simulasi serangan siber dan studi kasus nyata membantu peserta memahami situasi yang mungkin dihadapi dalam dunia nyata. Dengan demikian, sosialisasi dapat dikatakan berhasil pada tahap peningkatan kesadaran awal, tetapi perlu dirancang lebih terstruktur, aplikatif, dan berulang untuk memastikan perubahan perilaku yang konsisten dalam menjaga keamanan siber oleh remaja.

Simpulan

Sosialisasi keamanan siber di SMAN 10 Jambi berhasil meningkatkan pemahaman awal siswa mengenai ancaman digital dan cara pencegahannya. Kegiatan ini memberikan materi terstruktur tentang jenis serangan, ancaman internal, serta langkah praktis perlindungan data, dan ditunjang dengan sesi interaktif serta evaluasi melalui kuis. Hasil kuesioner menunjukkan adanya peningkatan kesadaran siswa dalam penggunaan kata sandi yang kuat dan kewaspadaan terhadap penipuan *online*. Kegiatan serupa perlu dilakukan secara berkelanjutan untuk memastikan terbentuknya kebiasaan digital yang aman dan bertanggung jawab pada remaja.

Daftar Pustaka

- Abidde, W. N., Eyidia, N., & Eme, E. S. J. (2025). CIA Triad: A Review of Confidentiality, Integrity, and Availability. *International Research Journal of Modernization in Engineering Technology and Science*, 7(3), 12824-12828. <https://doi.org/10.56726/IRJMETS68704>
- Badeges, W., & Fauzi, M. N. (2023). Implementasi Multi Factor Authentication Pada PHPMyAdmin. *TRIPLE A: Jurnal Pendidikan Teknologi Informasi*, 2(1), 35-39.
- Budiyanto, D., & Mabururi, M. (2025). Pentingnya Keamanan Siber dalam Era Digital: Tinjauan Global dan Kondisi di Indonesia. *Prosiding Seminar Nasional Sains Dan Teknologi Seri III Fakultas Sains Dan Teknologi, Universitas Terbuka*, 2(1), 981-994.
- Cuhanazriansyah, M. R. (2025). Dari Gamer ke Guardian: Peningkatan Kesadaran Generasi Muda dalam Keamanan Dunia Siber. *Technologica*, 4(2), 100-108.

- E, A. D. (2025). *Prediksi Lanskap Keamanan Siber Asia-Pasifik 2025, dari Deepfake hingga Transparansi AI*. Kompas.Com. <https://tekno.kompas.com/read/2025/01/22/12020027/prediksi-lanskap-keamanan-siber-asia-pasifik-2025-dari-deepfake-hingga#:~:text=Berdasarkan laporan National Cyber Security Index %28NC SI%29%2C skor,menjadi prioritas bagi organisasi%2C baik pemerintah maup>
- Erdiyanto, R. P. (2023). Penipuan Mengatasnamakan Bank Berbentuk Phising. *Jurnal Inovasi Global*, 1(2), 76. <https://jig.rivierapublishing.id/index.php/rv/index>
- Kompas.com. (2025). *Riset: Semester I 2025, Indonesia Alami 133,4 Juta Serangan Siber*. Kompas.Com. <https://tekno.kompas.com/read/2025/08/26/17450097/riset--semester-i-2025-indonesia-alami-133-4-juta-serangan-siber>
- Kristianti, N., & Kurniasi, R. (2024). Peraturan dan Regulasi Keamanan Siber di Era Digital. *Satya Dharma : Jurnal Ilmu Hukum*, 7(1), 297-310. <https://ejournal.iahntp.ac.id/index.php/satya-dharma/article/view/1243>
- Microsoft Security. (2025). *Apa itu Ransomware?* Microsoft. <https://www.microsoft.com/id-id/security/business/security-101/what-is-ransomware>
- Muslim, Sephira, A., Abrar, M. H., Angin, S. L. S. P., & Hidayatullah, H. (2024). Analisis Keamanan Siber (Cyber Security) Dalam Era Digital “Tantangan Dan Strategi Pengamanan.” *Jurnal Ilmu Komputer Revolusioner*, 8(2), 43-52. <https://com.ojs.co.id/index.php/jikr/article/view/116/129>
- Pasha, D., Rahayu, M., Sulistiani, H., Suhartanto, A., Sobirin, M. H., Sangha, Z. K., & Aryatama, F. A. (2024). Pelatihan Keamanan Jaringan dan Antisipasi Kejahatan Siber bagi Siswa SMK N 1 Padang Cermin, Lampung. *Dharma Nusantara: Jurnal Ilmiah Pemberdayaan Dan Pengabdian Kepada Masyarakat*, 2(1), 15-19. <https://doi.org/10.32664/dharma.v2i1.1343>
- Pureti, N. (2022). Insider Threats: Identifying and Preventing Internal Security Risks. *International Journal of Advanced Engineering Technologies and Innovations*, 01(02), 98-132. <https://media.neliti.com/media/publications/603776-insider-threats-identifying-and-preventi-afa338c5.pdf>
- Ray, G., McDermott, C. D., & Nicho, M. (2024). Cyberbullying on Social Media: Definitions, Prevalence, and Impact Challenges. *Journal of Cybersecurity*, 10(1). <https://doi.org/10.1093/cybsec/tyae026>
- Sari, R. P. (2024). *Apa itu Malware? Jenis dan Cara Pencegahannya*. Cloud Computing Indonesia. <https://www.cloudcomputing.id/pengetahuan-dasar/apa-itu-malware-jenis>
- Sovina, M., Harahap, F. A., Lazuly, I., & Khalid, M. A. (2024). Pelatihan Edukasi Macam-Macam Tindak Kejahatan Teknologi Informasi (Cyber Crime) Dunia Maya dan Penanganannya. *PUBLIDIMAS (Publikasi Pengabdian Masyarakat)*, 4(1), 74-83. <https://www.doi.org/10.22303/publidimas.1.1.2021.01-10>
- Yi, J., & Tian, Y. (2024). Insider Threat Detection Model Enhancement Using Hybrid Algorithms between Unsupervised and Supervised Learning. *Electronics (Switzerland)*, 13(5). <https://doi.org/10.3390/electronics13050973>
- Yusuf, S. M., & Kamariah, S. (2025). Transformasi Digital dalam Pendidikan: Analisis Literatur terhadap Implikasi Teknologi terhadap Praktik Kependidikan. *Al-Zayn : Jurnal Ilmu Sosial & Hukum*, 3(2), 1240-1248. <https://doi.org/10.61104/alz.v3i2.1356>
- Zein, H. H. (2025). *Melindungi Gen Z sebagai Generasi Digital dari Ancaman Siber*. retizen.republika.co.id. <https://retizen.republika.co.id/posts/528738/melindungi-gen-z-sebagai-generasi-digital-dari-ancaman-siber#:~:text=Badan Siber dan Sandi Negara %28BSSN%29 melaporkan 12.691,platform daring untuk tugas kuliah dan jejaring sosial.>