

Pengenalan Firewall, Antivirus, dan Enkripsi untuk Keamanan Siber Studi Kasus: SMAN 11 Kota Jambi

Nanda Rizqi Maharani, M. Dzikri Albani, Muliana
UIN Sultan Thaha Saifuddin Jambi
Email : nandaaarizqimaharani@gmail.com

ABSTRAK

Dalam dunia yang serba digital, risiko siber kini menjadi salah satu masalah yang serius yang dapat mengancam berbagai bidang, termasuk lembaga pendidikan. Penelitian ini bertujuan untuk memberikan sosialisasi dan meningkatkan pemahaman siswa terhadap konsep dasar keamanan siber, yaitu firewall, antivirus, dan enkripsi, sebagai langkah perlindungan diri di dunia maya. Kegiatan dilakukan di SMAN 11 Kota Jambi dengan melibatkan 50 siswa kelas XI menggunakan metode sosialisasi edukatif berbasis participatory learning.

Studi ini mengadopsi metode kuantitatif deskriptif dengan menggunakan pre-test dan post-test untuk menilai seberapa jauh pengetahuan siswa sebelum dan setelah sosialisasi dilakukan. Temuan menunjukkan adanya peningkatan yang signifikan pada tingkat pemahaman siswa, di mana rata-rata kenaikannya dari 30-40% pada pre-test meningkat menjadi 85% pada post-test. Selain dari peningkatan ilmu, terjadi pula perubahan perilaku siswa terkait keamanan digital, di mana mereka lebih peka terhadap potensi ancaman siber dan lebih proaktif dalam menerapkan langkah-langkah untuk melindungi data pribadi mereka.

Hasil penelitian ini menegaskan bahwa pendekatan sosialisasi yang berbasis partisipatif terbukti efektif dalam meningkatkan kesadaran akan literasi keamanan siber di kalangan siswa. Dengan demikian, kegiatan seperti ini dapat menjadi model edukasi keamanan digital yang relevan dan berkelanjutan bagi institusi pendidikan dalam mendukung budaya keamanan siber nasional.

Kata Kunci: Keamanan Siber, Firewall, Antivirus, Enkripsi, Literasi Digital

ABSTRACT

In the digital era, cyber threats have become a serious challenge affecting various sectors, including educational institutions. This study aims to introduce and enhance students' understanding of basic cybersecurity concepts firewall, antivirus, and encryption as essential measures for online protection. The activity was conducted at SMAN 11 Kota Jambi, involving 50 eleventh-grade students through an educational socialization program using the participatory learning approach.

A quantitative descriptive method was employed using pre-test and post-test instruments to measure students' knowledge levels before and after the socialization. The results indicated a significant improvement in students' understanding, with average scores increasing from 30-40% in the pre-test to 85% in the post-test. Moreover, students demonstrated positive behavioral changes toward digital safety, becoming more cautious about cyber risks and more proactive in protecting their personal data.

These findings suggest that participatory-based socialization is effective in improving cybersecurity literacy among high school

Article History

Received: November 2025
Reviewed: November 2025
Published: November 2025

Plagiarism Checker No 585
Prefix DOI: Prefix DOI:
10.8734/sindoro.v1i2.360
Copyright: Author
Publish by: SINDORO



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

students. Therefore, similar programs can serve as an effective and sustainable model for promoting digital security awareness in educational environments and supporting the development of a national cybersecurity culture.

Keywords: *Cybersecurity, Firewall, Antivirus, Encryption, Digital Literacy*

PENDAHULUAN

Dalam zaman digital yang saling terhubung, aktivitas manusia tidak dapat dipisahkan dari penggunaan informasi dan komunikasi teknologi. Hampir seluruh kegiatan belajar, administrasi, dan interaksi sosial kini dilakukan melalui perangkat digital yang terhubung ke jaringan internet. Namun, kemudahan ini juga diikuti oleh meningkatnya ancaman siber yang dapat menyerang siapa pun, termasuk institusi pendidikan (Ariffin et al., 2022). Serangan siber seperti *phishing*, *malware*, dan *ransomware* telah banyak menyasar sekolah dan universitas karena lemahnya sistem keamanan serta rendahnya kesadaran pengguna terhadap praktik keamanan digital (Yeboah-Boateng & Amanor, 2014).

Sekolah, sebagai lembaga yang menyimpan berbagai data pribadi peserta didik dan guru mulai dari data identitas, nilai akademik, hingga informasi keuangan menjadi target potensial bagi pelaku kejahatan siber. Kebocoran data sekolah dapat menimbulkan dampak serius seperti penyalahgunaan informasi pribadi dan kerugian reputasi lembaga pendidikan (Mansfield-Devine, 2019). Oleh karena itu, penting bagi siswa SMA untuk memahami konsep dasar keamanan siber, seperti *firewall*, *antivirus*, dan *enkripsi* sebagai bentuk perlindungan diri di dunia maya (Kumar & Rajasekar, 2021).

Firewall berfungsi sebagai penghalang pertama yang menyaring lalu lintas jaringan antara komputer pengguna dan internet, sehingga dapat mencegah akses tidak sah ke sistem (Garg et al., 2022). *Antivirus* bekerja untuk mendeteksi dan menghapus perangkat lunak berbahaya yang dapat mencuri data atau merusak perangkat komputer (Kumar et al., 2020). Sementara itu, *enkripsi* memastikan bahwa data yang dikirim atau disimpan hanya dapat diakses oleh pihak yang berwenang melalui proses penyandian informasi (Rahmawati & Nugroho, 2023).

Tujuan dari sosialisasi yang diadakan di SMAN 11 Kota Jambi adalah untuk memperbaiki literasi digital dan meningkatkan kesadaran akan keamanan siber bagi para siswa, supaya mereka mampu memanfaatkan teknologi dengan cara yang aman, bertanggung jawab, dan produktif. Kegiatan ini tidak hanya menanamkan pengetahuan teknis, tetapi juga membangun sikap kritis terhadap ancaman digital yang sering kali tersembunyi dalam aktivitas daring sehari-hari, seperti penggunaan media sosial atau pengunduhan aplikasi (Sari & Kurniawan, 2020).

Upaya sosialisasi ini juga selaras dengan Strategi Nasional Keamanan Siber Indonesia, yang menekankan pentingnya peran pendidikan dalam membangun budaya keamanan digital di masyarakat (Rahmawati & Nugroho, 2023). Dengan demikian, pembekalan pemahaman tentang *firewall*, *antivirus*, dan *enkripsi* di lingkungan sekolah menjadi langkah strategis dalam menciptakan generasi muda yang memiliki kesadaran dan kemampuan menjaga keamanan data pribadi di dunia maya.

METODE PENELITIAN

Metode yang dipakai dalam kegiatan ini adalah sosialisasi berbasis pendidikan dengan pendekatan pembelajaran partisipatif, di mana peserta tidak hanya mendengarkan, tetapi juga aktif terlibat dalam proses belajar (Sugiyono, 2021). Pendekatan ini dipilih karena sesuai dengan karakter siswa SMA yang lebih cepat memahami konsep melalui interaksi langsung dan kegiatan praktis. Dengan metode ini, diharapkan para siswa dapat menginternalisasi prinsip dasar keamanan siber dan mempraktekannya dalam kehidupan sehari-hari.

Penelitian ini dilakukan di SMAN 11 Kota Jambi dengan seluruh siswa kelas XI sebagai populasi dan sebanyak 50 siswa dipilih melalui purposive sampling, berdasarkan ketersediaan waktu dan kesiapan mereka untuk mengikuti sosialisasi. Kegiatan berlangsung selama dua hari dengan pembagian sesi yang terstruktur: sesi teori, demonstrasi, dan evaluasi.

1. Tahapan Kegiatan

a. Tahap Persiapan

Pada tahap ini, koordinasi dengan pihak sekolah dilakukan, materi sosialisasi disusun, serta alat penelitian berupa kuesioner pre-test dan post-test dibuat. Materi sosialisasi difokuskan pada tiga topik utama, yaitu:

- Pengertian dan fungsi *firewall* dalam melindungi jaringan sekolah dari ancaman eksternal.
- Pentingnya penggunaan *antivirus* dalam perangkat pribadi maupun perangkat sekolah untuk mendeteksi dan menghapus malware.
- Prinsip dasar *enkripsi* data untuk menjaga kerahasiaan informasi pribadi dan institusi.

b. Tahap Pelaksanaan Sosialisasi

Sosialisasi dilakukan menggunakan kombinasi metode ceramah interaktif, demonstrasi langsung, dan diskusi kelompok kecil. Dalam sesi ceramah, pemateri menjelaskan teori dasar keamanan siber dengan contoh-contoh nyata kasus kebocoran data di lingkungan pendidikan (Rahmawati & Nugroho, 2023). Sesi demonstrasi mencakup praktik mengaktifkan *firewall*, menjalankan pemindaian *antivirus*, serta mengenkripsi file sederhana menggunakan perangkat lunak umum.

Pendekatan *participatory learning* diterapkan dengan melibatkan siswa untuk berdiskusi, bertanya, serta mencoba langsung setiap langkah yang diajarkan. Kegiatan ini mendorong munculnya pembelajaran kolaboratif dan meningkatkan kemampuan berpikir kritis siswa dalam menghadapi ancaman digital (Sari & Kurniawan, 2020).

c. Tahap Evaluasi dan Refleksi

Untuk mengukur efektivitas kegiatan, data dikumpulkan melalui kuesioner pre-test dan post-test yang berisi 20 pertanyaan pilihan ganda tentang firewall, antivirus, dan enkripsi. Hasil dari pre-test digunakan untuk menilai tingkat pengetahuan awal siswa sebelum sosialisasi dilakukan, sedangkan post-test digunakan untuk menilai peningkatan pengetahuan mereka setelah kegiatan selesai.

Data yang diperoleh kemudian dianalisis menggunakan pendekatan deskriptif kuantitatif, dengan cara membandingkan skor rata-rata pre-test dan post-test (Sugiyono, 2021). Analisis ini bertujuan untuk menggambarkan secara objektif perubahan tingkat pemahaman siswa setelah mendapatkan intervensi berupa sosialisasi edukatif.

2. Validitas dan Keabsahan Data

Untuk menjaga validitas instrumen, kuesioner divalidasi oleh dua ahli pendidikan teknologi informasi dan seorang praktisi keamanan siber. Uji reliabilitas dilakukan menggunakan metode Cronbach's Alpha, dengan nilai yang diharapkan $\geq 0,7$ untuk menunjukkan konsistensi internal yang baik (Sugiyono, 2021).

3. Dokumentasi dan Observasi

Selain data kuantitatif, dokumentasi kegiatan seperti foto, rekaman video, dan catatan observasi lapangan juga dikumpulkan untuk memberikan gambaran kualitatif mengenai partisipasi siswa selama kegiatan berlangsung. Observasi dilakukan untuk melihat antusiasme, tingkat keaktifan, serta kemampuan siswa dalam menerapkan praktik keamanan digital secara langsung.

Dengan metode yang terstruktur dan pendekatan partisipatif ini, kegiatan sosialisasi tidak hanya memberikan pengetahuan teoritis, tetapi juga melatih keterampilan praktis siswa dalam menjaga keamanan data dan perangkat mereka. Hasilnya diharapkan dapat memberikan kontribusi nyata terhadap peningkatan kesadaran dan perilaku aman dalam penggunaan teknologi di lingkungan pendidikan.

HASIL DAN PEMBAHASAN

Hasil dari kegiatan sosialisasi yang dilakukan di SMAN 11 Kota Jambi menunjukkan adanya peningkatan yang signifikan dalam pemahaman dan kesadaran siswa terhadap konsep dasar keamanan siber. Dari data yang diperoleh melalui pre-test dan post-test, sebelum kegiatan berlangsung, hanya 30% siswa yang mengetahui fungsi dari firewall, 40% siswa yang menyadari manfaat dari antivirus, dan 25% siswa yang memahami konsep dasar enkripsi. Namun, setelah sosialisasi dilaksanakan, tingkat pemahaman ini melonjak drastis hingga mencapai 85% pada post-test. Kenaikan ini menunjukkan efektivitas metode pembelajaran partisipatif dalam edukasi digital (Sugiyono, 2021).

Kegiatan sosialisasi terbukti mampu mengubah cara pandang siswa terhadap pentingnya keamanan siber. Sebelum kegiatan, sebagian besar siswa menganggap bahwa ancaman siber hanya menyangkut instansi besar seperti perusahaan atau lembaga pemerintahan. Namun setelah mendapat penjelasan dan simulasi, mereka memahami bahwa ancaman siber dapat menyerang siapa pun, termasuk pengguna individu dan institusi pendidikan (Ariffin et al., 2022). Kesadaran baru ini tercermin dari peningkatan skor pemahaman serta tingginya antusiasme siswa dalam sesi diskusi.

1. Pemahaman Konsep Firewall

Dari hasil observasi, siswa menunjukkan pemahaman yang lebih baik terhadap fungsi *firewall* setelah mengikuti demonstrasi interaktif. Mereka memahami bahwa *firewall* bukan sekadar perangkat lunak tambahan, melainkan komponen penting dalam melindungi jaringan komputer dari akses tidak sah dan serangan eksternal (Mansfield-Devine, 2019). Siswa juga diberikan contoh nyata bagaimana *firewall* dapat memblokir situs berbahaya atau upaya peretasan yang mencoba masuk melalui jaringan Wi-Fi sekolah. Hal ini memperkuat kesadaran mereka akan pentingnya konfigurasi jaringan yang aman, bahkan di lingkungan pendidikan.

2. Pemahaman dan Penggunaan Antivirus

Hasil post-test memperlihatkan peningkatan yang signifikan dalam pengertian siswa mengenai peran antivirus. Sebelumnya, sebagian besar siswa menganggap *antivirus* hanya berfungsi untuk menghapus virus komputer. Setelah sosialisasi, siswa mampu menjelaskan bahwa *antivirus* juga berperan dalam mendeteksi, mengisolasi, dan mencegah malware serta serangan berbahaya lainnya seperti *spyware* dan *ransomware* (Yeboah-Boateng & Amanor, 2014). Selain itu, siswa juga belajar pentingnya melakukan *update* berkala pada perangkat lunak *antivirus* agar dapat mengenali jenis ancaman baru yang terus berkembang (Garg et al., 2022).

Demonstrasi penggunaan *antivirus* pada laptop sekolah memberikan pengalaman langsung bagi siswa tentang bagaimana perangkat lunak tersebut bekerja, mulai dari proses pemindaian (*scanning*), identifikasi ancaman, hingga penghapusan file berbahaya. Pembelajaran berbasis praktik ini membantu meningkatkan pemahaman sekaligus keterampilan teknis siswa.

3. Pemahaman Konsep Enkripsi

Pemahaman siswa terhadap *enkripsi* juga meningkat signifikan. Sebelumnya, hanya sedikit siswa yang mengenal istilah tersebut dan cenderung menganggap *enkripsi* sebagai hal yang kompleks dan hanya digunakan oleh profesional IT. Usai sesi penjelasan dan simulasi, siswa mulai mengerti bahwa enkripsi adalah proses yang digunakan untuk mengamankan data sehingga informasi yang dikirim atau disimpan tidak dapat diakses oleh pihak yang tidak memiliki izin (Kumar et al., 2020).

Melalui demonstrasi sederhana menggunakan perangkat lunak *file encryption*, siswa diperlihatkan bagaimana data yang awalnya dapat dibaca berubah menjadi teks acak yang tidak dapat dimengerti tanpa kunci dekripsi. Pemahaman ini sangat penting mengingat banyak siswa yang sering mengunggah dan berbagi file pribadi melalui platform daring tanpa memperhatikan aspek keamanannya.

4. Dampak Sosialisasi terhadap Sikap dan Kesadaran Siswa

Selain peningkatan pengetahuan, hasil observasi selama kegiatan menunjukkan perubahan sikap positif terhadap keamanan digital. Siswa menjadi lebih berhati-hati dalam menggunakan perangkat digital, terutama saat mengunduh file, mengakses situs web, dan membagikan informasi pribadi secara daring. Mereka juga menunjukkan ketertarikan yang besar untuk menerapkan langkah-langkah perlindungan digital, seperti menggunakan kata sandi yang kuat dan secara rutin memperbarui aplikasi keamanan (Sari & Kurniawan, 2020).

Hal ini sejalan dengan temuan Rahmawati & Nugroho (2023) yang mengungkapkan bahwa peningkatan kesadaran akan keamanan siber di tingkat pendidikan menengah dapat membangun budaya keamanan digital di kalangan para pelajar. Dengan demikian, kegiatan sosialisasi semacam ini berpotensi menjadi model pembelajaran efektif untuk diterapkan di sekolah lain.

5. Interpretasi dan Implikasi

Secara keseluruhan, peningkatan pemahaman siswa sebesar 55-60% setelah kegiatan menunjukkan bahwa metode sosialisasi edukatif berbasis partisipatif sangat efektif dalam membangun literasi keamanan siber di kalangan remaja. Hasil ini juga mengindikasikan bahwa pendidikan formal dapat berperan sebagai garda terdepan dalam memperkuat pertahanan siber nasional (Rahmawati & Nugroho, 2023).

Temuan ini mendukung teori literasi digital yang dikemukakan oleh Garg et al. (2022), bahwa pembelajaran yang mengintegrasikan teori dan praktik secara langsung akan lebih berdampak terhadap perubahan perilaku pengguna. Oleh karena itu, kegiatan seperti ini perlu dikembangkan secara berkelanjutan melalui kerja sama antara sekolah, pemerintah, dan lembaga keamanan siber agar tercipta ekosistem pendidikan yang aman dan sadar digital.

KESIMPULAN

Kegiatan sosialisasi mengenai pengenalan firewall, antivirus, dan enkripsi yang dilaksanakan di SMAN 11 Kota Jambi berhasil mencapai tujuannya, yaitu meningkatkan pemahaman dan kesadaran siswa terhadap pentingnya keamanan siber di lingkungan pendidikan. Hasil analisis mengindikasikan bahwa terdapat peningkatan yang signifikan dalam pemahaman siswa setelah dilaksanakan kegiatan, dengan rerata peningkatan pemahaman mencapai 85% berdasarkan hasil tes akhir.

Melalui metode participatory learning, siswa tidak hanya memperoleh pemahaman teoritis, tetapi juga keterampilan praktis dalam menerapkan konsep keamanan digital. Mereka mampu memahami fungsi firewall sebagai pelindung jaringan dari akses tidak sah, peran antivirus dalam mendeteksi dan menghapus malware, serta pentingnya enkripsi untuk menjaga kerahasiaan data pribadi.

Selain peningkatan pengetahuan, sosialisasi ini juga menumbuhkan sikap positif dan perilaku aman dalam penggunaan teknologi digital. Siswa menjadi lebih berhati-hati dalam berbagi informasi daring, memanfaatkan kata sandi yang kuat, dan rutin memperbarui perangkat lunak keamanan.

Secara keseluruhan, kegiatan ini memperlihatkan bahwa pendekatan pendidikan yang melibatkan partisipasi sangat berpengaruh dalam meningkatkan literasi keamanan siber di kalangan siswa SMA. Diharapkan kegiatan serupa dapat dilakukan secara berkelanjutan di berbagai lembaga pendidikan untuk memperkuat budaya keamanan digital dan mendukung program perlindungan data serta keamanan siber nasional di Indonesia.

DAFTAR PUSTAKA

- Ariffin, M., Ahmad, R., & Rosli, N. (2022). Cybersecurity Awareness in Educational Institutions. *Journal of Information Security Education*, 15(2), 45-59.
- Garg, P., Singh, R., & Sharma, N. (2022). Cybersecurity Education in Schools: Challenges and Solutions. *Education and Information Technologies*, 27(5), 6333-6350. <https://doi.org/10.1007/s10639-022-10945-1>
- Kumar, A., & Rajasekar, R. (2021). Understanding Cyber Hygiene among Students. *Cybersecurity Research Review*, 9(4), 102-110.
- Kumar, S., Singh, R., & Gupta, P. (2020). Encryption Techniques for Data Security. *International Journal of Cyber Studies*, 8(3), 34-48. <https://doi.org/10.1016/j.ijcs.2020.03.004>
- Mansfield-Devine, S. (2019). Firewall Fundamentals and Network Protection. *Network Security Journal*, 2019(7), 6-11. [https://doi.org/10.1016/S1353-4858\(19\)30094-2](https://doi.org/10.1016/S1353-4858(19)30094-2)
- Rahmawati, S., & Nugroho, T. (2023). Implementasi Strategi Keamanan Siber Nasional di Dunia Pendidikan. *Jurnal Keamanan Digital Indonesia*, 4(1), 12-25.

- Sari, D., & Kurniawan, H. (2020). Peran Literasi Digital dalam Pencegahan Kejahatan Siber pada Pelajar SMA. *Jurnal Teknologi dan Pendidikan*, 3(2), 77-88.
- Sugiyono. (2021). *Metode Penelitian Pendidikan: Pendekatan Kuantitatif, Kualitatif, dan R&D*. Bandung: Alfabeta.
- Yeboah-Boateng, E. O., & Amanor, P. M. (2014). Phishing, SMiShing & Vishing: An Assessment of Threats for Mobile Devices. *International Journal of Computer Applications*, 84(5), 1-9. <https://doi.org/10.5120/14673-2661>
- Ignatenko, A. I. (2024). *Metode Perlindungan Informasi Pengguna di Ruang Digital: Tugas Akhir (Skripsi Sarjana) Program Studi Keamanan Siber*. Universitas Nasional Odessa. Diakses dari <https://dspace.onua.edu.ua/items/828540fa-df35-4696-bdd3-4ebbacb52eb>