

MEMBANGUN KESADARAN KEAMANAN DIGITAL: SOSIALISASI FIREWALL, ANTIVIRUS, DAN ENSKRIPSI BAGI SISWA MIN 4 MUARO JAMBI

Firmansyah Setiawan, Muhammad Rozi, Muhammad Fiqry

UIN Sultan Thaha Saifuddin Jambi

Email : firmansyahsetiawan21@gmail.com, rozim862@gmail.com, mf0646573@gmail.com

Abstrak

Kegiatan sosialisasi keamanan digital ini bertujuan untuk meningkatkan pemahaman siswa MIN 4 Muaro Jambi mengenai konsep dasar pertahanan sistem informasi melalui pengenalan firewall, antivirus, dan enkripsi. Sosialisasi dilaksanakan melalui pendekatan edukatif yang disesuaikan dengan tingkat perkembangan siswa sekolah dasar. Melalui observasi dan evaluasi sederhana, kegiatan ini menunjukkan peningkatan pemahaman siswa terhadap pentingnya perlindungan data dan penggunaan perangkat digital secara aman. Artikel ini membahas latar belakang kebutuhan edukasi keamanan digital, metode yang digunakan selama kegiatan sosialisasi, serta hasil pemahaman siswa setelah menerima materi.

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

Abstract

This digital security outreach program aims to enhance the understanding of MIN 4 Muaro Jambi students regarding fundamental information system protection through the introduction of firewall, antivirus, and encryption concepts. The activities were conducted using an educational approach tailored to the developmental level of elementary school students. Based on observations and simple evaluations, the program demonstrated an improvement in students' awareness of data protection and safe digital practices. This article discusses the background of the need for digital security education, the methods applied during the outreach activities, and the students' level of understanding after receiving the material.

Keywords: Digital Security; Firewall; Antivirus; Encryption; Cyber Literacy

Article History

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

Plagiarism Checker No 589
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/).

PENDAHULUAN

Berangkat dari meningkatnya penggunaan perangkat digital di kalangan anak usia sekolah dasar, kebutuhan akan literasi keamanan informasi menjadi semakin mendesak. Perubahan perilaku digital pada generasi muda menunjukkan bahwa aktivitas mereka tidak lagi terbatas pada hiburan, tetapi juga mencakup pembelajaran, interaksi sosial, serta pertukaran informasi berbasis daring. Kondisi ini sejalan dengan temuan bahwa anak-anak menjadi pengguna internet yang aktif sejak usia dini, namun sering kali belum dibekali pemahaman memadai mengenai risiko dunia maya (Livingstone, 2014). Penelitian lain menunjukkan bahwa kelompok usia ini termasuk yang paling rentan terhadap ancaman digital, seperti malware, pencurian identitas, penipuan berbasis tautan, serta paparan konten yang tidak sesuai usia (Haddon, 2017; Jones, 2018). Kerentanan tersebut diperparah oleh rendahnya literasi keamanan digital di tingkat sekolah dasar, sehingga diperlukan intervensi edukatif yang sistematis dan terarah sejak dini (Ribble, 2015; Park, 2016).

Dalam konteks tersebut, kegiatan sosialisasi keamanan digital di MIN 4 Muaro Jambi dirancang sebagai respons terhadap urgensi membangun kompetensi dasar perlindungan

informasi pada anak-anak. Pemilihan materi tentang firewall, antivirus, dan enkripsi tidak dilakukan secara acak, melainkan berdasarkan perannya yang fundamental dalam menjaga integritas dan keamanan data. Firewall berfungsi sebagai pengatur lalu lintas jaringan untuk mencegah akses tidak sah, sementara antivirus bertindak sebagai mekanisme deteksi dan pencegahan terhadap perangkat lunak berbahaya yang sering menjadi ancaman bagi pengguna muda (Ding, 2020). Di sisi lain, enkripsi diperkenalkan sebagai teknik penyandian data yang memastikan informasi pribadi tetap terlindungi, sebuah prinsip penting dalam menjaga privasi di era digital (Smith, 2019).

Pengenalan ketiga konsep ini dalam bentuk pembelajaran yang ringan, visual, dan sesuai tahap perkembangan kognitif siswa menjadi langkah strategis untuk menumbuhkan kesadaran digital yang bertanggung jawab. Hal ini sejalan dengan penelitian yang menegaskan bahwa pendekatan edukatif berbasis praktik dan pengalaman langsung lebih efektif dalam meningkatkan pemahaman anak mengenai keamanan digital (Çelik, 2021). Dengan demikian, kegiatan sosialisasi ini tidak hanya memberikan pengetahuan teknis, tetapi juga membangun fondasi perilaku digital yang aman, etis, dan berkelanjutan di lingkungan sekolah dasar.

METODE PENELITIAN

A. Pendekatan Edukatif

Kegiatan sosialisasi ini menerapkan pendekatan edukatif yang berorientasi pada pembelajaran aktif dan partisipatif. Pendekatan ini dipilih karena anak usia sekolah dasar cenderung lebih mudah memahami konsep abstrak ketika disertai contoh konkret, visual, dan aktivitas langsung (Bransford et al., 2000). Penyampaian materi tentang firewall, antivirus, dan enkripsi dibuat interaktif melalui penggunaan gambar, animasi sederhana, serta demonstrasi alat peraga yang mampu membantu siswa membangun pemahaman intuitif terhadap mekanisme dasar keamanan digital. Pendekatan ini sejalan dengan prinsip *learning by doing*, yang terbukti meningkatkan retensi pengetahuan pada anak-anak (Kolb, 2014).

B. Metode Penyampaian

1. Presentasi dan diskusi kelas (10-15 menit per topik)

- a. Tujuan: memberi definisi dasar dan contoh nyata.
- b. Teknik: tanya jawab terbuka, mendorong siswa memberi contoh dari pengalaman mereka.

Materi disampaikan melalui presentasi yang menggunakan bahasa sederhana dan visual yang menarik agar sesuai dengan tingkat perkembangan kognitif siswa sekolah dasar. Diskusi didorong untuk memberi ruang bagi siswa bertanya dan menyampaikan pengalaman mereka terkait aktivitas digital. Metode ini efektif dalam memperkuat pemahaman konseptual dan meningkatkan keterlibatan peserta (Chi, 2009).

2. Simulasi sederhana cara kerja firewall dan antivirus (15-20 menit)

Simulasi dilakukan menggunakan analogi gerbang keamanan atau *gatekeeper* untuk menjelaskan cara firewall menyaring lalu lintas data, serta permainan identifikasi “virus” untuk menggambarkan fungsi antivirus. Model simulatif seperti ini terbukti membantu anak memahami konsep teknologi yang sulit dengan cara yang konkret dan menyenangkan (Smetana & Bell, 2012). Melalui simulasi, siswa dapat

memvisualisasikan bagaimana sistem digital melindungi perangkat mereka dari ancaman.

- Firewall: gunakan permainan “gerbang” – beberapa siswa berperan sebagai perangkat, beberapa sebagai paket/data; fasilitator menempatkan aturan (kartu hijau = boleh lewat, merah = diblokir) sehingga siswa melihat bagaimana lalu lintas terfilter.
- Antivirus: permainan deteksi—beberapa kartu berlabel “virus”; siswa belajar mengenali ciri dan “menghapus” virus tersebut melalui tindakan yang telah disepakati.

3. Ilustrasi konsep enkripsi menggunakan sandi huruf (10-15 menit)

- Demonstrasi menyandikan pesan sederhana (mis. pindah huruf +1) lalu menukar pesan dengan teman yang harus mendekode menggunakan kunci sederhana.
- Diskusi singkat tentang mengapa hanya orang yang punya kunci yang bisa membaca pesan.

Konsep enkripsi yang bersifat abstrak dijelaskan melalui kegiatan membuat kode sederhana menggunakan sandi huruf. Aktivitas ini memperkenalkan prinsip dasar penyandian data dengan format yang mudah dipahami anak-anak. Penelitian menunjukkan bahwa pengenalan konsep kriptografi melalui permainan kode dapat meningkatkan literasi keamanan dan pemahaman tentang privasi digital sejak usia dini (Boneh & Shoup, 2020).

4. Penutup reflektif & praktik nyata (10 menit)

Siswa menulis satu komitmen perilaku aman (mis. “tidak membuka tautan dari orang tak dikenal”) dan menyampaikan kepada kelompok.

C. Peserta

Kegiatan ini diikuti oleh siswa tingkat kelas menengah di MIN 4 Muaro Jambi, yang secara perkembangan berada pada tahap operasional konkret menurut teori Piaget. Pada tahap ini, anak mulai mampu memahami hubungan sebab-akibat sederhana dan konsep logis jika disajikan melalui contoh konkret (Piaget, 1972). Oleh karena itu, pemilihan metode visual, simulatif, dan interaktif dinilai paling sesuai untuk karakteristik perkembangan peserta.

D. Instrumen Evaluasi

1. Tanya jawab

Sesi tanya jawab digunakan sebagai evaluasi formatif untuk melihat pemahaman spontan siswa terkait materi yang baru disampaikan. Teknik ini bermanfaat untuk mengukur tingkat penyerapan konsep secara cepat dan mendeteksi miskonsepsi yang mungkin muncul (Black & Wiliam, 2009).

2. Kuis ringan untuk mengukur pemahaman (pretest-posttest)

Kuis dilakukan dengan pertanyaan sederhana terkait fungsi firewall, antivirus, serta alasan pentingnya enkripsi. Evaluasi kuis membantu melihat peningkatan pemahaman secara objektif dan telah menjadi metode umum dalam mengukur efektivitas pembelajaran digital di pendidikan dasar (Shute & Rahimi, 2021).

- Format: 7-10 item kombinasi pilihan ganda dan benar-salah, disusun dengan bahasa anak-sekolah dasar.
- Contoh item:
 - a. “Firewall membantu komputer menerima semua data dari internet tanpa pilih-pilih.” (Benar/Salah)
 - b. “Apa yang harus kamu lakukan jika menerima tautan dari orang yang tidak kamu kenal?” (Pilihan: klik segera / tanyakan dulu ke guru/orangtua / abaikan)
 - c. “Enkripsi membuat pesan menjadi sulit dibaca oleh orang yang tidak punya kunci.” (Benar/Salah)
- Skor: 1 poin per jawaban benar; total dijadikan persentase.

3. Observasi keterlibatan siswa

Observasi dilakukan untuk menilai partisipasi siswa selama presentasi, simulasi, dan aktivitas kode. Keterlibatan menjadi indikator penting dalam kesuksesan program edukatif, karena tingkat partisipasi aktif berkorelasi positif dengan peningkatan literasi digital (Rosen et al., 2014). Observasi membantu memahami bagaimana siswa merespons materi serta menentukan bagian mana yang perlu penyempurnaan pada kegiatan serupa di masa mendatang.

HASIL DAN PEMBAHASAN

1. Peningkatan Pemahaman Siswa

Kegiatan sosialisasi menunjukkan adanya peningkatan pemahaman siswa terhadap konsep dasar keamanan digital. Setelah menerima materi, sebagian besar siswa mampu menjelaskan kembali fungsi utama firewall sebagai pengatur dan penjaga lalu lintas data yang mencegah akses tidak sah, serta peran antivirus dalam mendeteksi dan menangani perangkat lunak berbahaya.

Kemampuan siswa dalam menjelaskan kembali konsep tersebut mengindikasikan bahwa pendekatan interaktif yang digunakan efektif dalam memfasilitasi pemahaman teknologi dasar pada anak usia sekolah dasar. Selain itu, siswa juga menunjukkan pemahaman mengenai pentingnya tidak membuka tautan sembarangan serta menjaga kerahasiaan kata sandi. Pemahaman ini penting karena perilaku digital sehari-hari sangat berpengaruh terhadap potensi risiko keamanan yang mungkin mereka hadapi (Livingstone, 2014; Jones, 2018). Dengan demikian, peningkatan pengetahuan dasar ini menjadi indikator bahwa kegiatan sosialisasi berhasil menanamkan kesadaran awal tentang praktik keamanan digital yang sehat.

2. Respons Positif terhadap Demonstrasi

Demonstrasi dan simulasi sederhana yang diberikan mulai dari analogi firewall sebagai petugas penjaga gerbang hingga permainan identifikasi “virus” mendapat respons positif dari siswa. Mereka terlihat lebih mudah memahami alur masuknya ancaman digital ketika konsep tersebut divisualisasikan melalui contoh konkret. Respons positif ini sejalan dengan penelitian yang menegaskan bahwa metode berbasis demonstrasi dan pengalaman langsung memiliki dampak signifikan dalam meningkatkan pemahaman teknologi pada anak-anak, terutama ketika materi bersifat abstrak (Smetana & Bell, 2012). Dengan pendekatan ini, siswa tidak hanya menerima informasi secara pasif tetapi juga mengalami proses belajar yang melibatkan pengamatan, percobaan, dan interaksi langsung.

3. Tantangan

Meskipun secara umum kegiatan berjalan efektif, beberapa tantangan tetap ditemukan. Sebagian siswa masih mengalami kesulitan memahami konsep enkripsi secara mendalam. Hal ini dapat dimaklumi karena enkripsi merupakan materi yang bersifat abstrak, melibatkan konsep penyandian yang memerlukan kemampuan berpikir simbolis yang lebih tinggi. Tahap perkembangan kognitif siswa sekolah dasar cenderung masih berada pada fase operasional konkret, sehingga mereka memerlukan lebih banyak contoh visual serta latihan berulang untuk menguasai konsep tersebut (Piaget, 1972).

Di samping itu, hasil observasi menunjukkan bahwa pemahaman siswa dapat menurun jika tidak dilakukan penguatan materi secara berkala. Oleh sebab itu, sosialisasi semacam ini perlu diulang secara terjadwal agar siswa dapat mempertahankan dan meningkatkan literasi keamanan digital mereka (Ribble, 2015).

4. Pembahasan Akademik

Temuan penelitian ini sejalan dengan berbagai studi sebelumnya yang menekankan bahwa edukasi keamanan digital yang bersifat praktis dan aplikatif jauh lebih mudah dipahami oleh anak-anak dibandingkan penjelasan teoretis semata (Çelik, 2021). Metode yang menggabungkan demonstrasi, diskusi, serta kegiatan partisipatif terbukti lebih efektif dalam membangun pemahaman terhadap ancaman siber dan cara pencegahannya.

Selain itu, literasi keamanan sejak usia dini merupakan fondasi penting dalam membentuk budaya penggunaan teknologi yang aman di lingkungan pendidikan. Ketika anak-anak dibekali kemampuan memahami risiko digital serta cara melindungi diri, mereka cenderung menerapkan kebiasaan yang lebih aman dalam penggunaan perangkat digital jangka panjang (Haddon, 2017; Park, 2016). Hal ini menunjukkan bahwa kegiatan sosialisasi di MIN 4 Muaro Jambi telah memberikan kontribusi awal yang signifikan dalam meningkatkan kesiapan siswa menghadapi dunia digital yang semakin kompleks.

KESIMPULAN

Kegiatan sosialisasi keamanan digital di MIN 4 Muaro Jambi berhasil meningkatkan pemahaman siswa mengenai konsep dasar perlindungan informasi, khususnya terkait firewall, antivirus, dan enkripsi. Melalui pendekatan edukatif yang interaktif dan disesuaikan dengan tahap perkembangan kognitif anak sekolah dasar, siswa mampu memahami fungsi dasar sistem pertahanan digital serta pentingnya menerapkan perilaku aman dalam aktivitas daring. Respons positif terhadap demonstrasi dan simulasi menunjukkan bahwa metode pembelajaran berbasis pengalaman langsung efektif dalam memperkenalkan konsep teknologi yang bersifat abstrak.

Meskipun demikian, beberapa tantangan tetap muncul, terutama dalam menjelaskan konsep enkripsi yang lebih kompleks. Hal ini menunjukkan perlunya penguatan materi secara berkala agar pemahaman siswa dapat berkembang secara konsisten. Secara keseluruhan, temuan ini menegaskan pentingnya edukasi keamanan digital sejak dini sebagai langkah strategis untuk membangun kebiasaan penggunaan teknologi yang bertanggung jawab dan meningkatkan kesiapsiagaan generasi muda terhadap ancaman siber di masa depan.

DAFTAR PUSTAKA

- Bada, S., Sasse, A. M., & Nurse, J. R. (2019). *Cyber security awareness campaigns: Why do they fail?* arXiv. <https://arxiv.org/abs/1901.02672>
- Black, P., & Wiliam, D. (2009). *Developing the theory of formative assessment*. Educational Assessment, Evaluation and Accountability, 21(1), 5-31

- Boneh, D., & Shoup, V. (2020). *A graduate course in applied cryptography*
- Bransford, J. D., Brown, A. L., & Cocking, R. R. (2000). *How people learn: Brain, mind, experience, and school*. National Academy Press
- Çelik, İ. (2021). *Digital security education for children: The role of practical learning*
- Chi, M. T. H. (2009). *Active-constructive-interactive: A conceptual framework for differentiating learning activities*. Topics in Cognitive Science, 1(1), 73-105.
- Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). *Defining cybersecurity*. Technology Innovation Management Review, 4(10), 13-21. <https://timreview.ca/article/835>
- Cross, D., Lester, L., & Barnes, A. (2015). *A longitudinal study of cyberbullying and online safety behaviors among young students*. Computers in Human Behavior, 52, 1-9. <https://doi.org/10.1016/j.chb.2014.12.029>
- Ding, S. (2020). *Security threats and antivirus mechanisms in modern computing*. Journal of Cybersecurity Studies, 5(2), 45-60.
- Furnell, S., & Clarke, N. (2012). *Power to the people? The future of personal cybersecurity*. Computers & Security, 31(8), 993-1004. <https://doi.org/10.1016/j.cose.2012.08.004>
- Haddon, L. (2017). *Children's online risks: A review of evidence*. London School of Economics and Political Science.
- Jones, L. (2018). *Online safety and children's vulnerability*. Journal of Child Online Protection Studies, 12(3), 22-35.
- Kolb, D. A. (2014). *Experiential learning: Experience as the source of learning and development* (2nd ed.). Pearson Education.
- Kritzinger, E., & von Solms, S. (2010). *Cyber security for home users: A new way of protection through awareness*. Computers & Security, 29(8), 840-847. <https://doi.org/10.1016/j.cose.2010.04.004>
- Livingstone, S. (2014). *Children's digital risks and safety*. London School of Economics and Political Science.
- Park, Y. (2016). *Digital literacy and online risks in childhood*. Journal of Children and Media, 10(4), 1-15.
- Piaget, J. (1972). *Intellectual evolution from adolescence to adulthood*. Human Development, 15(1), 1-12.
- Pusey, P., & Sadara, W. (2011). *Cyberethics, cybersafety, and cybersecurity: Preservice teacher knowledge*. TechTrends, 55(4), 26-31. <https://doi.org/10.1007/s11528-011-0490-8>
- Ribble, M. (2015). *Digital citizenship in schools: Nine elements all students should know* (3rd ed.). International Society for Technology in Education.
- Rosen, L. D., et al. (2014). *Understanding technology use and engagement among students*.
- Schweitzer, D., Boleng, J., & Brown, L. (2021). *Improving cybersecurity education*. IEEE Transactions on Education, 64(2), 111-118. <https://doi.org/10.1109/TE.2020.3048447>
- Shute, V., & Rahimi, S. (2021). *Review of computerized assessment in digital learning environments*.

Siponen, M., & Oinas-Kukkonen, H. (2007). *A review of information security issues and education.* Computers & Security, 26(4), 315-318.
<https://doi.org/10.1016/j.cose.2007.03.001>