



PENINGKATAN LITERASI KEAMANAN SIBER MAHASISWA SISTEM INFORMASI MELALUI SOSIALISASI FIREWALL, ANTIVIRUS, DAN ENKRIPSI

Indah Sulistiawati¹, Muhammad Al Arif², Iwan Kurniawan³

^{1,2,3} Sistem Informasi, Universitas Islam Negeri Sulthan Thaha Saifuddin Jambi

E-mail: indahsulistiawati457@gmail.com, muhammadalarif542@gmail.com,

Iwanqu143@gmail.com

ABSTRACT

Rapid developments in the field of information technology are accompanied by increased risks of cybercrime that can threaten the security of systems and the confidentiality of information. Students, especially those enrolled in Information Systems Study Programs, are a group that actively uses digital technology, but does not yet fully possess sufficient knowledge about cyber security literacy. This study aims to increase cyber security awareness among students through outreach activities that focus on introducing the basics of firewalls, antivirus software, and encryption methods. The method applied in this research is descriptive with an educational approach, which includes the delivery of material in an interactive manner, hands-on practice, and simple demonstrations, followed by an evaluation session through discussion and question and answer sessions. These socialization activities were carried out for students in the Information Systems Study Program class E at the State Islamic University Sulthan Thaha Saifuddin University in Jambi, with 42 participants. The results of this activity show an increase in students' understanding of the basics of cybersecurity, the role of firewalls in protecting networks, the contribution of antivirus software in preventing malware, and the significance of encryption in maintaining information confidentiality. In addition, this outreach also contributed to increasing students' awareness and attitude towards implementing safer and more responsible digital security practices.

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

ABSTRAK

Perkembangan cepat teknologi informasi beriringan dengan meningkatnya ancaman kejahatan siber yang dapat memberikan risiko pada keamanan serta kerahasiaan informasi. Mahasiswa, terutama yang sedang belajar di Program Studi Sistem Informasi, merupakan kelompok yang aktif menggunakan teknologi digital, tetapi tingkat pemahaman mereka tentang keamanan siber masih belum optimal. Penelitian ini bertujuan untuk meningkatkan pengetahuan tentang keamanan siber di kalangan mahasiswa melalui kegiatan sosialisasi yang menitikberatkan pada pengenalan konsep dasar tentang firewall, antivirus, dan enkripsi. Metode yang digunakan dalam penelitian ini adalah deskriptif dengan

Article History

Received: Desember 2025

Reviewed: Desember 2025

Published: Desember 2025

Plagiarism Checker No
235

Prefix DOI :

[10.8734/Kohesi.v1i2.365](https://doi.org/10.8734/Kohesi.v1i2.365)

Copyright : Author

Publish by : Kohesi



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



pendekatan penyuluhan, yang mencakup penyampaian materi secara interaktif, praktik dan refleksi sederhana, serta evaluasi melalui diskusi dan tanya jawab. Kegiatan sosialisasi ini dilaksanakan untuk mahasiswa Program Studi Sistem Informasi kelas E di Universitas Islam Negeri Sultan Thaha Saifuddin Jambi dengan total 42 peserta. Hasil dari kegiatan tersebut menunjukkan adanya peningkatan pemahaman mahasiswa mengenai dasar-dasar keamanan siber, fungsi firewall dalam melindungi jaringan, peran antivirus dalam mencegah malware, serta pentingnya enkripsi untuk menjaga privasi. Selain itu, kegiatan ini juga berhasil meningkatkan kesadaran dan sikap mahasiswa untuk menerapkan praktik keamanan digital dengan cara yang lebih aman dan bertanggung jawab.

Kata Kunci: *Literasi Keamanan Siber, Firewall, Antivirus, Enkripsi, Sosialisasi*

1. PENDAHULUAN

Era digital yang terus berkembang menuntut adanya sistem keamanan informasi yang efektif dan andal. Seiring meningkatnya kompleksitas ancaman siber serta tingginya ketergantungan terhadap teknologi informasi, organisasi, perusahaan, maupun individu menjadi semakin rentan terhadap serangan peretas, pencurian data, dan pelanggaran privasi (Pardosi et al., 2024). Oleh karena itu, kesadaran akan pentingnya keamanan dan risiko kebocoran data, khususnya data yang bersifat rahasia dan strategis, menjadi aspek krusial dalam pemanfaatan informasi teknologi. Informasi dan data saat ini dipandang sebagai aset bernilai tinggi karena memuat berbagai detail penting tentang suatu organisasi. Kondisi tersebut memicu munculnya berbagai bentuk kejahatan di dunia maya yang dikenal sebagai kejahatan siber. Dengan semakin intensifnya kejahatan siber, diperlukan sistem keamanan informasi dan persandian yang handal untuk mencegah pencurian data dan informasi (Saputra et al., 2023).

Lingkungan jaringan saat ini tidak lagi terbatas pada infrastruktur lokal, melainkan telah berkembang menuju arsitektur berbasis komputasi awan (cloud computing) dan perangkat Internet of Things (IoT) yang saling terhubung. Perubahan ini meningkatkan potensi risiko keamanan karena semakin banyak titik akses yang dapat dimanfaatkan oleh pelaku kejahatan siber. Dalam kondisi tersebut, penerapan teknologi keamanan yang tepat menjadi sangat penting. Beberapa teknologi seperti firewall, antivirus, dan enkripsi masih menjadi elemen utama yang banyak digunakan untuk melindungi sistem dari ancaman, baik yang berasal dari luar maupun dari dalam organisasi (Nopiansa et al., 2025).

Literasi keamanan digital tidak hanya berkaitan dengan kemampuan menggunakan teknologi, tetapi juga mencakup pemahaman yang mendalam mengenai risiko di dunia digital



serta upaya mitigasinya. Pemahaman tersebut meliputi pengetahuan tentang privasi hak, penggunaan kata sandi yang kuat, kemampuan mengenali ancaman seperti phishing dan malware, serta penerapan norma dan etika dalam beraktivitas di ruang digital. Perlindungan data pribadi menjadi aspek yang sangat penting karena informasi pribadi merupakan sumber daya berharga yang dapat disalahgunakan apabila tidak dilindungi dengan baik. Pendidikan yang tepat diharapkan mampu meningkatkan kesadaran serta kemampuan generasi muda dalam menjaga privasi mereka, sekaligus membentuk budaya digital yang aman dan bertanggung jawab (Prawiro et al., 2025). Selain itu, penelitian lain menunjukkan bahwa tingkat literasi digital memiliki hubungan signifikan dengan perilaku keamanan siber di kalangan mahasiswa, sehingga pendidikan dan sosialisasi menjadi aspek penting dalam pembentukan sikap keamanan yang lebih baik (Oktapiyadi et al., 2024). Meskipun berbagai penelitian mengenai risiko siber telah banyak dilakukan, tingkat pemahaman masyarakat, khususnya di kalangan pelajar, masih tergolong rendah.

Seiring meningkatnya ancaman siber, kebutuhan akan pendekatan keamanan yang lebih komprehensif dan terintegrasi menjadi semakin mendesak. Upaya pencegahan dalam keamanan siber tidak hanya berfokus pada penggunaan perangkat dan teknologi, tetapi juga harus mencakup kebijakan, regulasi, serta pemahaman individu dan organisasi dalam melindungi informasi. Inovasi dalam perangkat keamanan, seperti firewall, enkripsi, sistem deteksi intrusi, serta metode autentikasi yang lebih aman, perlu diimbangi dengan penerapan strategi risiko manajemen yang tepat (Susilowati, 2024). Analisis terhadap kesadaran dan praktik keamanan siber di lingkungan akademik menunjukkan bahwa meskipun mahasiswa aktif menggunakan teknologi digital, terdapat celah penting dalam pemahaman dan praktik keamanan yang perlu diatasi melalui intervensi edukatif yang berkelanjutan (Sussolaikah et al., 2024).

Firewall merupakan komponen penting dari keamanan jaringan yang menjadi penghalang awal yang melindungi dari ancaman siber dan pengguna yang tidak berwenang. Firewall berada di garis depan keamanan jaringan dengan memantau lalu lintas dan menerapkan aturan keamanan yang telah ditentukan antara lalu lintas masuk dan keluar (Chopra, 2016 dalam Miracle, 2024). SMADAV Antivirus adalah solusi yang efektif untuk melindungi sistem operasi Windows dari ancaman malware, khususnya virus lokal. Namun, perlu perawatan rutin dan perlu diingat bahwa SMADAV tidak dapat mendeteksi semua jenis malware. Oleh karena itu, pengguna harus memastikan bahwa SMADAV selalu diupdate dan dijalankan secara teratur untuk tetap efektif dalam melindungi sistem. Penggunaannya sebagai lapisan proteksi tambahan, fitur pemulihan yang handal, dan portabilitas menjadikan SMADAV pilihan yang baik bagi banyak pengguna (Tri et al., 2024). Enkripsi adalah aktivitas mengubah bentuk data yang awalnya



mudah dipahami menjadi kode yang sulit dipahami. Hal tersebut karena fungsi utama enkripsi adalah mengamankan data. Enkripsi dipakai untuk menanggulangi seiring adanya cyber crime atau (kejahatan dunia maya). Seperti peretasan email, phishing, pencurian data, carding dan sejenisnya (Wulandari et al., 2023). Program pelatihan keamanan siber dengan pendekatan sistematis juga telah terbukti meningkatkan kemampuan dasar peserta dalam mengenali dan menerapkan praktik keamanan digital, terutama melalui peningkatan wawasan perlindungan data dan mitigasi risiko (Andria et al., 2025).

Pemanfaatan kemajuan teknologi informasi dan komunikasi di berbagai aspek kehidupan mencerminkan pergeseran peradaban manusia menuju masyarakat yang lebih canggih dalam hal informasi (Ayu et al., 2024). Pentingnya keamanan digital di kalangan mahasiswa atau di mana pun menjadi perhatian penting bagi semua pihak. Berdasarkan kondisi tersebut, program sosialisasi keamanan siber ini diselenggarakan untuk meningkatkan kesadaran dan pengetahuan mahasiswa Program Studi Sistem Informasi kelas E UIN Sultan Thaha Saifuddin Jambi berbagai risiko serangan siber, seperti malware (virus dan ransomware), peretasan (hacking), akses tidak sah, penyadapan data. Program studi ini dipilih karena tingginya intensitas penggunaan teknologi digital oleh mahasiswa, sementara pemahaman mereka terhadap risiko keamanan siber masih perlu ditingkatkan.

Rumusan masalah yang ingin diatasi melalui kegiatan ini adalah bagaimana meningkatkan kesadaran mahasiswa terhadap risiko kejahatan siber serta langkah-langkah yang dapat dilakukan untuk melindungi diri dari ancaman tersebut. Tujuan dari kegiatan sosialisasi ini adalah memberikan pemahaman kepada mahasiswa mengenai cara mengenali dan menghindari ancaman dunia maya, serta mendorong penggunaan teknologi secara aman dan bertanggung jawab. Dengan meningkatnya pengetahuan dan kesadaran mahasiswa tentang keamanan siber, diharapkan mereka dapat berperan sebagai agen perubahan yang menyebarkan edukasi mengenai pentingnya keamanan digital di lingkungan sekitar.

2. METODE PENELITIAN

Metode pelaksanaan dalam kegiatan ini pada mahasiswa Program Studi Sistem Informasi kelas E di UIN Sultan Thaha Saifuddin Jambi yang berjumlah 42 orang, dengan tujuan untuk meningkatkan kesadaran dan pemahaman mengenai berbagai ancaman yang terkait dengan kejahatan siber. Kegiatan ini diikuti oleh mahasiswa yang aktif menggunakan teknologi digital dalam kegiatan baik akademik maupun non-akademik. Metode yang diterapkan mencakup penyampaian materi secara langsung, diskusi interaktif, serta sesi tanya jawab. Tahapan dalam pelaksanaan kegiatan sosialisasi ini yaitu sebagai berikut:

**a) Tahap Persiapan**

Tahap persiapan yaitu tahapan awal dalam pelaksanaan penelitian guna memastikan seluruh kebutuhan penelitian telah direncanakan dan disiapkan secara matang sebelum kegiatan inti dilaksanakan. Pada tahapan ini, peneliti memfokuskan kegiatan pada perencanaan aspek pemahaman dan implementasi agar proses sosialisasi dapat berjalan secara terstruktur, terarah, dan sesuai dengan tujuan penelitian. Persiapan yang baik diharapkan dapat meminimalkan kendala selama pelaksanaan serta mendukung pencapaian hasil penelitian yang optimal. Berikut tahapannya:

1. Studi Literatur, dilakukan untuk memperoleh landasan teoretis terkait tingkat pengetahuan keamanan siber dan mekanisme pengamanan sistem informasi.
2. Penyusunan dan Penyesuaian Materi, agar materi sesuai dengan tingkat pemahaman mahasiswa.
3. Penentuan Target Peserta, yaitu mahasiswa kelas 3E Program Studi Sistem Informasi.
4. Persiapan Perangkat Pendukung, meliputi media presentasi dan sarana pendukung pelaksanaan kegiatan.

b) Tahap Penyuluhan

Tahapan dalam penyuluhan adalah serangkaian langkah yang dilakukan dengan cara teratur dalam kegiatan untuk menyebarkan informasi atau pengetahuan demi meningkatkan pemahaman, sikap, dan tindakan dari target yang dituju. Berikut tahapannya:

1. Pelaksanaan Sosialisasi

Kegiatan penyuluhan dilaksanakan dengan cara memberikan materi interaktif tentang keamanan di dunia maya, peran firewall, antivirus, dan enkripsi, dengan ditambahkan contoh ancaman serta cara-cara untuk melindungi diri.

2. Praktik dan Demonstrasi

Para peserta mendapatkan contoh langsung yang sederhana tentang cara penerapan firewall, pemakaian antivirus, dan contoh enkripsi data untuk memperdalam pemahaman yang praktis.

3. Evaluasi

Proses evaluasi dilakukan lewat diskusi dan tanya jawab untuk menilai seberapa besar peningkatan pengetahuan tentang keamanan siber mahasiswa setelah mengikuti kegiatan sosialisasi.

3. HASIL DAN PEMBAHASAN

Berdasarkan hasil pelaksanaan kegiatan sosialisasi, mahasiswa menunjukkan tingkat partisipasi dan ketertarikan yang tinggi, khususnya pada sesi penyampaian materi mengenai pemahaman dasar firewall, antivirus, dan enkripsi sebagai bentuk perlindungan terhadap sistem dan data digital. Sebagian besar mahasiswa menyampaikan bahwa sebelum kegiatan dilaksanakan, mereka belum memiliki pemahaman yang mendalam terkait peran firewall dalam mengendalikan akses jaringan, fungsi antivirus dalam mendeteksi serta mencegah serangan malware, maupun pentingnya enkripsi dalam menjaga kerahasiaan informasi. Materi disampaikan secara komunikatif dan interaktif dengan dukungan contoh kasus serta ilustrasi penerapan keamanan siber dalam aktivitas digital sehari-hari, sebagaimana ditampilkan pada Gambar 1. Pendekatan tersebut dinilai efektif dalam membantu mahasiswa memahami materi keamanan siber yang bersifat teknis secara lebih mudah dan aplikatif.



Gambar 1 Proses penyampaian materi kepada mahasiswa

Secara umum, hasil kegiatan menunjukkan bahwa sosialisasi keamanan siber berperan efektif sebagai media edukasi dalam meningkatkan literasi keamanan digital mahasiswa Program Studi Sistem Informasi. Kegiatan ini tidak hanya memperluas wawasan mahasiswa terkait berbagai ancaman siber dan cara pengamanannya, tetapi juga menumbuhkan kesadaran akan pentingnya menjaga keamanan sistem serta melindungi data pribadi. Melalui sosialisasi ini, mahasiswa menjadi lebih memahami risiko penggunaan teknologi digital tanpa perlindungan

yang memadai dan menyadari perlunya penerapan praktik keamanan dasar dalam lingkungan akademik.

Pada sesi diskusi dan tanya jawab, terlihat adanya peningkatan pemahaman mahasiswa terhadap materi yang telah disampaikan. Peningkatan tersebut tercermin dari kemampuan mahasiswa dalam menguraikan kembali fungsi firewall, antivirus, dan enkripsi, serta mengidentifikasi langkah-langkah pencegahan ancaman siber, seperti melakukan pembaruan perangkat lunak secara berkala, menerapkan penggunaan kata sandi yang kuat dan berbeda pada setiap akun, serta meningkatkan kewaspadaan terhadap aktivitas digital yang mencurigakan. Hasil diskusi juga menunjukkan bahwa sebagian besar mahasiswa baru menyadari bahwa ancaman siber tidak hanya bersumber dari malware, tetapi juga dari lemahnya pengelolaan keamanan sistem dan perilaku pengguna. Tingginya antusiasme dan partisipasi aktif mahasiswa selama diskusi ditunjukkan pada Gambar 2.



Gambar 2 Foto bersama setelah kegiatan sosialisasi

Selain itu, kegiatan sosialisasi ini memberikan kontribusi positif terhadap perubahan sikap dan peningkatan kesadaran digital mahasiswa. Mahasiswa menunjukkan pemahaman yang lebih baik mengenai pentingnya menjaga kerahasiaan data pribadi serta menerapkan perilaku digital yang aman dalam penggunaan perangkat dan layanan teknologi informasi. Pendekatan edukatif dan komunikatif yang digunakan dalam sosialisasi dinilai efektif dalam meningkatkan kesiapan mahasiswa untuk menghadapi berbagai tantangan keamanan siber di era digital.

4. KESIMPULAN

Berdasarkan hasil pelaksanaan kegiatan sosialisasi firewall, antivirus, dan enkripsi pada mahasiswa Program Studi Sistem Informasi, dapat disimpulkan bahwa kegiatan ini berhasil



meningkatkan literasi keamanan siber mahasiswa secara signifikan. Sosialisasi yang dilakukan melalui penyampaian materi secara interaktif dan aplikatif mampu meningkatkan pemahaman siswa mengenai peran firewall dalam membatasi akses jaringan, fungsi antivirus dalam mendeteksi dan mencegah malware, serta pentingnya enkripsi dalam menjaga kerahasiaan data digital. Sebelum kegiatan berlangsung, sebagian besar siswa belum memahami secara komprehensif mekanisme dasar keamanan siber, namun setelah mengikuti sosialisasi, siswa menunjukkan peningkatan pengetahuan, kesadaran, dan sikap yang lebih bertanggung jawab dalam penggunaan teknologi digital. Selain meningkatkan pemahaman konsep, kegiatan ini juga mendorong perubahan perilaku siswa dalam menerapkan praktik keamanan dasar, seperti pengelolaan kata sandi yang kuat, pemeliharaan sistem secara berkala, dan kewaspadaan terhadap ancaman siber. Dengan demikian, sosialisasi keamanan siber terbukti efektif sebagai upaya edukatif dalam meningkatkan literasi keamanan siber mahasiswa Sistem Informasi serta membekali mereka dalam menghadapi tantangan keamanan digital di era teknologi informasi yang terus berkembang.

DAFTAR PUSTAKA

- [1] Andria, Sussolaikah, K., Laksono, R. D., & Lenawati, M. (2025). *Jurnal Komputer Multidisipliner*. 8(4), 2021-2024.
- [2] Ayu, N., Pertiwi, S., Umardiyah, F., Mansyur, M. N., Sapi, I., Sholichah, A., & Fudlah, T. N. (2024). *Sosialisasi Kesadaran Keamanan Digital di Era Revolusi Industri 4 . 0*. 5(1).
- [3] Miracle, N. O. (2024). *The Importance of Network Security in Protecting Sensitive Data and Information*. IX(2454), 259-270. <https://doi.org/10.51584/IJRIAS>
- [4] Nopiansa, D., Baharja, F. P., & Wahyuni, T. (2025). *Perbandingan Efektivitas Firewall, Antivirus, dan Enkripsi dalam Mitigasi Ancaman Siber pada Lingkungan Jaringan Modern*. 10(6), 1-18.
- [5] Oktapiyadi, W., Saepudin, E., & Yanto, A. (2024). *HUBUNGAN LITERASI DIGITAL DENGAN PERILAKU*. 5, 164-180. <https://doi.org/10.24036/ib.v5i2.464>
- [6] Pardosi, V. B. A., Deta, B., Nugroho, F., & Vandika, A. Y. (2024). *Sistem Keamanan Informasi*.
- [7] Prawiro, R., Jamhur, A. I., Ariandi, V., & Afira, R. (2025). *Literasi Keamanan Digital Edukasi Perlindungan Data Pribadi bagi Remaja di Era Media Sosial pada organisasi Pemuda dan Karang Taruna Nagari Sungai Pinang*. 1, 7-15.
- [8] Saputra, A. D., Dione, F., & Uluputty, I. (2023). *Pengelolaan Keamanan Informasi dan Persandian di Dinas Komunikasi dan*. 5(2), 159-187.



- [9] Susilowati, W. (2024). *Studi Literatur : Strategi Pengamanan Siber dalam Menghadapi Cyber Crime*. 2(4).
- [10] Sussolaikah, K., Laksono, R. D., & Lenawati, M. (2024). *Jurnal Abdimas Teknologi Informatika & Komputer (JATIK) Pelatihan Keamanan Siber Guna Meningkatkan Literasi Digital di SMPN 14 Kota Madiun Jurnal Abdimas Teknologi Informatika & Komputer (JATIK)*. 1, 53-60.
- [11] Tri, A., Sanjaya, B., Mei, A., Ageng, G., & Fatmawati, S. R. (2024). *Analisis Keamanan SMADAV Antivirus Dalam Sistem Operasi Windows*. 371-378.
- [12] Wulandari, I. W., Ekonomi, F., Bisnis, D., Ekonomi, F., & Bisnis, D. (2023). *Peran sistem informasi akuntansi dalam pengaplikasian enkripsi terhadap peningkatan keamanan perusahaan*. 1(1).