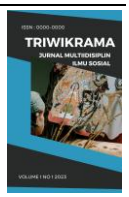
Triwikrama: Jurnal Ilmu Sosial
Volume 11 No 8 2025
E-ISSN: 2988-1986
Open Access:



# SOSIALISASI PERISAI SISTEM INFORMASI: FIREWALL, ANTIVIRUS DAN ENKRIPSI DALAM MENINGKATKAN KEAMANAN DIGITAL PADA MAHASISWA PRODI KIMIA UNIVERSITAS ISLAM NEGERI SULTHAN THAHA SYAIFUDDIN JAMBI

**Kalvin Prasetyo, Retno Wahyuningsih, Linda Ardianti**
Sistem informasi, Sains dan Teknologi, Universitas Islam Negeri Sulthan Thaha Syaifuddin Jambi

**ARTICLE INFO**

**Article history:**
Received November 2025
Revised November 2025
Accepted November 2025
Available online November 2025

**Email:**
vinprasetyo04@gmail.com,
ningsihretnowahyu754@gmail.com,
lindaardianti939@gmail.com



**Abstrak**

Perkembangan teknologi informasi menuntut peningkatan pemahaman mahasiswa terhadap mekanisme perlindungan data dan ancaman siber yang dapat muncul dalam aktivitas akademik. Kegiatan sosialisasi ini bertujuan memperkenalkan tiga komponen utama perisai sistem informasi—firewall, antivirus, dan enkripsi—kepada mahasiswa Program Studi Kimia UIN STS Jambi sebagai upaya memperkuat keamanan digital mereka. Metode yang digunakan yaitu sosialisasi lapangan dengan pendekatan deskriptif kualitatif, melibatkan 32 mahasiswa sebagai peserta. Materi disusun berdasarkan prinsip keamanan informasi yang berlaku secara nasional, mencakup pengelolaan akses jaringan, pencegahan malware, serta perlindungan data pribadi melalui enkripsi. Hasil sosialisasi menunjukkan peningkatan signifikan dalam pemahaman mahasiswa lebih dari 80% peserta mampu menjelaskan fungsi firewall, pentingnya pembaruan antivirus, serta peran enkripsi dalam menjaga kerahasiaan data akademik. Selain itu, mahasiswa memperlihatkan perubahan perilaku digital yang lebih aman, termasuk kebiasaan menggunakan kata sandi kuat, menghindari tautan berisiko, serta lebih selektif dalam membagikan informasi pribadi. Sosialisasi ini terbukti berperan dalam meningkatkan literasi keamanan digital serta membangun budaya penggunaan teknologi yang aman dan bertanggung jawab.
Kata kunci : Firewall, Antivirus, Enkripsi, Keamanan Digital, Mahasiswa

***Abstract***

*The development of information technology requires students to strengthen their understanding of data protection mechanisms and the various cyber threats that may arise in academic activities. This socialization program aims to introduce three key components of information system protection—firewall, antivirus, and encryption—to Chemistry students at UIN STS Jambi as part of efforts to enhance their digital security. The activity employed a descriptive qualitative approach through field-based socialization, involving 60 students as participants and several lecturers as facilitators. The materials were structured based on nationally recognized information security principles, including network access management, malware prevention, and personal data protection through encryption. The results indicate a significant improvement in students' understanding; more than 80% of participants were able to clearly explain the functions of firewalls, the importance of antivirus updates, and the role of encryption in securing academic data. Furthermore, students demonstrated safer digital behavior, such as using stronger passwords, avoiding risky links, and being more selective when sharing personal information. Overall, this socialization effectively strengthens digital security literacy and fosters a responsible and secure approach to technology use among university students.*
***Keywords:*** *Firewall, Antivirus, Encryption, Digital Security, University Students*

## Pendahuluan

Perkembangan teknologi informasi telah membawa perubahan signifikan dalam kegiatan akademik di perguruan tinggi, termasuk pada Program Studi Kimia UIN STS Jambi. Aktivitas seperti pengumpulan tugas secara digital, penggunaan platform pembelajaran daring, penyimpanan data penelitian, serta komunikasi akademik berbasis internet kini menjadi bagian integral dari proses pembelajaran sehari-hari. Integrasi teknologi ini memberikan kemudahan, terutama dalam efisiensi waktu, akses fleksibel, dan kemampuan berbagi data antar mahasiswa maupun dosen. Namun demikian, peningkatan penggunaan teknologi tersebut tidak selalu diiringi dengan pemahaman yang memadai mengenai prinsip keamanan informasi. Banyak

mahasiswa masih mengandalkan perangkat pribadi tanpa memahami potensi ancaman digital yang dapat merusak data, memanipulasi informasi, atau bahkan mengakses identitas digital mereka secara ilegal.

Minimnya kesadaran mahasiswa terhadap risiko siber membuat aktivitas digital mereka rentan terhadap ancaman seperti malware, phishing, pencurian data, peretasan akun, serta kerusakan sistem karena penggunaan software yang tidak kredibel. Kondisi ini semakin diperparah dengan kebiasaan penggunaan kata sandi sederhana, akses jaringan Wi-Fi publik tanpa perlindungan, serta kebiasaan mengunduh file sembarangan. Fenomena tersebut menunjukkan bahwa peningkatan kecakapan digital mahasiswa tidak otomatis sejalan dengan kesiapan mereka dalam melindungi data pribadi dan akademik. Banyak mahasiswa menggunakan perangkat tanpa perlindungan dasar seperti firewall aktif, antivirus yang diperbarui, atau enkripsi pada data sensitif. Akibatnya, berbagai risiko seperti kebocoran data penelitian, pengambilalihan akun e-learning, hingga kerusakan file laporan laboratorium akibat infeksi virus dapat terjadi tanpa disadari.

Kelemahan pemahaman mengenai keamanan sistem informasi ini juga tercermin dalam berbagai survei literasi digital nasional, di mana sebagian besar pengguna internet berusia produktif belum memahami mekanisme perlindungan data pribadi dan teknik dasar keamanan perangkat (Kominfo, 2023). Temuan ini konsisten dengan laporan kegiatan edukasi digital sebelumnya yang menunjukkan bahwa rendahnya literasi keamanan informasi sering kali berimplikasi pada meningkatnya risiko penyalahgunaan data, pelanggaran etika digital, serta ancaman siber di lingkungan pendidikan. Situasi ini semakin mendesak diatasi mengingat mahasiswa merupakan kelompok pengguna internet yang aktif, sering berpindah jaringan, dan banyak berinteraksi melalui platform digital yang menyimpan beragam informasi penting.

Dalam konteks ini, edukasi mengenai perisai sistem informasi meliputi firewall, antivirus, dan enkripsi menjadi langkah strategis untuk memperkuat perlindungan digital mahasiswa. Firewall berfungsi sebagai penjaga gerbang jaringan yang dapat menyaring dan memblokir akses tidak sah sehingga mencegah pihak luar masuk ke sistem. Antivirus berperan mengidentifikasi, mendeteksi, dan menghapus berbagai bentuk malware yang dapat merusak atau mencuri data. Sementara itu, enkripsi memberikan lapisan keamanan tambahan dengan mengonversi data menjadi bentuk yang tidak dapat dibaca tanpa kunci tertentu sehingga informasi tetap terlindungi meskipun perangkat hilang atau dicuri. Ketiga komponen ini sangat relevan bagi mahasiswa Kimia yang banyak bekerja dengan data hasil eksperimen, laporan praktikum, gambar instrumen laboratorium, dan file akademik lain yang membutuhkan keamanan tinggi.

Sosialisasi mengenai perisai sistem informasi diharapkan dapat meningkatkan pemahaman mahasiswa terhadap protokol keamanan digital serta membentuk perilaku penggunaan teknologi yang lebih aman dan bertanggung jawab. Melalui kegiatan sosialisasi, mahasiswa tidak hanya diperkenalkan pada konsep dasar keamanan digital, tetapi juga dilatih untuk mengenali ancaman, memahami cara kerja sistem keamanan, serta mempraktikkan langkah pencegahan yang dapat diterapkan pada perangkat mereka sendiri. Upaya ini sejalan dengan kebutuhan nasional untuk memperkuat literasi digital generasi muda serta mendukung penerapan langkah perlindungan informasi sebagaimana direkomendasikan dalam regulasi keamanan data dan praktik keamanan sistem elektronik di Indonesia. Dengan demikian, sosialisasi ini menjadi langkah penting dalam membangun budaya keamanan digital di lingkungan akademik, sekaligus membantu mahasiswa lebih siap menghadapi berbagai risiko siber dalam proses pembelajaran modern.

Triwikrama: Jurnal Ilmu Sosial
Volume 11 No 8 2025
E-ISSN: 2988-1986
Open Access:

## Metode Penelitian

Penelitian ini mengadopsi pendekatan deskriptif kualitatif dengan metode sosialisasi lapangan, berfungsi sebagai aktivitas pendidikan.Pendekatan deskriptif kualitatif dipilih karena bertujuan untuk menggambarkan secara faktual dan sistematis fenomena yang terjadi di lapangan, yaitu tingkat pemahaman mahasiswa terhadap konsep perisai sistem informasi (Sugiyono, 2022).

Kegiatan ini dilaksanakan di Universitas Islam Negeri Sulthan Thaha Syaifuddin Jambi, pada bulan Oktober 2025 dengan melibatkan 32 mahasiswa dari prodi kimia. Pemilihan lokasi dilakukan secara purposive sampling, karena mahasiswa prodi Kimia UIN STS Jambi aktif menggunakan perangkat digital untuk kegiatan praktikum, pengolahan data, dan pembelajaran daring, kampus ini membutuhkan penguatan pemahaman mengenai firewall, antivirus, dan enkripsi agar mahasiswa mampu melindungi data akademik serta aktivitas digital mereka dari berbagai ancaman keamanan sistem informasi.

### 1. Tahap Persiapan

Pada tahap awal, peneliti menyusun rancangan kegiatan sosialisasi dan materi yang akan diberikan kepada mahasiswa. Penyusunan materi difokuskan pada tiga elemen utama perisai sistem informasi, yaitu firewall, antivirus, dan enkripsi, yang berperan penting dalam menjaga keamanan data dan aktivitas digital. Dasar penyusunan materi merujuk pada regulasi nasional yang mengatur penyelenggaraan sistem elektronik dan perlindungan data pribadi, di antaranya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahan dalam Undang-Undang Nomor 19 Tahun 2016, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, serta Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

2. Tahap Pelaksanaan

a. Pada tahap studi kasus dan simulasi, mahasiswa diajak menganalisis contoh situasi nyata yang sering terjadi dalam aktivitas digital di lingkungan akademik, khususnya terkait ancaman terhadap keamanan sistem informasi. Mahasiswa mempelajari berbagai bentuk risiko seperti upaya masuknya malware melalui unduhan tidak aman, percobaan akses jaringan tanpa izin, serta potensi kebocoran data akibat penggunaan perangkat tanpa perlindungan enkripsi.
b. Pada sesi demonstrasi, mahasiswa diperkenalkan pada praktik sederhana mengenai cara menerapkan perlindungan dasar terhadap ancaman digital menggunakan firewall, antivirus, dan enkripsi. Demonstrasi ini mencakup cara memantau aktivitas jaringan melalui firewall untuk mendeteksi upaya akses mencurigakan, memeriksa file dan perangkat menggunakan antivirus untuk mengidentifikasi potensi malware, serta menerapkan enkripsi pada dokumen akademik agar data tetap terlindungi meskipun file berpindah antarperangkat.

Dalam proses ini, mahasiswa didorong untuk aktif bertanya dan berdiskusi. Metode learning by doing dipilih agar mahasiswa tidak hanya memahami secara teoritis tetapi juga secara praktis mengenai pentingnya perisai sistem informasi (Yasin, 2025).

3. Tahap Evaluasi

Data yang terkumpul dianalisis menggunakan pendekatan deskriptif naratif. Hasil observasi, tes, dan wawancara diolah menjadi tema-tema yang menunjukkan perkembangan pengetahuan mahasiswa, seperti perubahan pemahaman mengenai ancaman siber, peningkatan kemampuan mengenali serangan malware, serta bertambahnya kesadaran pentingnya penggunaan firewall

dan enkripsi dalam sistem akademik. Prosedur analisis mengikuti model Miles & Huberman (2014) yang meliputi reduksi data, penyajian data, dan penarikan kesimpulan untuk memastikan bahwa setiap temuan tersusun secara sistematis.

4. Validitas dan Etika Penelitian

Dalam penelitian mengenai *sosialisasi perisai sistem informasi: firewall, antivirus, dan enkripsi dalam meningkatkan keamanan digital pada mahasiswa kimia Universitas Islam Negeri Sulthan Thaha Syaifuddin Jambi,* validitas penelitian merujuk pada sejauh mana instrumen kuesioner yang diberikan benar-benar mengukur pemahaman mahasiswa terhadap materi yang telah disampaikan. Validitas ini dijaga dengan memastikan bahwa setiap pertanyaan dalam kuesioner sesuai dengan isi materi sosialisasi, seperti fungsi firewall, pentingnya pembaruan antivirus, serta peran enkripsi dalam melindungi data akademik. Pertanyaan yang digunakan tidak keluar dari topik dan langsung berkaitan dengan konsep yang telah dijelaskan selama sosialisasi, sehingga hasil kuesioner dapat mencerminkan pemahaman mahasiswa secara akurat. Selain itu, pemberian kuesioner setelah penyampaian materi turut memperkuat hubungan antara proses sosialisasi dan hasil evaluasi, sehingga data yang diperoleh dapat dianggap sah untuk menilai efektivitas kegiatan.

Etika penelitian dalam kegiatan ini diterapkan dengan memastikan bahwa seluruh proses pengumpulan data menghormati hak dan keamanan peserta. Mahasiswa mengikuti sosialisasi dan mengisi kuesioner secara sukarela setelah mendapatkan penjelasan mengenai tujuan penelitian dan penggunaan data. Jawaban kuesioner dikumpulkan tanpa meminta identitas pribadi yang sensitif, sehingga kerahasiaan dan privasi peserta tetap terjaga. Link kuesioner yang digunakan berasal dari platform resmi dan aman agar tidak menimbulkan risiko digital bagi peserta. Peneliti juga menjamin bahwa hasil kuesioner digunakan hanya untuk keperluan penelitian dan penyusunan laporan kegiatan, tanpa manipulasi data maupun penyebaran informasi pribadi. Dengan menerapkan prinsip-prinsip ini, penelitian berlangsung secara etis dan tetap menjaga integritas akademik

**Hasil dan Pembahasan**

Hasil kegiatan sosialisasi menunjukkan adanya peningkatan pemahaman yang nyata pada mahasiswa mengenai konsep dasar perlindungan sistem informasi melalui firewall, antivirus, dan enkripsi. Sebelum sosialisasi dimulai, sebagian mahasiswa hanya mengenal antivirus secara umum sebagai alat untuk menghapus virus, sementara fungsi firewall serta peran enkripsi dalam menjaga kerahasiaan data belum dipahami secara mendalam. Mahasiswa juga cenderung belum menyadari bahwa ketiga komponen tersebut merupakan bagian penting dari upaya perlindungan data yang mereka gunakan sehari-hari, termasuk file akademik, hasil penelitian, dan akses ke platform pembelajaran digital. Setelah penyampaian materi disertai demonstrasi dan contoh penerapan langsung, memahami pentingnya pembaruan antivirus secara rutin, serta menyadari bahwa enkripsi berfungsi mengamankan data dari akses pihak yang tidak berwenang. Perubahan ini menunjukkan bahwa metode sosialisasi berbasis praktik dan simulasi efektif dalam membangun kesadaran keamanan digital. Peningkatan pemahaman tersebut sejalan dengan pola hasil sosialisasi pada penelitian sebelumnya yang menekankan bahwa pendekatan edukatif interaktif mampu meningkatkan literasi keamanan informasi peserta secara substansial .

Firewall, antivirus, dan enkripsi memegang peran penting sebagai lapisan pertahanan utama dalam menjaga keamanan digital mahasiswa, terutama dalam aktivitas akademik yang sangat bergantung pada perangkat dan data elektronik. Firewall berperan sebagai penjaga gerbang yang mengatur lalu lintas jaringan dan memblokir akses yang mencurigakan. Dalam kegiatan sosialisasi, mahasiswa melihat bahwa firewall membantu mencegah masuknya program

berbahaya saat mereka mengakses berbagai sumber online, yang mekanismenya sejalan dengan prinsip perlindungan data yang juga ditekankan dalam sosialisasi keamanan digital pada dokumen acuan . Pemahaman ini membuat mahasiswa lebih sadar bahwa setiap koneksi jaringan memiliki risiko yang harus diantisipasi.

Sementara itu, antivirus berperan sebagai sistem pertahanan yang mendeteksi dan menghapus ancaman seperti malware, trojan, worm, atau program berbahaya lainnya yang dapat merusak data akademik mahasiswa. Sebelum sosialisasi, mahasiswa cenderung mengabaikan pembaruan antivirus karena menganggap perangkat mereka aman. Namun setelah mendapatkan penjelasan dan demonstrasi, mereka mulai memahami bahwa ancaman digital dapat merusak file laporan, mengubah data penelitian, bahkan mencuri kredensial akun kampus. Pemahaman ini menunjukkan pola perubahan perilaku yang mirip dengan peningkatan kesadaran keamanan pada pelajar dalam temuan acuan .

Adapun enkripsi memiliki peran sebagai mekanisme perlindungan data dengan cara mengubah informasi menjadi format yang tidak dapat dibaca tanpa kunci tertentu. Dalam konteks mahasiswa kimia yang sering menyimpan data percobaan, laporan praktikum, atau dokumen sensitif lainnya, enkripsi menjadi unsur vital untuk menjaga kerahasiaan dan integritas data. Setelah sosialisasi, mahasiswa mulai memahami bahwa enkripsi mampu memberikan perlindungan tambahan ketika mereka menyimpan file di flashdisk, laptop, atau layanan penyimpanan cloud. Prinsip perlindungan data yang dijelaskan dalam riset acuan semakin menekankan pentingnya mekanisme seperti enkripsi untuk mencegah penyalahgunaan informasi.

Secara keseluruhan, ketiga komponen ini berperan sebagai perisai sistem informasi yang saling melengkapi. Firewall mencegah ancaman masuk, antivirus menangani ancaman yang lolos, dan enkripsi menjaga keamanan data dari penyadapan atau akses ilegal. Sosialisasi mengenai ketiganya terbukti memberikan dampak positif terhadap pemahaman mahasiswa, sejalan dengan efektivitas sosialisasi yang juga tercatat dalam dokumen acuan . Kombinasi pemahaman ini mendorong terbentuknya perilaku digital yang lebih aman dan bertanggung jawab di lingkungan akademik.

**Kesimpulan**

Sosialisasi yang diberikan kepada mahasiswa Kimia UIN STS Jambi mampu meningkatkan pemahaman mereka mengenai peran firewall, antivirus, dan enkripsi sebagai elemen yang sangat penting dalam perlindungan sistem informasi. Pada tahap awal, sebagian mahasiswa hanya memahami konsep keamanan digital secara umum dan belum menyadari bahwa perangkat yang mereka gunakan setiap hari memiliki kerentanan serius terhadap ancaman siber seperti malware, phishing, dan akses ilegal. Melalui sosialisasi yang disusun secara terstruktur, mahasiswa diperkenalkan pada fungsi firewall sebagai pengendali lalu lintas jaringan, disertai contoh kasus bagaimana firewall dapat mencegah upaya penyusupan dari jaringan luar. Penjelasan mengenai antivirus juga disertai dengan ilustrasi cara kerja deteksi ancaman, pembaruan sistem keamanan, serta risiko yang dapat muncul ketika perangkat tidak dilindungi. Selain itu, materi mengenai enkripsi disampaikan untuk menunjukkan pentingnya perlindungan data akademik seperti laporan praktikum, hasil eksperimen, serta dokumen pribadi, agar tidak mudah diakses, disalin, atau dimodifikasi pihak yang tidak berwenang.

Pendekatan edukatif yang digunakan dalam kegiatan ini termasuk demonstrasi teknis, simulasi ancaman, dan diskusi interaktif menjadikan mahasiswa tidak hanya memahami konsep secara teoritis, tetapi juga melihat secara langsung bagaimana ancaman siber dapat terjadi pada aktivitas digital sehari-hari mereka. Pengalaman ini memperkuat kesadaran bahwa keamanan digital tidak hanya bergantung pada teknologi yang digunakan, tetapi juga sangat dipengaruhi oleh kebiasaan dan kehati-hatian pengguna. Mahasiswa kemudian menyadari bahwa

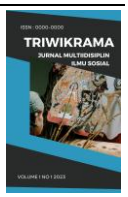
menjaga perangkat, memperbarui aplikasi keamanan, berhati-hati dalam mengunduh file, serta menerapkan enkripsi pada dokumen penting merupakan bagian dari tanggung jawab mereka sebagai pengguna teknologi.

Kesimpulannya, sosialisasi ini terbukti efektif dalam meningkatkan pengetahuan sekaligus membentuk sikap mahasiswa terhadap keamanan sistem informasi. Mahasiswa tidak hanya memahami fungsi firewall, antivirus, dan enkripsi, tetapi juga mampu menghubungkannya dengan kebutuhan akademik mereka, terutama dalam mengelola data laboratorium dan tugas perkuliahan secara aman. Kegiatan ini juga mendorong terbentuknya perilaku digital yang lebih bertanggung jawab, seperti menghindari situs tidak aman, menggunakan kata sandi yang kuat, serta menjaga privasi akses akun akademik. Dengan demikian, sosialisasi ini tidak hanya memberikan wawasan teknis, tetapi juga memperkuat budaya keamanan digital di lingkungan kampus, sehingga mahasiswa lebih siap menghadapi berbagai risiko siber yang dapat memengaruhi kelancaran proses belajar mereka.

**Dokumentasi**

**Referensi**

1. Kementerian Komunikasi dan Informatika Republik Indonesia. (2023). *Pedoman Literasi Digital Nasional dan Perlindungan Data Pribadi di Era Siber*. Jakarta: Ditjen Aptika.
2. International Organization for Standardization (ISO). (2022). *ISO/IEC 27001:2022 - Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements*. Geneva: ISO.
3. Miles, M. B., & Huberman, A. M. (2014). *Qualitative Data Analysis: A Methods Sourcebook* (3rd ed.). Thousand Oaks, CA: Sage Publications.
4. Republik Indonesia. (2012). *Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE)*. Jakarta: Sekretariat Negara.




5. Republik Indonesia. (2016). *Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Jakarta: Sekretariat Negara.
6. Republik Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP)*. Jakarta: Sekretariat Negara.
7. Titan, T. P. Y. (2023). Audit keamanan sistem informasi menggunakan COBIT 5 di lembaga pendidikan. *Jurnal Teknologi dan Sistem Informasi Pendidikan*, 5(1), 33–42.
8. Yasin, M. (2025). Sosialisasi keamanan digital dan pencegahan kejahatan daring di sekolah menengah. *Jurnal Pengabdian Masyarakat Digital Indonesia*, 4(2), 66–75.