SOSIALISASI PENGENALAN MALWARE DAN PENCEGAHANNYA BAGI MAHASISWA BARU PROGRAM STUDI SISTEM INFORMASI UIN SULTHAN THAHA SAIFUDDIN JAMBI

Wajid Nur Karim[1], Julia[2], Andrian Jandra Kurniawan[3]

[1]*Program Studi Sistem Informasi, Fakultas Sains dan Teknologi, Universitas Islam Negeri Sulthan Thaha Saifuddin Jambi, Indonesia*
e-mail: [1]wajidnurrkarim@gmail.com

[2,3]*Program Studi Sistem Informasi, Fakultas Sains dan Teknologi, Universitas Islam Negeri Sulthan Thaha Saifuddin Jambi, Indonesia*
e-mail: [2]juliaa28304@gmail.com, [3]Andrianjandra1307@gmail.com

Abstract

The rapid development of digital technology has provided numerous benefits as well as increasing information security risks, particularly among university students as active digital users. This community service activity aimed to provide fundamental understanding about *malware* threats and their prevention to new students of the Information Systems Study Program at UIN Sulthan Thaha Saifuddin Jambi. The activity was conducted through an educational-participatory socialization method using presentation media, followed by discussion and question–answer sessions. The event took place on September 18, 2025, involving 25 new students. Based on observations, participants demonstrated high enthusiasm and were able to comprehend the delivered material. This activity contributed to raising initial awareness among students about digital security and the importance of safe behavior in using information technology within academic settings.

Keywords*: cybersecurity, malware, socialization, digital literacy, university students*

Abstrak

Perkembangan teknologi digital yang pesat telah membawa berbagai manfaat sekaligus risiko terhadap keamanan informasi, terutama bagi mahasiswa sebagai pengguna aktif perangkat digital. Kegiatan sosialisasi ini bertujuan memberikan pemahaman dasar mengenai ancaman *malware* dan langkah-langkah pencegahannya kepada mahasiswa baru Program Studi Sistem Informasi Universitas Islam Negeri Sulthan Thaha Saifuddin Jambi. Kegiatan dilaksanakan dengan metode sosialisasi edukatif partisipatif melalui penyampaian materi menggunakan media presentasi, disertai sesi diskusi dan tanya jawab. Kegiatan berlangsung pada 18 September 2025 dengan melibatkan 25 mahasiswa baru. Berdasarkan hasil observasi, peserta menunjukkan antusiasme tinggi dan mampu memahami materi yang disampaikan. Sosialisasi ini berkontribusi terhadap peningkatan kesadaran awal mahasiswa terhadap keamanan digital dan pentingnya perilaku aman dalam penggunaan teknologi informasi di lingkungan akademik.

Kata kunci: keamanan siber, malware, sosialisasi, literasi digital, mahasiswa

1. PENDAHULUAN

Perkembangan teknologi informasi yang sangat pesat telah mengubah cara masyarakat berinteraksi dan beraktivitas, termasuk di lingkungan pendidikan tinggi. Mahasiswa sebagai generasi digital (*digital native*) menggunakan berbagai perangkat dan aplikasi daring dalam aktivitas akademik sehari-hari. Namun, tingginya ketergantungan terhadap teknologi juga diikuti meningkatnya potensi ancaman keamanan digital, terutama dari perangkat lunak berbahaya atau *malware* (Chang & Coppel, 2020).

Di Indonesia, ancaman siber terus meningkat dari tahun ke tahun. Berdasarkan analisis (Pratiwi et al., 2024), sektor pendidikan menjadi salah satu target utama serangan siber karena lemahnya sistem keamanan jaringan dan rendahnya kesadaran pengguna terhadap perlindungan data. (Awan et al., 2024) menambahkan bahwa kawasan Asia Tenggara kini

menghadapi tantangan besar berupa serangan siber lintas batas, termasuk penyebaran *ransomware* dan *phishing* yang menargetkan mahasiswa dan institusi pendidikan.

Rendahnya kesadaran keamanan siber di kalangan mahasiswa Indonesia telah dibuktikan oleh berbagai penelitian sebelumnya. (Al-Misran & Candiwan, 2025) menegaskan bahwa tingkat literasi keamanan digital mahasiswa di Indonesia masih di bawah rata-rata negara ASEAN lainnya karena minimnya kegiatan edukasi dan pelatihan praktis di kampus. Sementara itu, (Anwar et al., 2024) menyoroti masih terbatasnya program peningkatan kapasitas siber berbasis masyarakat, khususnya di wilayah dengan infrastruktur digital yang belum merata.

Mahasiswa baru Program Studi Sistem Informasi UIN Sulthan Thaha Saifuddin Jambi merupakan kelompok yang aktif menggunakan perangkat digital untuk kebutuhan belajar, namun belum memiliki pemahaman yang cukup terhadap ancaman malware dan praktik keamanan siber yang baik. Berdasarkan pengamatan awal, sebagian besar mahasiswa hanya mengenal istilah "virus komputer" dan belum memahami jenis-jenis ancaman lain seperti *trojan* atau *spyware*. Kondisi ini menunjukkan perlunya kegiatan edukatif dasar yang bersifat sosialisatif untuk menumbuhkan kesadaran keamanan digital sejak dini.

Kegiatan Pengabdian Kepada Masyarakat (PKM) ini dirancang dalam bentuk sosialisasi edukatif partisipatif mengenai pengenalan malware dan pencegahannya. Pendekatan ini menekankan keterlibatan aktif peserta dalam diskusi dan tanya jawab interaktif, sehingga proses pembelajaran menjadi lebih menarik dan mudah dipahami (Katuk et al., 2023; Liang et al., 2024). Kegiatan ini tidak bertujuan mengukur hasil secara statistik, tetapi berfokus pada peningkatan pemahaman dan kesadaran awal mahasiswa terhadap keamanan siber.

Melalui kegiatan sosialisasi ini, diharapkan mahasiswa baru memiliki pemahaman dasar mengenai ancaman malware, dampaknya terhadap aktivitas akademik, serta langkah-langkah sederhana yang dapat dilakukan untuk melindungi perangkat pribadi. Selain itu, kegiatan ini diharapkan dapat menjadi model edukatif sederhana untuk meningkatkan budaya sadar keamanan digital di lingkungan kampus berbasis keislaman.

2. METODE

Kegiatan Pengabdian Kepada Masyarakat (PKM) ini dilaksanakan dengan metode sosialisasi edukatif partisipatif yang menekankan keterlibatan aktif peserta dalam proses pembelajaran. Pendekatan ini dipilih karena efektif untuk memperkenalkan konsep dasar keamanan digital melalui interaksi langsung antara pemateri dan peserta (Baraka et al., 2023; Liang et al., 2024).

a. Lokasi dan Waktu Pelaksanaan

Kegiatan dilaksanakan pada Kamis, 18 September 2025, bertempat di ruang perkuliahan Program Studi Sistem Informasi, Fakultas Sains dan Teknologi, Universitas Islam Negeri Sulthan Thaha Saifuddin Jambi. Kegiatan berlangsung selama dua jam dengan melibatkan 25 mahasiswa baru semester pertama kelas 1D sebagai peserta. Mahasiswa baru dipilih karena merupakan pengguna aktif perangkat digital dan media sosial, namun sebagian besar belum memiliki pemahaman mendasar tentang ancaman malware.

b. Tahapan Pelaksanaan

Pelaksanaan kegiatan dibagi menjadi tiga tahapan utama, yaitu persiapan, pelaksanaan, dan refleksi hasil kegiatan.

1. Tahap Persiapan

Tim pengabdi menyiapkan materi sosialisasi dalam bentuk presentasi PowerPoint yang menjelaskan pengertian malware, jenis-jenisnya, dampak yang ditimbulkan, serta cara pencegahan sederhana. Selain itu, dilakukan koordinasi dengan pihak kelas untuk penggunaan ruang, fasilitas proyektor, dan dokumentasi kegiatan.

2. Tahap Pelaksanaan

Kegiatan dimulai dengan pembukaan dan tanya jawab awal untuk menggali pemahaman dasar peserta mengenai malware. Selanjutnya, pemateri menyampaikan materi utama secara interaktif dan mendorong peserta untuk berbagi pengalaman pribadi terkait infeksi virus komputer. Di akhir kegiatan, dilakukan kuis ringan dengan pemberian hadiah (*reward*) bagi peserta yang mampu menjawab pertanyaan dengan benar. Strategi ini bertujuan untuk meningkatkan antusiasme serta memperkuat pemahaman peserta terhadap materi yang disampaikan.

3. Tahap Refleksi dan Evaluasi Kualitatif

Evaluasi kegiatan dilakukan secara deskriptif kualitatif berdasarkan observasi langsung terhadap keaktifan, antusiasme, dan partisipasi peserta selama kegiatan berlangsung. Indikator keberhasilan kegiatan ditinjau dari:

a. Tingginya keterlibatan peserta dalam sesi tanya jawab,

b. Kemampuan peserta menjawab pertanyaan dengan benar, dan
c. Respon positif terhadap pentingnya keamanan digital.

Penilaian semacam ini digunakan sebagai ukuran keberhasilan non-statistik dalam konteks sosialisasi partisipatif (Kurniawan et al., 2025).

c. Instrumen dan Media

Instrumen kegiatan berupa materi presentasi PowerPoint dan lembar dokumentasi kegiatan. Media ini dirancang untuk membantu peserta memahami konsep dasar malware. Selain itu, sesi tanya jawab berfungsi sebagai alat ukur informal untuk menilai tingkat pemahaman peserta secara langsung (Berkouk et al., 2025).

d. Etika Pelaksanaan dan Kolaborasi

Kegiatan dilaksanakan dengan memperhatikan etika akademik, melibatkan koordinasi antara pelaksana dan mahasiswa PKM. Setiap peserta diberikan kesempatan berpendapat tanpa paksaan, dan kegiatan berlangsung dalam suasana terbuka serta kondusif. Pendekatan ini sejalan dengan prinsip *community-based learning*, yang menempatkan peserta sebagai mitra dalam proses pembelajaran (Anwar et al., 2024).

3. HASIL DAN PEMBAHASAN

Kegiatan Pengabdian Kepada Masyarakat (PKM) ini dilaksanakan dalam bentuk sosialisasi edukatif mengenai pengenalan malware dan pencegahannya kepada mahasiswa baru Program Studi Sistem Informasi, Fakultas Sains dan Teknologi, Universitas Islam Negeri Sulthan Thaha Saifuddin Jambi. Kegiatan dilaksanakan pada tanggal 18 September 2025 dengan melibatkan 25 mahasiswa baru sebagai peserta. Tujuan utama kegiatan ini adalah memberikan pemahaman dasar tentang konsep malware, dampaknya terhadap aktivitas digital, serta langkah pencegahan sederhana yang dapat diterapkan dalam kehidupan akademik.

Pelaksanaan kegiatan berjalan sesuai dengan jadwal yang telah dirancang sebagaimana ditunjukkan pada Tabel 1.

Table I. Jadwal Pelaksanaan Kegiatan

Waktu	Kegiatan	Penanggung Jawab
14 : 30	Pembukaan	Andrian
14 : 35	Pengantar dan Tanya Jawab Awal	Wajid
14 : 42	Penyampaian Materi	Wajid
15 : 34	Diskusi & Tanya Jawab	Julia
15 : 40	Penutup	Andrian

Kegiatan diawali dengan sambutan dan penjelasan singkat tentang tujuan pelaksanaan PKM. Pada sesi pembuka, dilakukan tanya jawab awal untuk mengetahui sejauh mana mahasiswa memahami istilah *malware*. Hasil interaksi menunjukkan bahwa sebagian besar peserta hanya mengenal "virus komputer" sebagai ancaman utama dan belum memahami bentuk-bentuk malware lainnya seperti *trojan*, *ransomware*, atau *spyware*.

Selanjutnya, pemateri menyampaikan materi menggunakan PowerPoint untuk memberikan penjelasan cara kerja malware secara sederhana. Kegiatan berlangsung secara interaktif, di mana peserta diajak berdiskusi mengenai pengalaman pribadi mereka saat menghadapi infeksi virus komputer atau perangkat yang melambat akibat malware. Menurut (Liang et al., 2024), metode partisipatif semacam ini meningkatkan retensi pemahaman karena peserta terlibat langsung dalam pembentukan makna pengetahuan baru.

Sesi diskusi dan tanya jawab berlangsung dinamis. Peserta aktif memberikan tanggapan, berbagi pengalaman, dan menanyakan cara aman mengunduh aplikasi. Di akhir kegiatan, dilakukan kuis ringan dengan pemberian hadiah (reward) bagi peserta yang dapat menjawab pertanyaan dengan benar. Strategi ini efektif meningkatkan motivasi dan antusiasme peserta terhadap topik keamanan digital, sejalan dengan temuan (Katuk et al., 2023) bahwa pendekatan berbasis penghargaan dapat memperkuat pemahaman konsep keamanan siber dasar di kalangan mahasiswa.

Berdasarkan hasil observasi lapangan, kegiatan sosialisasi ini berjalan dengan baik dan mendapat tanggapan positif dari peserta. Indikator keberhasilan kegiatan dinilai dari:

1. Keaktifan peserta dalam sesi tanya jawab dan diskusi,
2. Kemampuan peserta menjawab pertanyaan akhir dengan benar, dan
3. Antusiasme peserta yang terlihat dari keterlibatan mereka dalam setiap sesi.

Aspek-aspek tersebut menunjukkan bahwa kegiatan berhasil menumbuhkan kesadaran awal mahasiswa terhadap pentingnya keamanan digital. Pendekatan ini juga mendukung konsep *community awareness learning*, yaitu pembelajaran berbasis kesadaran kolektif melalui kegiatan sosial-edukatif (Berkouk et al., 2025).

Dari sisi keunggulan kegiatan, metode sosialisasi partisipatif mudah diterapkan, tidak

memerlukan peralatan khusus, dan dapat diadaptasi oleh dosen atau lembaga lain untuk tema edukatif berbeda. Kegiatan ini memperlihatkan efektivitas komunikasi interpersonal dalam membangun literasi digital (Baraka et al., 2023; Kurniawan et al., 2025).

Namun demikian, terdapat beberapa keterbatasan, antara lain keterbatasan waktu sehingga sesi tanya jawab tidak dapat menampung seluruh pertanyaan peserta, serta keterbatasan fasilitas proyektor yang sempat mengganggu penyampaian materi PowerPoint. Kendala teknis tersebut tidak mempengaruhi substansi kegiatan, tetapi dapat menjadi pertimbangan untuk perbaikan pelaksanaan di masa mendatang.

Secara keseluruhan, kegiatan ini memberikan dampak positif terhadap peningkatan kesadaran mahasiswa baru terhadap keamanan siber, khususnya ancaman malware. Kegiatan ini juga membuka peluang untuk dikembangkan menjadi program edukatif rutin dengan cakupan lebih luas, seperti pelatihan keamanan data pribadi dan etika penggunaan teknologi informasi di lingkungan kampus keagamaan.

Gambar 1. Kegiatan Sosialisasi Pengenalan Malware

4. KESIMPULAN

Kegiatan Pengabdian Kepada Masyarakat (PKM) dengan tema *"Sosialisasi Pengenalan Malware dan Pencegahannya bagi Mahasiswa Baru Program Studi Sistem Informasi UIN Sulthan Thaha Saifuddin Jambi"* telah dilaksanakan dengan baik dan berjalan sesuai rencana. Melalui metode sosialisasi edukatif partisipatif, kegiatan ini berhasil meningkatkan pemahaman awal mahasiswa terhadap konsep malware, jenis-jenisnya, serta langkah-langkah sederhana dalam pencegahannya.

Meskipun kegiatan ini tidak menggunakan instrumen pengukuran kuantitatif, keberhasilannya dapat dilihat dari partisipasi aktif, antusiasme, serta kemampuan peserta dalam menjawab pertanyaan dan berdiskusi mengenai materi yang disampaikan. Pendekatan interaktif terbukti efektif dalam membangun kesadaran awal mahasiswa terhadap pentingnya keamanan digital, sejalan dengan prinsip literasi digital berbasis komunitas.

Kegiatan ini juga memberikan dampak positif terhadap pembentukan budaya *security awareness* di lingkungan kampus. Melalui sosialisasi ini, mahasiswa baru mulai menyadari bahwa keamanan siber bukan hanya tanggung jawab teknis, melainkan bagian dari perilaku etis dalam penggunaan teknologi informasi di kehidupan akademik.

Adapun saran dari pelaksanaan kegiatan ini yaitu agar kegiatan serupa dapat dilaksanakan secara berkala dan dikembangkan ke dalam bentuk pelatihan lanjutan yang mencakup praktik langsung, seperti simulasi deteksi malware dan pelatihan keamanan data pribadi. Selain itu, kolaborasi antara dosen, mahasiswa senior, dan pihak fakultas dapat memperluas dampak kegiatan, menjadikannya program edukatif berkelanjutan di lingkungan UIN Sulthan Thaha Saifuddin Jambi.

5. UCAPAN TERIMAKASIH

Penulis mengucapkan terima kasih kepada para pelaksana yang telah memberikan dukungan dalam pelaksanaan kegiatan Pengabdian Kepada Masyarakat ini. Ucapan terima kasih juga disampaikan kepada para mahasiswa peserta sosialisasi atas partisipasi aktif dan antusiasme mereka selama kegiatan berlangsung.

DAFTAR PUSTAKA

[1] Al-Misran, S. A., & Candiwan, C. (2025). Cybersecurity awareness in Indonesia: Factors, attitude, and practical implications. *Proceedings of the IEEE 11th International Conference on ICT*. https://ieeexplore.ieee.org/document/11088470

[2] Anwar, M., Karolita, D., Areni, I. S., & Wardhani, T. P. M. (2024). Cyber capacity building in Indonesia: A study of cyber security awareness in rural community. In *Digital Society and Cyber Empowerment* (pp. 245–260). Springer. https://link.springer.com/chapter/10.1007/978-981-96-0868-3_21

[3] Awan, J. H., Shah, S. R. H., & Charan, K. (2024). Southeast Asia and the growing challenge of cyber-attacks: A regional security insight. *Journal of Far East & South East Asia Studies*, *18*(2), 77–95. https://www.researchgate.net/publication/392927116

[4] Baraka, H., Suleiman, A., & Mutia, M. (2023). Evaluating participatory community engagement approaches for digital literacy in higher education institutions. *Journal of Applied Information and Communication*, *12*(2), 45–58.

https://doi.org/10.1016/j.jaic.2023.04.009

[5] Berkouk, D., Chatterjee, U., Bouzir, T. A. K., & Dhaou, I. B. (2025). *Proceedings of the 1st International Conference on Creativity, Technology, and Sustainability (CCTS 2024)*. OAPEN. https://library.oapen.org/handle/20.500.12657/100786

[6] Chang, L. Y. C., & Coppel, N. (2020). Building cyber security awareness in a developing country: Lessons from Myanmar. *Computers & Security*, *97*, 102–118. https://doi.org/10.1016/j.cose.2020.102235

[7] Katuk, N., Zaimy, N. A., Krishnan, S., & Kunhiraman, R. K. (2023). Fostering cyber-resilience in higher education: A pilot evaluation of a malware awareness program for college students. In *Innovations in Digital Education* (pp. 155–168). Springer. https://link.springer.com/chapter/10.1007/978-981-99-9592-9_12

[8] Kurniawan, W., Romadloni, N. T., & Bintang, R. A. K. N. (2025). Pemberdayaan literasi digital siswa melalui kegiatan lokakarya kolaboratif Disarpus Karanganyar. *Cahaya Pengabdian*, *3*(1), 34–41. https://jurnalapik.id/index.php/cp/article/view/191

[9] Liang, C. W., Cheng, K. T., & Lin, M. (2024). Evaluating cybersecurity participatory awareness programs among university students: A mixed-method approach. *Computers & Security*, *140*, 103781. https://doi.org/10.1016/j.cose.2024.103781

[10] Pratiwi, F. I., Hennida, C., & Soesilowati, S. (2024). Cybersecurity challenges in Indonesia: Threat and responses analysis. *Perspectives on Global Development and Technology*, *22*(3–4), 239–259. https://brill.com/view/journals/pgdt/22/3-4/article-p239_6.xml