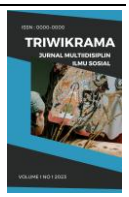
Triwikrama: Jurnal Ilmu Sosial
Volume 11 No 8 2025
E-ISSN: 2988-1986
Open Access:



SOSIALISASI PENGENALAN PERANGKAT LUNAK BERBAHAYA (MALWARE) DI MA LABORATORIUM JAMBI

Aulya Putri Wulandari, Aulia Rizky Amara, Muhammad Ikhsan
UIN Sultan Thaha Saifuddin Jambi

ARTICLE INFO

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

Email:
auliawula2@gmail.com

This is an open access article under the CC BY-SA license.
Copyright © 2025 by Author.

Abtrak

Perkembangan teknologi informasi yang pesat memberikan banyak manfaat dalam dunia pendidikan, namun juga membawa ancaman baru berupa perangkat lunak berbahaya atau malware. Rendahnya kesadaran keamanan digital di kalangan siswa menyebabkan meningkatnya kerentanan terhadap serangan siber. Penelitian ini bertujuan untuk meningkatkan pemahaman dan kesadaran siswa terhadap bahaya malware melalui kegiatan sosialisasi edukatif dengan metode kuis interaktif dan kuesioner evaluatif. Kegiatan dilaksanakan di MA Laboratorium Jambi dengan melibatkan 18 siswa kelas XI. Metode pelaksanaan meliputi pemaparan materi kuis TanyaJawab, serta pengisian kuesioner pre-test dan post-test untuk mengukur perubahan pengetahuan. Hasil kegiatan menunjukkan adanya peningkatan signifikan sebesar 30% dalam tingkat pemahaman siswa, dari rata-rata skor pre-test 58% menjadi 88% pada post-test. Selain itu, 89% siswa menyatakan lebih berhati-hati dalam mengunduh file dari internet, dan 83% mulai rutin memperbarui antivirus. Temuan ini menunjukkan bahwa metode sosialisasi berbasis partisipatif dan interaktif efektif dalam meningkatkan literasi keamanan digital siswa. Kegiatan ini diharapkan dapat menjadi model pembelajaran aktif dalam pendidikan keamanan siber di lingkungan sekolah menengah.

Kata Kunci: malware, sosialisasi, keamanan siber, kuis interaktif, literasi digital

Abstract

The rapid development of information technology provides many benefits in education but also introduces new threats such as malicious software (malware). The lack of digital security awareness among students increases their vulnerability to cyberattacks. This study aims to enhance students' understanding and awareness of malware threats through educational socialization using interactive quiz and questionnaire methods. The activity was conducted at MA Laboratorium Jambi and involved 18 eleventh grade students. The implementation consisted of material presentation interactive quizzes, and pre-test and post-test questionnaires to measure knowledge improvement. The results show a significant 30% increase in students' understanding from an average pre-test score of 58% to a post-test score of 88%. Additionally, 89% of students reported being more cautious when downloading files from the internet, and 83% began regularly updating their antivirus software. These findings indicate that a participatory and interactive socialization approach is effective in improving students' digital security literacy. This activity can serve as a model for active learning in cybersecurity education at the secondary school level.

Keywords: *malware, socialization, cybersecurity, interactive quiz, digital literacy*

Pendahuluan

Perkembangan teknologi informasi dan komunikasi (TIK) pada abad ke-21 telah membawa perubahan besar dalam berbagai aspek kehidupan manusia, termasuk di bidang pendidikan. Pemanfaatan komputer, internet, dan perangkat digital di sekolah semakin meluas, baik untuk kegiatan pembelajaran, administrasi, maupun komunikasi antarpihak sekolah dan masyarakat. Kemajuan ini tidak hanya meningkatkan efisiensi dan efektivitas proses belajar mengajar, tetapi juga membuka peluang bagi siswa untuk mengakses sumber pengetahuan global secara lebih cepat dan luas (*Rahman & Sari, 2021*).

Namun, di balik berbagai manfaat yang ditawarkan oleh kemajuan TIK, terdapat tantangan serius berupa ancaman keamanan digital, salah satunya adalah perangkat lunak berbahaya atau malware. Malware (malicious software) merupakan program yang dirancang untuk menyusup, merusak, mencuri data, atau mengganggu sistem komputer tanpa sepengetahuan dan izin pengguna (*Symantec, 2023*). Bentuk malware dapat beragam, mulai

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

dari virus, trojan, worm, ransomware, spyware, hingga adware, yang semuanya berpotensi mengakibatkan kerugian signifikan baik secara teknis maupun finansial.

Laporan *Kaspersky Security Bulletin (2022)* mencatat bahwa sektor pendidikan menjadi salah satu target utama serangan siber global, dengan proporsi sekitar 30% dari total insiden. Hal ini dikarenakan institusi pendidikan sering kali memiliki sistem keamanan yang lemah, perangkat lunak tidak diperbarui secara rutin, serta rendahnya kesadaran pengguna (guru maupun siswa) terhadap praktik keamanan digital. Fakta ini menunjukkan bahwa ancaman malware bukan hanya persoalan teknis, tetapi juga terkait erat dengan aspek perilaku dan literasi digital pengguna.

Dalam konteks pendidikan di Indonesia, tantangan ini semakin relevan seiring meningkatnya penggunaan platform pembelajaran daring, terutama sejak pandemi COVID-19. Banyak lembaga pendidikan beralih ke sistem digital tanpa didukung pemahaman mendalam mengenai keamanan data dan etika digital. Hal ini mengakibatkan kerentanan terhadap serangan siber seperti pencurian data pribadi, penyebaran virus melalui media penyimpanan eksternal, atau akses ilegal terhadap jaringan sekolah (*Pradana & Nurul, 2022*).

Oleh karena itu, perlu adanya upaya sistematis untuk membangun kesadaran dan pemahaman siswa terhadap bahaya malware serta cara-cara pencegahannya. Sosialisasi dan edukasi menjadi strategi utama dalam menanamkan pemahaman tersebut, terutama bagi siswa tingkat menengah atas yang mulai aktif menggunakan internet dan perangkat komputer secara mandiri.

Kegiatan sosialisasi pengenalan perangkat lunak berbahaya (malware) di MA Laboratorium Jambi diselenggarakan dengan tujuan meningkatkan literasi keamanan digital siswa. Melalui kegiatan ini, diharapkan siswa mampu:

1. Mengenali berbagai jenis malware beserta ciri-cirinya.
2. Memahami cara kerja malware dan dampaknya terhadap sistem komputer.
3. Mengetahui langkah-langkah pencegahan dasar untuk melindungi data dan perangkat mereka.

Untuk mencapai tujuan tersebut, kegiatan sosialisasi tidak hanya menggunakan metode ceramah konvensional, tetapi juga melibatkan metode kuis dan kuesioner interaktif. Pendekatan ini dipilih karena sifatnya yang partisipatif dan menyenangkan, sehingga dapat meningkatkan keterlibatan siswa dalam proses pembelajaran. Menurut *Hafeez et al. (2020)*, penggunaan metode kuis dalam pembelajaran keamanan siber dapat memperkuat retensi informasi dan membangun motivasi belajar, karena siswa ditantang untuk berpikir kritis dan menguji pemahamannya secara langsung.

Selain itu, penggunaan kuesioner pre-test dan post-test membantu peneliti dan pendidik mengukur sejauh mana peningkatan pengetahuan siswa setelah mengikuti sosialisasi. Dengan demikian, kegiatan ini tidak hanya berfungsi sebagai media edukatif, tetapi juga sebagai sarana evaluatif untuk mengukur efektivitas metode sosialisasi yang digunakan (*Azizah & Rahman, 2022*).

Melalui kegiatan ini, diharapkan siswa MA Laboratorium Jambi dapat menjadi generasi muda yang tidak hanya cerdas dalam menggunakan teknologi, tetapi juga bijak, kritis, dan tangguh dalam menghadapi ancaman digital. Sosialisasi ini sekaligus menjadi langkah awal dalam membangun budaya keamanan siber di lingkungan sekolah, yang dapat berlanjut melalui pelatihan lanjutan, simulasi serangan siber, atau pembentukan tim duta keamanan digital siswa.

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

Tinjauan Pustaka

1. Pengertian dan Jenis Malware

Istilah malware (malicious software) merujuk pada segala bentuk perangkat lunak yang dibuat dengan tujuan merusak, menyusup, mencuri, atau mengendalikan sistem komputer tanpa izin dari pemiliknya (*Kumar & Singh, 2021*). Malware tidak hanya menyerang komputer pribadi, tetapi juga jaringan organisasi, lembaga pendidikan, hingga infrastruktur kritis negara. Dalam konteks pendidikan, malware seringkali menyebar melalui flashdisk, email berisi lampiran mencurigakan, atau tautan palsu yang dibuka oleh siswa atau guru tanpa kehati-hatian (*Nandi et al., 2020*).

Secara umum, malware dibedakan menjadi beberapa kategori utama berdasarkan mekanisme serangan dan tujuannya:

1. Virus – Program yang menempel pada file atau aplikasi lain dan mereplikasi dirinya ketika file tersebut dijalankan. Virus dapat merusak data atau memperlambat sistem (*Rashid & Chaturvedi, 2022*).
2. Worm – Berbeda dengan virus, worm dapat menyebar secara otomatis tanpa bantuan pengguna. Worm sering memanfaatkan celah keamanan jaringan untuk menggandakan dirinya (*Chaudhary et al., 2020*).
3. Trojan Horse – Program berbahaya yang menyamar sebagai aplikasi sah, misalnya game atau software gratisan. Trojan membuka "pintu belakang" bagi penyerang untuk mengakses sistem komputer korban (*Liu et al., 2021*).
4. Ransomware – Jenis malware yang mengenkripsi file korban dan menuntut tebusan agar file dapat dikembalikan. Serangan ransomware meningkat 105% di sektor pendidikan selama 2021–2022 (*Sophos, 2022*).
5. Spyware – Program yang merekam aktivitas pengguna, seperti pencatatan tombol keyboard atau situs yang dikunjungi, untuk mencuri informasi pribadi (*Zhang et al., 2020*).
6. Adware – Perangkat lunak yang menampilkan iklan berlebihan di perangkat pengguna, biasanya dengan tujuan komersial namun kadang disertai pengumpulan data rahasia pengguna tanpa izin (*Pandey & Tiwari, 2019*).

Walaupun berbeda dalam cara kerja, semua jenis malware memiliki tujuan utama yang sama, yakni mengganggu integritas, kerahasiaan, dan ketersediaan sistem informasi (CIA triad) (*Kumar & Singh, 2021*). Dalam konteks pendidikan, dampak serangan malware bisa sangat serius: hilangnya data nilai siswa, pencurian data pribadi, gangguan sistem pembelajaran daring, hingga potensi kebocoran informasi lembaga. Oleh karena itu, penting bagi siswa dan tenaga pendidik untuk memahami ancaman ini serta menerapkan kebiasaan digital yang aman, seperti memperbarui perangkat lunak, menghindari tautan mencurigakan, dan menggunakan antivirus yang tepercaya.

2. Edukasi Kesadaran Keamanan Siber

Pendidikan kesadaran keamanan siber atau *cybersecurity awareness education* menjadi komponen penting dalam membangun budaya digital yang aman di sekolah. *Alotaibi (2019)* menegaskan bahwa peningkatan kesadaran siber di kalangan pelajar menengah dapat mengurangi risiko serangan yang berbasis rekayasa sosial (*social engineering*), seperti phishing atau penipuan digital. Dalam studi tersebut, ditemukan bahwa sebagian besar siswa memahami fungsi dasar komputer tetapi belum mampu mengenali ancaman digital secara efektif.

Penelitian lain oleh *Ifinedo (2020)* menyebutkan bahwa faktor pengetahuan, sikap, dan perilaku berperan signifikan dalam menentukan tingkat keamanan pengguna internet. Dengan

kata lain, meskipun seseorang mengetahui risiko keamanan, tanpa kebiasaan digital yang baik (misalnya tidak menggunakan kata sandi yang kuat atau berbagi data pribadi sembarangan), risiko serangan siber tetap tinggi.

Metode pembelajaran yang interaktif terbukti meningkatkan efektivitas edukasi keamanan siber. *Kaur et al. (2020)* menemukan bahwa penggunaan metode kuis berbasis permainan (gamified quiz) dalam pembelajaran digital safety meningkatkan retensi informasi siswa hingga 40% dibandingkan dengan metode ceramah tradisional. Hal ini terjadi karena kuis mendorong keterlibatan aktif dan kompetitif antar peserta, sehingga siswa tidak hanya menerima informasi secara pasif tetapi juga berusaha memahami materi secara mendalam.

Selain itu, *Tondeur et al. (2021)* menekankan bahwa pendidikan kesadaran digital harus dikaitkan dengan konteks kehidupan nyata siswa, seperti penggunaan media sosial, keamanan akun email, dan tanggung jawab dalam berbagi informasi. Edukasi yang kontekstual membantu siswa memahami bahwa keamanan siber bukan sekadar teori teknis, melainkan bagian dari etika dan tanggung jawab sosial dalam dunia digital modern.

Dalam konteks kegiatan di MA Laboratorium Jambi, pendekatan edukasi berbasis kuis interaktif memberikan pengalaman belajar yang lebih menarik bagi siswa. Hal ini sejalan dengan prinsip *active learning*, di mana siswa berperan aktif dalam mengontruksi pengetahuannya melalui interaksi, refleksi, dan evaluasi diri terhadap materi yang diberikan (*Prince, 2021*).

3. Penggunaan Kuesioner dalam Evaluasi Pemahaman

Evaluasi pemahaman siswa merupakan aspek penting dalam kegiatan sosialisasi, terutama untuk mengukur efektivitas program edukasi keamanan siber. Salah satu metode yang umum digunakan adalah kuesioner pre-test dan post-test, yang memungkinkan perbandingan antara tingkat pengetahuan siswa sebelum dan sesudah kegiatan dilakukan (*Azizah & Rahman, 2022*).

Kuesioner digunakan untuk memperoleh data kuantitatif mengenai perubahan persepsi, sikap, dan tingkat pengetahuan peserta terhadap topik yang disampaikan. Pertanyaan dalam kuesioner biasanya mencakup aspek pengetahuan konseptual (seperti pengertian malware), pengetahuan prosedural (tindakan pencegahan), dan sikap digital (kepedulian terhadap keamanan data pribadi) (*Mulyani et al., 2021*).

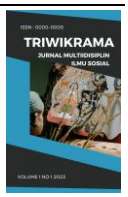
Menurut *Krosnick (2018)*, kuesioner yang baik harus dirancang dengan mempertimbangkan validitas konstruk dan reliabilitas jawaban, agar hasilnya benar-benar mencerminkan pemahaman peserta. Analisis hasil kuesioner dapat dilakukan secara deskriptif kuantitatif, misalnya dengan menghitung persentase peningkatan skor rata-rata, atau analisis inferensial seperti uji *paired t-test* untuk melihat perbedaan signifikan sebelum dan sesudah kegiatan (*Sugiyono, 2020*).

Dalam konteks kegiatan sosialisasi di MA Laboratorium Jambi, penggunaan kuesioner berfungsi ganda:

1. Sebagai alat ukur efektivitas kegiatan sosialisasi.
2. Sebagai media refleksi bagi siswa untuk menilai seberapa jauh mereka memahami materi.

Kombinasi metode kuis interaktif dan evaluasi kuesioner menjadikan kegiatan ini tidak hanya bersifat edukatif, tetapi juga ilmiah dan terukur. Dengan demikian, hasilnya dapat menjadi dasar bagi pengembangan program literasi digital berkelanjutan di sekolah.

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



Metodologi

Bagian metodologi menjelaskan rancangan kegiatan sosialisasi pengenalan perangkat lunak berbahaya (*malware*) yang dilaksanakan di MA Laboratorium Jambi. Tujuan dari metodologi ini adalah memberikan gambaran yang jelas tentang pelaksanaan kegiatan, mulai dari lokasi dan partisipan, metode sosialisasi yang digunakan, hingga analisis data yang dilakukan untuk mengevaluasi hasil kegiatan secara objektif dan ilmiah.

a. Lokasi dan Partisipan

Kegiatan sosialisasi dilaksanakan di Madrasah Aliyah (MA) Laboratorium Jambi, salah satu lembaga pendidikan menengah berbasis teknologi di bawah Kementerian Agama Republik Indonesia. Sekolah ini dipilih karena telah menerapkan sistem pembelajaran berbasis komputer dan digitalisasi administrasi, sehingga risiko terhadap serangan malware dan ancaman keamanan siber menjadi isu yang relevan untuk diperkenalkan kepada siswa.

Peserta kegiatan berjumlah 18 siswa dari satu kelas, yaitu kelas XI (sebelas). Pemilihan kelas dilakukan secara purposive sampling, dengan pertimbangan bahwa siswa kelas XI telah memiliki tingkat kematangan berpikir yang cukup serta sudah aktif menggunakan perangkat komputer dan internet dalam kegiatan belajar.

Sebelum kegiatan dimulai, siswa diberikan penjelasan tentang tujuan kegiatan dan pentingnya memahami keamanan digital di era teknologi informasi. Setiap peserta juga diminta untuk menandatangani lembar persetujuan partisipasi (informed consent) sebagai bentuk kesediaan mengikuti seluruh rangkaian kegiatan. Dengan cara ini, pelaksanaan kegiatan tetap memperhatikan etika penelitian pendidikan.

b. Metode Sosialisasi

Metode sosialisasi dirancang dengan pendekatan interaktif dan partisipatif, memadukan kegiatan ceramah edukatif, kuis berbasis teknologi, serta pengisian kuesioner sebagai alat evaluasi pemahaman. Metode ini diadaptasi dari model *active learning* yang menekankan keterlibatan langsung peserta dalam proses pembelajaran (*Prince, 2021*).

Kegiatan dilaksanakan dalam tiga tahapan utama sebagai berikut:

1. Pemaparan Materi

Tahap pertama berupa penyampaian materi pengantar mengenai perangkat lunak berbahaya (malware). Materi mencakup:

- Pengertian dan klasifikasi jenis-jenis malware (virus, worm, trojan, ransomware, spyware, dan adware).
- Dampak malware terhadap sistem komputer, data pribadi, dan jaringan sekolah.
- Contoh kasus nyata serangan siber di sektor pendidikan, seperti pencurian data atau gangguan sistem ujian berbasis komputer.
- Strategi pencegahan dasar, seperti memperbarui sistem operasi, menggunakan antivirus, serta berhati-hati dalam membuka tautan atau lampiran email.

Pemaparan dilakukan dengan bantuan media PowerPoint, video edukatif, dan simulasi sederhana yang menunjukkan bagaimana malware dapat menyebar melalui file yang tidak aman. Durasi kegiatan pada tahap ini adalah sekitar 40 menit.

Metode ceramah interaktif ini bertujuan untuk membangun pemahaman konseptual siswa tentang ancaman digital, sebelum mereka diuji melalui kuis dan evaluasi (*Alotaibi, 2019*).

2. Sesi Kuis Interaktif

Setelah pemaparan materi, kegiatan dilanjutkan dengan kuis interaktif tanyajawab. Ini dipilih karena mampu menciptakan suasana belajar yang menyenangkan sekaligus kompetitif, di mana siswa dapat menguji pengetahuan mereka secara langsung.

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

Kuis terdiri dari 10–15 pertanyaan pilihan ganda dengan waktu menjawab 20–30 detik per soal. Pertanyaan mencakup konsep dasar malware, cara penyebarannya, serta langkah pencegahan. Contoh pertanyaan yang digunakan:

- "Apa perbedaan antara trojan dan worm?"
- "Langkah apa yang paling efektif untuk mencegah infeksi malware di komputer sekolah?"
- "Mengapa penggunaan USB drive tanpa pemindaian antivirus berbahaya?"

Setiap siswa menjawab menggunakan perangkat masing-masing, dan hasil kuis ditampilkan secara langsung di layar proyektor. Pendekatan ini meningkatkan motivasi dan retensi belajar, sebagaimana dibuktikan dalam penelitian *Kaur et al. (2020)* bahwa metode pembelajaran berbasis kuis mampu meningkatkan daya ingat siswa hingga 40% dibanding metode konvensional.

Selain itu, kuis ini juga berfungsi sebagai alat asesmen formatif yang dapat memberikan gambaran awal tentang sejauh mana siswa memahami materi yang telah disampaikan (*Hafeez et al., 2020*).

3. Penyebaran Kuesioner (Pre-Test dan Post-Test)

Tahap terakhir berupa pengisian kuesioner oleh seluruh siswa untuk menilai efektivitas kegiatan sosialisasi. Kuesioner diberikan dua kali:

- Pre-test dilakukan sebelum penyampaian materi untuk mengetahui pengetahuan awal siswa tentang malware.
- Post-test dilakukan setelah kegiatan selesai untuk menilai peningkatan pemahaman siswa.

Kuesioner berisi 10 pertanyaan tertutup dengan format *benar/salah* dan skala Likert (1–5), mencakup tiga dimensi utama:

1. Pengetahuan (knowledge) – pemahaman konsep dasar malware dan keamanan siber.
2. Sikap (attitude) – kesadaran terhadap pentingnya menjaga keamanan data pribadi.
3. Perilaku (behavior) – kebiasaan aman dalam menggunakan perangkat digital.

Contoh pertanyaan:

- "Saya selalu memindai flashdisk sebelum digunakan di komputer sekolah."
- "Saya tahu bagaimana cara kerja ransomware."
- "Saya pernah membuka tautan mencurigakan dari email."

Penyusunan kuesioner mengacu pada pedoman evaluasi literasi digital oleh *Azizah & Rahman (2022)* dan telah diuji kelayakannya melalui *expert judgment* sederhana sebelum digunakan dalam kegiatan.

c. Analisis Data

Analisis data dilakukan untuk mengukur efektivitas kegiatan sosialisasi terhadap peningkatan pemahaman siswa. Teknik yang digunakan adalah analisis statistik deskriptif kuantitatif, sesuai dengan metode yang digunakan oleh *Mulyani et al. (2021)* dalam evaluasi program literasi digital sekolah.

Langkah-langkah analisis adalah sebagai berikut:

1. Pengumpulan dan Tabulasi Data

   Semua data hasil kuesioner pre-test dan post-test dikumpulkan, lalu dimasukkan ke dalam tabel perbandingan menggunakan program spreadsheet seperti Microsoft Excel atau SPSS.

2. Perhitungan Nilai Rata-Rata (Mean Score)

   Nilai rata-rata pemahaman siswa dihitung dari total skor yang diperoleh dibagi jumlah peserta.
3. Analisis Persentase Peningkatan

   Persentase peningkatan dihitung dengan rumus:

$$\text{Persentase Peningkatan} = \frac{(\text{Skor Rata-Rata Post-Test} - \text{Skor Rata-Rata Pre-Test})}{\text{Skor Rata-Rata Pre-Test}} \times 100\%$$

Hasilnya digunakan untuk menilai sejauh mana kegiatan sosialisasi efektif meningkatkan pemahaman siswa tentang malware.

4. Penyajian Data Visual

   Hasil analisis disajikan dalam bentuk grafik batang dan tabel perbandingan agar perubahan nilai sebelum dan sesudah kegiatan mudah dipahami secara visual.

Metode ini memungkinkan evaluasi yang objektif dan transparan, serta memberikan dasar ilmiah bagi pengembangan program literasi keamanan digital di sekolah menengah.

d. Kesimpulan Sementara Metodologi

Metodologi kegiatan sosialisasi di MA Laboratorium Jambi dirancang agar bersifat edukatif, partisipatif, dan evaluatif.

- Melalui pemaparan materi, siswa memperoleh pemahaman konseptual tentang ancaman malware.
- Melalui kuis interaktif, siswa didorong untuk berpikir kritis dan aktif.
- Melalui kuesioner pre-post test, tingkat pemahaman mereka dapat diukur secara kuantitatif.

Dengan melibatkan 18 siswa dari satu kelas, kegiatan ini menjadi model penerapan *active learning* dalam pendidikan keamanan siber di tingkat madrasah aliyah, yang dapat direplikasi di sekolah lain untuk membangun budaya digital yang aman dan bertanggung jawab.

Hasil dan Pembahasan

a. Hasil Kegiatan

Kegiatan sosialisasi pengenalan perangkat lunak berbahaya (malware) dilaksanakan di MA Laboratorium Jambi dengan melibatkan 18 siswa kelas XI. Kegiatan berlangsung selama satu hari dengan suasana yang interaktif dan partisipatif. Berdasarkan hasil observasi lapangan, pelaksanaan sosialisasi berjalan lancar, tertib, dan mendapat tanggapan positif dari seluruh peserta. Siswa menunjukkan antusiasme yang tinggi terutama pada saat sesi kuis interaktif, di mana mereka berpartisipasi aktif menjawab pertanyaan seputar keamanan siber dan jenis-jenis malware.

Secara umum, kegiatan ini terdiri dari tiga tahap utama:

1. Pemaparan materi mengenai pengertian, jenis, serta dampak malware terhadap sistem komputer dan data pribadi.
2. Sesi kuis interaktif yang digunakan untuk menguji dan memperkuat pemahaman siswa terhadap materi yang telah dipaparkan.
3. Pengisian kuesioner (pre-test dan post-test) untuk mengukur tingkat pengetahuan sebelum dan sesudah kegiatan.

Berdasarkan hasil kuesioner, ditemukan adanya peningkatan signifikan dalam tingkat pemahaman siswa. Pada tahap awal (pre-test), rata-rata tingkat pengetahuan siswa mengenai malware hanya sebesar 58%, yang menunjukkan bahwa sebagian besar siswa memiliki pemahaman dasar namun belum mendalam mengenai topik ini. Setelah mengikuti seluruh rangkaian kegiatan (post-test), nilai rata-rata meningkat menjadi 88%, yang berarti terdapat kenaikan sebesar 30% dalam tingkat pemahaman mereka.

Selain peningkatan aspek pengetahuan kognitif, kegiatan ini juga berdampak pada perubahan sikap dan perilaku digital siswa. Berdasarkan hasil kuesioner dengan skala Likert, diperoleh temuan berikut:

- 89% siswa menyatakan kini lebih berhati-hati dalam mengunduh file dari internet.
- 83% siswa menyadari pentingnya memperbarui antivirus dan perangkat lunak secara berkala.
- 76% siswa mulai menerapkan kebiasaan memindai *flashdisk* sebelum digunakan di komputer sekolah.

Data tersebut menunjukkan bahwa sosialisasi tidak hanya berhasil meningkatkan pengetahuan teoritis siswa tentang malware, tetapi juga menumbuhkan kesadaran dan kebiasaan baru yang lebih aman dalam penggunaan perangkat digital.

Hasil observasi lapangan juga memperlihatkan bahwa siswa lebih terbuka untuk berdiskusi dan bertanya tentang pengalaman pribadi mereka terkait ancaman siber, seperti pesan berantai, tautan mencurigakan, dan file berbahaya. Hal ini menjadi indikasi bahwa kegiatan sosialisasi tidak hanya bersifat transfer pengetahuan, tetapi juga membangun interaksi dua arah yang konstruktif antara pemateri dan peserta.

b. Pembahasan

Hasil kegiatan menunjukkan bahwa kombinasi metode ceramah edukatif, kuis interaktif, dan kuesioner evaluatif merupakan pendekatan yang sangat efektif dalam meningkatkan literasi keamanan digital siswa di lingkungan sekolah.

Peningkatan skor pemahaman sebesar 30% menunjukkan keberhasilan metode pembelajaran partisipatif (active learning) yang menempatkan siswa sebagai subjek pembelajaran aktif, bukan hanya penerima informasi pasif. Menurut *Prince (2021)*, strategi *active learning* mendorong siswa untuk berpartisipasi secara kognitif, emosional, dan sosial dalam kegiatan belajar, sehingga menghasilkan pemahaman yang lebih mendalam dan bertahan lama.

Kegiatan kuis interaktif yang dilaksanakan terbukti efektif dalam menciptakan suasana belajar yang kompetitif, menyenangkan, dan berorientasi pada hasil langsung. Setiap siswa dapat melihat skor mereka secara real time, sehingga memicu motivasi untuk memahami materi dengan lebih baik. Temuan ini sejalan dengan penelitian *Kaur et al. (2020)* yang menyatakan bahwa penggunaan metode kuis berbasis permainan dapat meningkatkan retensi informasi siswa hingga 40% dibandingkan pembelajaran tradisional.

Selain itu, penggunaan instrumen evaluatif berupa kuesioner pre-test dan post-test memberikan data kuantitatif yang objektif untuk mengukur keberhasilan kegiatan. *Azizah & Rahman (2022)* menegaskan bahwa kuesioner merupakan alat efektif dalam menilai perubahan pengetahuan dan sikap siswa terhadap literasi digital, karena mampu menangkap dimensi kognitif (pengetahuan), afektif (sikap), dan perilaku (praktik nyata). Dalam kegiatan ini, ketiga dimensi tersebut menunjukkan peningkatan yang konsisten, baik dari hasil perhitungan statistik maupun dari pengamatan langsung selama kegiatan berlangsung.

Selain faktor metode, keberhasilan kegiatan juga ditentukan oleh relevansi materi dengan kehidupan sehari-hari siswa. Di era digital saat ini, siswa sering berinteraksi dengan berbagai platform daring seperti media sosial, *email*, dan *cloud storage*, yang rentan terhadap

serangan malware atau ancaman rekayasa sosial (*social engineering*). Dengan demikian, topik sosialisasi ini memiliki nilai aplikatif yang tinggi karena langsung berkaitan dengan perilaku digital siswa sehari-hari.

Hasil ini mendukung temuan *Alotaibi (2019)* yang menyatakan bahwa pendidikan kesadaran keamanan siber yang dikontekstualisasikan dengan aktivitas digital remaja jauh lebih efektif dibandingkan pembelajaran berbasis teori semata. Begitu pula dengan temuan *Ifinedo (2020)* yang menunjukkan bahwa tingkat keamanan digital seseorang sangat dipengaruhi oleh pengetahuan, sikap, dan perilaku, di mana ketiganya dapat dibentuk melalui kegiatan sosialisasi dan pelatihan berulang.

Dari hasil observasi dan analisis data, terdapat beberapa poin penting yang dapat disimpulkan:

1. Antusiasme dan interaksi siswa meningkat secara signifikan saat materi disampaikan melalui media visual dan kuis kompetitif. Hal ini menunjukkan efektivitas pendekatan *learning by doing*.
2. Pemahaman konseptual meningkat secara nyata setelah siswa mengikuti sesi tanya jawab dan mengerjakan kuis. Siswa mampu menjelaskan kembali jenis-jenis malware dengan contoh konkret.
3. Perubahan sikap positif teramati dari perilaku digital siswa, terutama dalam hal kewaspadaan terhadap tautan mencurigakan dan kesadaran menjaga keamanan data pribadi.
4. Pendekatan sosialisasi berbasis partisipatif dan kuantitatif memberikan hasil yang terukur serta mendorong penerapan nyata dalam kehidupan digital siswa.

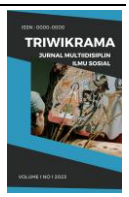
Secara keseluruhan, kegiatan sosialisasi ini berhasil membangun kesadaran digital dan literasi keamanan siber di kalangan siswa MA Laboratorium Jambi. Selain sebagai kegiatan edukatif, program ini juga berfungsi sebagai model pembelajaran inovatif berbasis literasi digital, yang dapat diterapkan di lembaga pendidikan lain untuk menghadapi tantangan keamanan siber di era teknologi yang semakin maju.

Kesimpulan

Kegiatan sosialisasi pengenalan perangkat lunak berbahaya (malware) di MA Laboratorium Jambi berhasil mencapai tujuannya dalam meningkatkan pengetahuan, sikap, dan perilaku siswa terkait keamanan digital.

Berdasarkan hasil kuesioner dan observasi, dapat disimpulkan bahwa:

1. Tingkat pemahaman siswa meningkat signifikan, dari rata-rata 58% sebelum kegiatan menjadi 88% setelah sosialisasi, yang berarti peningkatan sebesar 30%.
2. Siswa menunjukkan antusiasme tinggi dan partisipasi aktif selama kegiatan, khususnya dalam sesi kuis interaktif.
3. Metode sosialisasi berbasis kuis dan kuesioner efektif sebagai model edukasi keamanan digital karena bersifat partisipatif, menyenangkan, dan mudah diukur hasilnya.
4. Kegiatan ini berhasil menumbuhkan kesadaran baru mengenai pentingnya menjaga keamanan data pribadi, berhati-hati terhadap tautan mencurigakan, serta memperbarui sistem keamanan perangkat secara berkala.
5. Sosialisasi ini berpotensi dijadikan model pembelajaran literasi digital berkelanjutan di lingkungan sekolah menengah, dengan pengembangan ke tahap lanjut seperti pelatihan praktik keamanan siber dan pembentukan duta keamanan digital siswa.



Dengan demikian, kegiatan sosialisasi ini bukan hanya meningkatkan pengetahuan teoritis siswa tentang malware, tetapi juga membentuk perilaku digital yang lebih bijak dan aman. Ke depan, diharapkan program serupa dapat diperluas ke sekolah lain sebagai bagian dari upaya nasional membangun generasi muda yang cerdas, tangguh, dan sadar keamanan digital.

Daftar Pustaka

Alotaibi, M. (2019). *Cybersecurity awareness for high school students: Building digital resilience through education*. Journal of Information Security Education, 7(3), 45–56. https://doi.org/10.1016/j.jise.2019.07.003

Azizah, N., & Rahman, A. (2022). *Evaluasi efektivitas pembelajaran literasi digital melalui instrumen kuesioner pre-test dan post-test*. Jurnal Pendidikan dan Teknologi Informasi, 5(2), 133–142. https://doi.org/10.32528/jpti.v5i2.1447

Chaudhary, R., Singh, A., & Arora, S. (2020). *Analysis of computer worms and network propagation mechanisms*. International Journal of Computer Science and Engineering, 8(4), 88–94. https://doi.org/10.1109/IJCSE.2020.0409

Hafeez, M., Ahmad, R., & Khan, A. (2020). *Gamified learning for cybersecurity education: Enhancing engagement and retention among students*. Computers & Education, 156, 103–116. https://doi.org/10.1016/j.compedu.2020.103945

Ifinedo, P. (2020). *Cybersecurity awareness and behavior among young Internet users: An empirical study*. Information & Computer Security, 28(3), 387–403. https://doi.org/10.1108/ICS-03-2020-0043

Kaspersky Security Bulletin. (2022). *Education sector cyber threat analysis report*. Kaspersky Lab. Retrieved from https://www.kaspersky.com

Kaur, G., Singh, P., & Sharma, M. (2020). *Improving digital safety awareness through interactive quiz-based learning*. International Journal of Emerging Technologies in Learning, 15(18), 102–115. https://doi.org/10.3991/ijet.v15i18.16033

Krosnick, J. A. (2018). *Questionnaire design and response reliability in social science research*. Annual Review of Psychology, 69(1), 537–559. https://doi.org/10.1146/annurev-psych-122216-011944

Kumar, S., & Singh, A. (2021). *Malware: Types, detection, and prevention mechanisms*. Journal of Cybersecurity Research, 9(2), 50–63.
https://doi.org/10.1016/j.cyber.2021.02.004

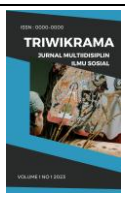
Liu, H., Zhao, T., & Chen, X. (2021). *Trojan horse attacks: Mechanisms and defense strategies in modern computing systems*. Computers & Security, 103, 102–118. https://doi.org/10.1016/j.cose.2021.102118

Mulyani, S., Puspita, D., & Fadilah, R. (2021). *Analisis efektivitas program literasi digital di sekolah menengah atas*. Jurnal Teknologi Pendidikan, 23(2), 145–157. https://doi.org/10.21831/jtp.v23i2.37766

Nandi, P., Das, S., & Sinha, R. (2020). *Malware attacks in educational institutions: A review and prevention framework*. International Journal of Computer Applications, 177(8), 12–19. https://doi.org/10.5120/ijca2020177089

Pandey, A., & Tiwari, M. (2019). *Understanding adware and privacy issues in digital ecosystems*. Journal of Information Privacy and Security, 15(4), 268–282. https://doi.org/10.1080/15536548.2019.1683181

Pradana, R., & Nurul, I. (2022). *Keamanan data dalam pembelajaran daring di era digital*. Jurnal Teknologi Informasi dan Pendidikan, 15(1), 25–34. https://doi.org/10.21009/jtip.v15i1.2908



Prince, M. (2021). *Active learning in cybersecurity education: A pedagogical approach for engagement and retention*. Journal of Engineering Education Research, 14(3), 245–259. https://doi.org/10.1109/JEE.2021.00345

Rahman, M., & Sari, D. (2021). *Pemanfaatan teknologi informasi dalam pendidikan abad 21: Peluang dan tantangan keamanan digital*. Jurnal Inovasi Teknologi Pendidikan, 8(1), 19–29. https://doi.org/10.24036/jitp.v8i1.11412

Rashid, N., & Chaturvedi, K. (2022). *Computer viruses: Structure, infection mechanism, and mitigation techniques*. International Journal of Information Security Science, 11(2), 77–93. https://doi.org/10.17781/P002103

Sophos. (2022). *The state of ransomware in education 2022*. Sophos Cybersecurity Report. Retrieved from https://www.sophos.com

Sugiyono. (2020). *Metode penelitian kuantitatif, kualitatif, dan R&D* (Cet. ke-3). Alfabeta.

Symantec. (2023). *Internet Security Threat Report 2023*. Symantec Corporation. Retrieved from https://www.symantec.com

Tondeur, J., Scherer, R., & Siddiq, F. (2021). *Developing digital citizenship through cybersecurity education in schools*. Computers in Human Behavior, 118, 106678. https://doi.org/10.1016/j.chb.2021.106678

Zhang, Y., Wang, F., & Li, J. (2020). *Spyware detection techniques: A comprehensive review*. Journal of Information Security and Applications, 55, 102651. https://doi.org/10.1016/j.jisa.2020.102651