



Edukasi Keamanan Digital sebagai Upaya Pencegahan Malware pada Penggunaan Smartphone di MAN 3 Kota Jambi

Fahri Fahrezi ^{1*}, Zam Zami Sihombing ², Siti Maryana ³

^{1,2,3,4,5}Program Studi Sistem Informasi, Fakultas Sains Dan Teknologi, Universitas Islam Negeri Sulthan Thaha Saifuddin Jambi

E-mail: fahrifahri1154@gmail.com, zamzamijanuari@gmail.com,
sitimaryana20017@gmail.com

ABSTRACT

Smartphones have become an essential device for daily activities, yet their high usage also increases exposure to malware attacks, particularly when users install applications from unofficial sources. This study focuses on identifying the awareness level of students at MAN 3 Kota Jambi regarding malware risks in smartphone use and examining their installation behaviors. A qualitative approach supported by eight Indonesian journals on malware detection, mobile security, and digital behavior is used. Findings show that students tend to underestimate malware threats and frequently install third-party APKs without evaluating permission and source legitimacy. This highlights the importance of digital literacy programs in academic environments.

Keywords: *Malware, Smartphone Security, APK, Cyber Threats, Digital Literacy*

ABSTRAK

Ponsel pintar telah menjadi perangkat penting dalam aktivitas sehari-hari, namun penggunaan yang intensif juga meningkatkan risiko terhadap serangan malware terutama ketika pengguna memasang aplikasi dari sumber tidak resmi. Penelitian ini berfokus pada tingkat kesadaran siswa MAN 3 Kota Jambi terkait ancaman malware serta analisis perilaku instalasi aplikasi mereka. Metode yang digunakan adalah deskriptif kualitatif dengan dukungan delapan jurnal Indonesia terkait deteksi malware, keamanan mobile, dan perilaku digital. Hasil penelitian menunjukkan bahwa siswa cenderung meremehkan ancaman malware dan sering memasang APK pihak ketiga tanpa mempertimbangkan izin maupun keamanan sumbernya. Temuan ini menguatkan pentingnya program literasi digital yang terstruktur di lingkungan pendidikan.

Kata Kunci: *Malware, Keamanan Ponsel, Aplikasi Non-Resmi, Ancaman Siber, Literasi Digital*

Article History

Received: November 2025

Reviewed: November 2025

Published: November 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/)

1. PENDAHULUAN

Perkembangan teknologi digital telah membawa perubahan besar dalam aktivitas manusia, termasuk dalam cara mengakses informasi, berkomunikasi, dan melakukan kegiatan



akademik. Smartphone menjadi perangkat utama bagi pelajar dalam menunjang proses belajar, terutama melalui penggunaan aplikasi pembelajaran, layanan cloud, dan platform berbasis internet Hidayat et al., (2024). Meski menawarkan banyak kemudahan, tingginya ketergantungan terhadap perangkat digital ini juga meningkatkan paparan terhadap ancaman keamanan siber.

Salah satu ancaman yang semakin meningkat adalah malware pada perangkat mobile. Malware dapat masuk melalui berbagai celah, seperti pemasangan aplikasi dari sumber tidak resmi, klik tautan berbahaya, penggunaan Wi-Fi publik, hingga pembaruan sistem yang tertunda Sapriadi et al., (2023). Di Indonesia, laporan keamanan digital menunjukkan bahwa serangan malware mobile meningkat secara signifikan beberapa tahun terakhir, bahkan sebagian besar kasus melibatkan pengguna remaja yang kurang memahami tanda-tanda infeksi malware (Anjani et al., 2024).

Di lingkungan pendidikan, termasuk di SMPN 30 Muaro Jambi, siswa secara aktif menggunakan smartphone sebagai sarana belajar. Namun hasil observasi awal menunjukkan bahwa banyak dari mereka belum memiliki pengetahuan dasar terkait keamanan digital, termasuk bagaimana mencegah atau mengenali malware. Oleh sebab itu, penelitian ini dilakukan untuk memperkuat literasi keamanan digital melalui sosialisasi khusus yang berfokus pada ancaman malware dan praktik penggunaan smartphone yang aman.

2. METODE PENELITIAN

Studi ini menerapkan metode deskriptif kualitatif dengan fokus penelitian di MAN 3 Kota Jambi. Pengumpulan data dilakukan melalui tiga teknik utama, yaitu sosialisasi keamanan digital, observasi langsung, dan telaah pustaka dari jurnal ilmiah serta laporan industri yang relevan.

Tahapan penelitian meliputi persiapan materi sosialisasi mengenai dasar-dasar keamanan smartphone, risiko instalasi aplikasi dari luar toko resmi, serta langkah pencegahan terhadap malware. Sosialisasi kemudian dilakukan melalui presentasi interaktif dan diskusi kasus, diikuti dengan pengamatan perubahan pengetahuan dan perilaku siswa setelah kegiatan berlangsung. Untuk memperkuat temuan lapangan, dilakukan perbandingan hasil observasi dengan literatur terbaru dari sumber akademis yang terpercaya.

3. HASIL DAN PEMBAHASAN

Sosialisasi yang dilaksanakan di MAN 3 Kota Jambi memberikan dampak positif terhadap peningkatan pemahaman siswa mengenai ancaman malware dan keamanan digital. Sebelum



kegiatan dilakukan, sebagian besar siswa hanya mengenal ancaman digital sebatas peretasan akun media sosial tanpa memahami bahwa malware dapat menyusup melalui aplikasi berbahaya, tautan palsu, maupun jaringan Wi-Fi publik. Setelah sosialisasi, mayoritas peserta dapat menyebutkan dan menjelaskan jenis-jenis malware seperti trojan, spyware, adware, dan ransomware, serta memahami ciri-ciri smartphone yang telah terinfeksi.

Hasil observasi menunjukkan bahwa terjadi perubahan pada kebiasaan siswa dalam mengelola keamanan perangkat mereka. Jika sebelumnya banyak siswa mengunduh aplikasi dari situs tidak resmi atau menonaktifkan pembaruan sistem karena dianggap mengganggu, setelah sosialisasi sebagian besar mulai memperhatikan sumber aplikasi, mengaktifkan pembaruan otomatis, dan memeriksa izin aplikasi secara lebih selektif. Selain itu, terdapat peningkatan signifikan dalam penggunaan kata sandi yang lebih kuat serta aktivasi autentikasi dua langkah pada akun media sosial yang mereka miliki.

Temuan lapangan juga menunjukkan bahwa sebagian siswa yang sebelumnya sering terpapar iklan pop-up, aplikasi tidak dikenal, dan penurunan kinerja perangkat mulai memahami bahwa gejala tersebut merupakan tanda potensi infeksi malware. Perubahan ini menunjukkan bahwa sosialisasi yang dilakukan mampu meningkatkan kesadaran siswa terhadap tanda-tanda ancaman digital serta langkah-langkah yang perlu diambil untuk mencegah kerusakan lebih lanjut.

PEMBAHASAN

Hasil penelitian ini memperkuat temuan dari berbagai studi sebelumnya yang menyatakan bahwa tingkat literasi digital memiliki hubungan erat dengan kerentanan pengguna terhadap malware, terutama di kalangan remaja. Berdasarkan penelitian Aulia et al. (2023), remaja cenderung menjadi target empuk serangan malware karena kebiasaan mengunduh aplikasi modifikasi dan sering mengabaikan izin aplikasi yang berlebihan. Kondisi ini sangat mirip dengan situasi yang ditemukan di MAN 3 Kota Jambi sebelum sosialisasi dilakukan, di mana sebagian siswa tidak memahami implikasi keamanan dari tindakan tersebut.

Penelitian Anjani et al. (2024) menegaskan bahwa peningkatan keamanan perangkat mobile dapat dicapai melalui edukasi yang terstruktur, karena pengetahuan tentang ancaman sangat memengaruhi sikap dan perilaku pengguna. Hal ini sejalan dengan hasil penelitian ini, di mana siswa mulai menerapkan langkah-langkah keamanan dasar setelah diberikan pemahaman yang jelas mengenai risiko malware.

Selanjutnya, temuan lapangan juga mendukung pendapat Serianti et al. (2024) yang menjelaskan bahwa instalasi aplikasi dari sumber tidak resmi merupakan jalur utama masuknya



malware ke perangkat mobile. Perubahan perilaku siswa setelah sosialisasi—terutama dalam memilih aplikasi hanya dari toko resmi—menunjukkan bahwa intervensi edukatif mampu menurunkan faktor risiko secara signifikan.

Dalam konteks penggunaan smartphone untuk aktivitas pembelajaran, literatur juga menunjukkan bahwa kebiasaan mengaitkan beberapa akun dalam satu aplikasi, membagikan data pribadi secara berlebihan, atau mengakses cloud tanpa pengaturan keamanan dapat meningkatkan peluang kebocoran data Istiqomah & Nasution, (2025). Temuan pada penelitian ini menunjukkan bahwa siswa mulai memperhatikan hal tersebut setelah mendapatkan penjelasan mengenai pentingnya manajemen data pribadi.

Secara keseluruhan, kegiatan sosialisasi ini terbukti mampu meningkatkan pemahaman konseptual sekaligus mengubah sebagian kebiasaan digital siswa. Namun, untuk mencapai perubahan yang lebih permanen, diperlukan program yang berkelanjutan dan melibatkan pihak sekolah secara aktif dalam membangun budaya keamanan digital.

KESIMPULAN

Penelitian mengenai kesadaran keamanan digital terkait ancaman malware pada penggunaan smartphone di MAN 3 Kota Jambi menunjukkan bahwa pemahaman siswa terhadap risiko instalasi aplikasi dari luar toko resmi, pembaruan sistem, serta praktik keamanan dasar masih tergolong rendah sebelum dilakukan sosialisasi. Setelah intervensi melalui kegiatan edukasi, siswa mulai memahami bentuk-bentuk ancaman seperti malware, phishing, dan pencurian data pribadi serta mampu menjelaskan dampaknya terhadap keamanan perangkat.

Temuan lapangan mengindikasikan bahwa faktor utama kerentanan berasal dari perilaku digital yang kurang aman, seperti penggunaan kata sandi yang lemah, kebiasaan mengunduh aplikasi dari sumber tidak resmi, serta kurangnya perhatian terhadap izin aplikasi. Kegiatan sosialisasi terbukti memberikan dampak positif, ditunjukkan dengan meningkatnya kesadaran siswa dalam menerapkan langkah pencegahan sederhana seperti autentikasi dua faktor, instalasi aplikasi dari toko resmi, dan pembaruan sistem secara rutin.

Dengan demikian, edukasi keamanan digital perlu diterapkan secara berkelanjutan agar perubahan perilaku dapat menjadi kebiasaan jangka panjang. Pihak sekolah disarankan untuk memperkuat program literasi digital, menyediakan pelatihan rutin untuk guru dan siswa, serta membuat kebijakan terkait penggunaan perangkat dan instalasi aplikasi yang aman. Upaya-upaya ini diharapkan dapat meminimalkan risiko terpapar malware dan meningkatkan ketahanan keamanan digital di lingkungan MAN 3 Kota Jambi.

**DAFTAR PUSTAKA**

- [1] Wiyono, T., Pratama, H., & Siregar, A. (2024). *Deteksi Malware Berbasiskan Analisis Statis Menggunakan Algoritma Convolutional Neural Network (CNN)*. Jurnal Sistem Komputer & Informatika (JSON), 7(1). <https://doi.org/10.30865/json.v7i1.8946>
- [2] Muhammad, A. H., Sugiantoro, B., & Luthfi, A. (2023). *Metode Klasifikasi dan Analisis Karakteristik Malware Menggunakan Konsep Ontologi*. Teknomatika: Jurnal Informatika & Komputer.
- [3] Cahyanto, T. A., Wahanggara, V., & Ramadana, D. (2023). *Analisis dan Deteksi Malware Menggunakan Metode Malware Analisis Dinamis dan Malware Analisis Statis*. JUSTINDO (Jurnal Sistem & Teknologi Informasi Indonesia).
- [4] Harjono, M. (2022). *Deteksi Malware dalam Jaringan Menggunakan Dionaea*. Jurnal Techno, Universitas Muhammadiyah Purwokerto. <https://doi.org/10.30595/techno.v14i2.96>
- [5] Jelita, I. N. B. A., & Siregar, H. (2024). *Systematic Literature Review: Evolusi Ancaman Siber dan Metode Deteksi Malware di Sistem Operasi Android (2020-2025)*. JUKTISI. <https://doi.org/10.62712/juktisi.v4i1.395>
- [6] Wijoyo, A., Putra, M., & Rahmadani, T. (2023). *Keamanan Cyber dalam Sistem Informasi Manajemen: Ancaman dan Solusi Terbaru*. Jurnal Ilmiah Wahana Pendidikan.
- [7] Anggana, N. D., Nurhayati, S., & Rahmawati, R. (2023). *Implementasi Pi-Hole untuk Membangun Sistem Pertahanan Jaringan dari Serangan Malvertising*. Teknomatika: Jurnal Informatika & Komputer.
- [8] Adenansi, R., & Novarina, L. A. (2021). *Malware Dynamic*. JoEICT (Journal of Education and ICT). <https://doi.org/10.29100/.v1i1.91>