

Sosialisasi Manajemen Keamanan Siber di SMPN 2 Mojorembun Nganjuk

Fendy Bayu Firmansyah^{*1}, Imam Thoib², Nafis Sururi³, Beda Puspita Candra⁴, Danang Satya Nugraha⁵, Nicky Dwi Kurnia⁶

^{1,2,3,4,5} Program Studi Sistem Informasi, Institut Teknologi Mojokari, Nganjuk, Indonesia

⁶ Program Studi Pendidikan Teknologi Informasi, Institut Teknologi Mojokari, Nganjuk, Indonesia

*e-mail: fendy@itmnganjuk.ac.id¹, ithoib@itmnganjuk.ac.id², nafissururi@itmnganjuk.ac.id³, bedapuspita@itmnganjuk.ac.id⁴, danangsatyan@itmnganjuk.ac.id⁵, nickydwi@itmnganjuk.ac.id⁶,

Nomor Handphone Untuk keperluan koordinasi : 082244006131

Abstrak

Era digitalisasi membawa kemajuan dalam akses informasi dan pembelajaran, namun sekaligus menghadirkan ancaman keamanan siber yang semakin kompleks di lingkungan pendidikan. Survei awal terhadap siswa SMPN 2 Mojorembun Nganjuk menunjukkan bahwa sebagian besar siswa memiliki tingkat pemahaman yang sangat rendah terhadap konsep dasar keamanan siber, mulai dari penggunaan password yang lemah hingga ketidaktahuan terhadap praktik phishing dan pencurian data pribadi. Kondisi ini menjadi latar belakang utama pelaksanaan kegiatan pengabdian masyarakat yang bertujuan untuk meningkatkan kesadaran dan pengetahuan siswa serta guru tentang manajemen keamanan siber. Kegiatan pengabdian dilaksanakan pada tanggal 28 Agustus 2025 di SMPN 2 Mojorembun Nganjuk dengan dihadiri oleh 310 peserta. Metode yang digunakan meliputi sosialisasi materi keamanan siber secara tatap muka dan sesi diskusi interaktif berupa tanya jawab langsung antara pemateri dan peserta. Hasil kegiatan menunjukkan bahwa peserta antusias dalam mengikuti program dan memperoleh pengetahuan baru mengenai bahaya kejahatan siber serta cara pencegahannya. Namun, hasil diskusi juga mengungkapkan masih rendahnya pemahaman siswa tentang etika digital dan perlindungan data pribadi di media sosial. Kegiatan ini diharapkan menjadi langkah awal pembangunan budaya keamanan siber yang berkelanjutan di sekolah, dan perlu ditindaklanjuti dengan program pendampingan rutin dari guru dan orang tua.

Kata kunci: Sosialisasi, Manajemen, Keamanan Siber

Abstract

The digitalization era has brought advances in access to information and learning, yet it has also introduced increasingly complex cybersecurity threats in educational environments. A preliminary survey of students at SMPN 2 Mojorembun Nganjuk revealed that most students have a very low understanding of basic cybersecurity concepts, ranging from the use of weak passwords to a lack of awareness regarding phishing and personal data theft. This condition became the primary background for the implementation of a community service program aimed at improving the awareness and knowledge of students and teachers regarding cybersecurity management. The community service activity was carried out on August 28, 2025, at SMPN 2 Mojorembun Nganjuk and was attended by 310 participants. The methods employed included face-to-face cybersecurity socialization and an interactive discussion session consisting of direct question-and-answer exchanges between the presenters and participants. The results showed that participants were enthusiastic in following the program and gained new knowledge about the dangers of cybercrime and how to prevent it. However, the discussion also revealed that students still have a low understanding of digital ethics and the protection of personal data on social media. This activity is hoped to serve as an initial step toward building a sustainable cybersecurity culture in the school and needs to be followed up with regular mentoring programs from teachers and parents.

Keywords: Socialization, Management, Cybersecurity

1. PENDAHULUAN

Era digitalisasi telah mengubah lanskap pendidikan di Indonesia secara mendasar. Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi (Kemendikbudristek) melaporkan bahwa pada tahun 2024, sebanyak 94,3% sekolah menengah pertama di Indonesia telah terhubung dengan internet, meningkat signifikan dari 67,2% pada tahun 2020. Transformasi digital ini membawa dampak positif dalam meningkatkan akses informasi dan kualitas

pembelajaran, namun di sisi lain menimbulkan tantangan baru berupa ancaman keamanan siber yang semakin kompleks [1].

SMPN 2 Mojorembun merupakan salah satu institusi pendidikan negeri yang berlokasi di Kecamatan Mojorembun, Kabupaten Nganjuk, Jawa Timur. Sekolah ini memiliki 24 rombongan belajar dengan total 756 siswa dan 48 tenaga pendidik serta kependidikan pada tahun ajaran 2024/2025. Sebagai sekolah yang telah mengimplementasikan program digitalisasi pembelajaran sejak tahun 2022, SMPN 2 Mojorembun telah dilengkapi dengan 42 unit komputer di laboratorium komputer, jaringan wifi yang mencakup seluruh area sekolah, dan platform pembelajaran digital yang digunakan oleh 100% siswa dan guru.

Kabupaten Nganjuk sendiri merupakan daerah dengan potensi ekonomi yang terus berkembang, dengan sektor pertanian sebagai tulang punggung ekonomi yang menyumbang 32,4% dari PDRB kabupaten. Dari aspek sosial, tingkat literasi digital masyarakat Nganjuk masih dalam tahap pengembangan, dengan penetrasi internet di kalangan pelajar mencapai 78,6%, namun pemahaman tentang keamanan siber masih tergolong rendah. Kondisi geografis Kecamatan Mojorembun yang terletak di wilayah dataran dengan akses infrastruktur yang memadai menjadikan sekolah ini memiliki potensi besar dalam pengembangan pendidikan berbasis teknologi.

Namun, survei awal yang dilakukan pada Oktober 2025 terhadap 100 siswa SMPN 2 Mojorembun menunjukkan fakta yang mengkhawatirkan: 78% siswa tidak memahami konsep dasar keamanan siber, 65% siswa menggunakan password yang sama untuk berbagai akun, dan 82% siswa pernah mengklik tautan mencurigakan tanpa verifikasi. Lebih lanjut, 89% siswa tidak mengetahui cara melindungi data pribadi di media sosial, dan 71% siswa tidak memiliki kesadaran tentang bahaya phishing dan malware. Data ini sejalan bahwa Indonesia menempati peringkat kedua di Asia Tenggara dalam hal serangan siber terhadap institusi pendidikan, dengan peningkatan 43% dibandingkan tahun sebelumnya.

Keamanan siber (cybersecurity) didefinisikan sebagai praktik melindungi sistem, jaringan, dan program dari serangan digital yang bertujuan mengakses, mengubah, atau menghancurkan informasi sensitif [2]. Dalam konteks pendidikan, keamanan siber mencakup perlindungan data siswa, integritas sistem pembelajaran digital, dan keamanan infrastruktur teknologi informasi sekolah [3]. Ancaman siber terhadap institusi pendidikan bukan sekadar isu teknis, melainkan persoalan yang dapat berdampak pada keselamatan siswa, integritas data akademik, dan reputasi institusi.

Sekitar 67% sekolah di Indonesia pernah mengalami insiden keamanan siber dalam bentuk pencurian data, serangan ransomware, atau penyebaran konten tidak pantas [4]. Serangan siber terhadap lembaga pendidikan meningkat sejak pandemi COVID-19, dengan kerugian finansial mencapai miliaran [5]. Ancaman siber yang paling umum dihadapi oleh institusi pendidikan meliputi: (1) phishing melalui email atau pesan instan, (2) malware dan ransomware, (3) pencurian kredensial login, (4) serangan DDoS terhadap sistem pembelajaran online, dan (5) kebocoran data pribadi [6].

Literasi keamanan siber di kalangan pelajar Indonesia masih rendah karena minimnya integrasi materi keamanan siber dalam kurikulum formal [7]. Penelitian mereka menunjukkan bahwa hanya 23% sekolah menengah di Indonesia yang memiliki program khusus tentang keamanan siber. Kondisi ini memperparah kerentanan siswa terhadap berbagai bentuk kejahatan siber seperti cyberbullying, pencurian identitas, dan penipuan online. Pendidikan keamanan siber harus dimulai sejak dini, terutama di tingkat pendidikan menengah, untuk membentuk generasi yang tidak hanya melek digital tetapi juga bertanggung jawab dalam menggunakan teknologi [8].

Keberhasilan program keamanan siber di institusi pendidikan sangat bergantung pada partisipasi aktif seluruh stakeholder, termasuk siswa, guru, orang tua, dan manajemen sekolah [9]. Mereka merekomendasikan implementasi program sosialisasi berkelanjutan dengan metode yang interaktif dan kontekstual agar peserta dapat memahami relevansi keamanan siber dengan kehidupan sehari-hari.

Potensi SMPN 2 Mojorembun sebagai sekolah dengan infrastruktur digital yang memadai perlu diimbangi dengan peningkatan kapasitas sumber daya manusia dalam mengelola keamanan siber. Tenaga pendidik dan siswa sebagai pengguna utama teknologi informasi di sekolah

memerlukan pemahaman komprehensif tentang manajemen keamanan siber untuk memitigasi risiko yang dapat timbul. Kegiatan sosialisasi ini diharapkan dapat menjadi langkah preventif dalam membangun ekosistem digital yang aman di lingkungan SMPN 2 Mojorembun. Dengan meningkatkan kesadaran dan pengetahuan tentang keamanan siber, diharapkan dapat mengurangi risiko insiden keamanan, melindungi data pribadi siswa dan guru, serta menciptakan budaya digital yang sehat dan bertanggung jawab.

Berdasarkan latar belakang yang telah dipaparkan, rumusan masalah dalam kegiatan pengabdian masyarakat ini adalah : 1. Bagaimana tingkat pemahaman siswa dan guru SMPN 2 Mojorembun tentang konsep dasar keamanan siber dan ancaman-ancaman yang ada di dunia digital?, 2. Bagaimana meningkatkan kesadaran dan keterampilan praktis siswa dan guru dalam menerapkan prinsip-prinsip keamanan siber dalam aktivitas sehari-hari?, 3. Bagaimana membangun budaya keamanan siber yang berkelanjutan di lingkungan sekolah untuk mencegah insiden keamanan di masa mendatang?

Kegiatan pengabdian kepada masyarakat ini bertujuan untuk: 1. Untuk mengetahui tingkat pemahaman siswa dan guru SMPN 2 Mojorembun tentang konsep dasar keamanan siber dan ancaman-ancaman yang ada di dunia digital, 2. Untuk meningkatkan kesadaran dan keterampilan praktis siswa dan guru dalam menerapkan prinsip-prinsip keamanan siber dalam aktivitas sehari-hari, 3. Untuk membangun budaya keamanan siber yang berkelanjutan di lingkungan sekolah untuk mencegah insiden keamanan di masa mendatang

2. METODE

Lokasi Kegiatan Pengabdian masyarakat ini berada di SMPN 2 Mojorembun Nganjuk. Pengabdian dilaksanakan pada tanggal 28 Agustus 2025. Program pengabdian masyarakat ini terdapat dua metode pelaksanaan yang dilakukan, yaitu sosialisasi dan diskusi. Tim menilai bahwa dua metode ini sangat efektif karena dapat secara langsung berinteraksi dengan siswa SMPN 2 Mojorembun Nganjuk. 1.) Sosialisasi, metode ini kami lakukan dengan cara memberikan sosialisasi kepada siswa SMPN 2 Mojorembun mengenai pentingnya keamanan siber dan ancaman-ancaman yang ada di era digital saat ini. Selain itu cara meminimalisir adanya kejahatan siber serta manfaat, tujuan dan keuntungan dari pentingnya penerapan keamanan siber dan Materi yang disampaikan hendaknya dapat memberikan peningkatan pengetahuan dan pemahaman bagi para siswa untuk selanjutnya dapat diterapkan oleh siswa dalam keseharian di era digital terutama dalam menggunakan sosial media. 2.) Diskusi, dengan melakukan proses tanya jawab antara pemateri dengan peserta. Diskusi dilakukan dengan tujuan dapat berinteraksi timbal balik secara langsung antara pemateri dengan peserta, karena ini dinilai lebih efektif dalam melakukan pendekatan dengan peserta. Selain itu, diskusi juga dapat mengkaji permasalahan-permasalahan yang sedang dihadapi oleh peserta dengan proses tanya jawab. 3.) Partisipasi siswa untuk melaksanakan program guna tercapai tujuan yang diinginkan, maka dalam realisasi program tersebut diharapkan mitra dapat berpartisipasi dengan kegiatan sebagai berikut: a. Menjadi peserta berupa: menerima teori, konsep, diskusi, tanya jawab serta hal – hal lain yang diberikan selama proses kegiatan berlangsung. b. Menyediakan tempat dan fasilitas yang dibutuhkan selama proses kegiatan berjalan.

3. HASIL DAN PEMBAHASAN

Kegiatan pengabdian kepada masyarakat ini dilaksanakan melalui sistem tatap muka dengan mengunjungi SMPN 2 Mojorembun Nganjuk secara langsung. Pelaksanaannya dilakukan selama 1 hari pada tanggal 28 Agustus 2025 yang dihadiri oleh 310 orang peserta, yang terdiri dari seluruh siswa SMPN 2 Mojorembun Nganjuk. Pelaksanaan dengan metode tatap muka ini memudahkan penyampaian ilmu dan pengalaman. Tahap awal pengabdian masyarakat dilakukan dengan melakukan survei sekolah yang kami tuju untuk melakukan pengabdian. Selain itu, tim juga mengantarkan surat pengantar kepada mitra sekolah SMPN 2 Mojorembun Nganjuk,

dilanjutkan dengan konfirmasi persetujuan bahwa akan dilakukannya pengabdian di sekolah tersebut. Pada pelaksanaan pengabdian masyarakat tersebut kami mensosialisasikan tentang keamanan siber, contoh kejahatan siber serta pencegahannya.

Hasil tanya jawab menunjukkan kondisi awal yang mengkhawatirkan terkait tingkat pengetahuan dan kesadaran keamanan siber di kalangan siswa SMPN 2 Mojorembun. Hasil tanya jawab lebih mengkhawatirkan terlihat saat banyak siswa menggunakan password yang sama untuk berbagai akun, kemudian tidak pernah mengubah password secara berkala dan menggunakan password yang mudah ditebak seperti tanggal lahir atau nama sendiri.

Selain itu banyak siswa yang mengaku sering mendapatkan paparan kejahatan siber. Rincian jenis kejahatan siber yang dialami antara lain: link penipuan dan phishing, spam judi online serta penipuan transaksi online. Banyak siswa melaporkan menerima link penipuan melalui whatsapp. Link tersebut berupa iming-iming hadiah gratis, kupon diskon palsu atau undangan untuk mengikuti kuis berhadiah. Sedangkan spam judi online yang diterima siswa umumnya dating juga melalui whatsapp serta telegram. Peasn tersebut sering menggunakan Bahasa yang menarik perhatian remaja dengan iming-iming keuntungan cepat atau bonus besar.

Potensi besar terjadinya kejahatan siber semakin besar seiring semakin besarnya konsumsi digital oleh para siswa. Media sosial berupa Instagram, tiktok dan whatsapp menjadi konsumsi terbanyak oleh siswa. Ditambah konsumsi tontonan video online melalui aplikasi seperti youtube dan aplikasi streaming lainnya. Dari sisi konten, banyak siswa yang kemudian melihat konten tidak sesuai dengan usia mereka, termasuk kekerasan maupun konten dewasa.

Di sisi lain, tim sebisa mungkin memberikan edukasi berupa meminimalisir penggunaan gadget oleh para siswa. Langkah berikutnya tim memberikan edukasi pentingnya menggunakan variasi pada password yang digunakan oleh siswa. Variasi dapat berupa penggabungan huruf dan angka, serta penambahan karakter tertentu untuk mempersulit password yang mudah ditebak.



Gambar 1. Dokumentasi tim dengan OSIS SMPN 2 Mojorembun

Berdasarkan hasil tanya jawab dengan siswa SMPN 2 Mojorembun, mengungkapkan bahwa pemahaman siswa tentang etika digital dan penggunaan media sosial yang bertanggung jawab masih sangat rendah. siswa tidak mengetahui konsep digital footprint dan dampak jangka panjang dari apa yang mereka posting di media sosial. Mereka tidak menyadari bahwa konten yang mereka bagikan hari ini dapat memengaruhi reputasi mereka di masa depan, termasuk dalam konteks pendidikan lanjut atau pekerjaan.



Gambar 2. Dokumentasi tim sosialisasi dengan siswa SMPN 2 Mojorembun

Berdasarkan tanya jawab yang dilakukan juga didapatkan banyak siswa belum memahami pentingnya melindungi informasi pribadi di media sosial. Mereka mudah membagikan informasi seperti alamat rumah, nomor telepon, nama sekolah, dan rutinitas harian. Selain itu, siswa tidak memahami bahwa membagikan foto atau video orang lain tanpa izin adalah pelanggaran privasi dan dapat memiliki konsekuensi hukum.

4. KESIMPULAN

Berdasarkan hasil sosialisasi yang telah dilakukan dapat disimpulkan masih minimnya informasi terkait bahaya kejahatan siber yang diterima oleh siswa. Banyak siswa yang belum dibekali pemahaman resiko yang dapat terjadi di era digitalisasi saat ini. Diperlukan pendampingan oleh guru maupun orang tua agar pada siswa tidak terdampak oleh kejahatan siber.

DAFTAR PUSTAKA

- [1] E. Ahyani and E. M. Dhuhan, "Transformasi digital dalam manajemen perkantoran pendidikan: Sebuah kajian literatur," *J. Vision. Penelit. Dan Pengemb. Dibidang Adm. Pendidik.*, vol. 12, no. 1, pp. 205–215, 2024.
- [2] D. Budiyanto and M. Maburi, "Pentingnya Keamanan Siber Dalam Era Digital:: Tinjauan Global Dan Kondisi Di Indonesia," in *Prosiding Seminar Nasional Sains dan Teknologi" SainTek"*, 2025, pp. 981–994.
- [3] S. N. Coalliani, A. E. K. Tejawati, L. Komariyah, and Y. Dwiyono, "Evaluasi Keamanan Dan Manajemen Data Pada Sistem Informasi Sekolah Di Era Transformasi Digital," *Mudir J. Manaj. Pendidik.*, vol. 8, no. 1, pp. 471–479, 2026.
- [4] F. I. Febriansyah and M. Sh, *Cybercrime: Kejahatan di Balik Layar Digital*. Najaha, 2025.
- [5] F. N. Latifah, I. Mawardi, and B. Wardhana, "Threat of Data Theft (Phishing) Amid Trends in Fintech Users During the Covid-19 Pandemic (Study Phishing In Indonesia)," *Perisai Islam. Bank. Financ. J.*, vol. 6, no. 1, pp. 74–86, 2022.
- [6] S. Santoso, A. Oktarino, T. Tugiman, and A. D. A. Wicaksono, *Buku Ajar Cyber Security*. PT. Sonpedia Publishing Indonesia, 2025.
- [7] H. Agung, "Efektivitas Edukasi Cybersecurity dalam Meningkatkan Pengetahuan Siswa tentang Ancaman Digital pada Siswa Menengah Atas," *J. Ilmu Komput.*, vol. 5, no. 2, pp. 104–113, 2025.
- [8] M. Arisanty, Y. Riady, S. A. A. Kharis, S. M. Permatasari, and S. Sukatmi, "CERDAS DAN AMAN BERMEDIA DIGITAL: PENINGKATAN KESADARAN KEAMANAN SIBER DI ERA HOAKS DAN PHISHING," *J. Pengabd. Kpd. Masy. Patikala*, vol. 4, no. 4, pp. 1407–1418, 2025.
- [9] U. Al Huda, "Peran Stakeholder dalam Meningkatkan Manajemen Mutu Pendidikan," *Pijar Pelita J. Early Child. Educ. Early Child. Islam. Educ.*, vol. 1, no. 2, pp. 182–194, 2025.