JURNAL TERAS PENGABDIAN MASYARAKAT
https://jurnal.tdinus.com/index.php/jtpm

Pelatihan Keamanan Siber pada Sistem Operasi Windows dan Linux bagi Siswa MTs Gintangan Blimbingsari

Cybersecurity Training on Windows and Linux Operating Systems for MTs Gintangan Blimbingsari Students

Zaehol Fatah[*1], Mada Tahliya[2]
[1,2]*Universitas Ibrahimy, Situbondo, 68374, Indonesia*

[*]Koresponding Author: madatahliya@gmail.com

INFO ARTIKEL
Riwayat artikel:
Diterima : 16 Mei 2026
Direvisi : 17 Mei 2026
Disetujui : 22 Mei 2026
Tersedia secara online: 01 Juli 2026

E-ISSN: 3090-0964 (Online)

ABSTRAK

Tujuan pelatihan pengaturan keamanan sistem operasi Windows dan Linux bagi siswa MTs Gintangan Blimbingsari adalah untuk meningkatkan pemahaman serta keterampilan siswa dalam menghadapi ancaman siber di era digital. Pelatihan dilaksanakan melalui metode praktik langsung yang meliputi penyampaian materi, simulasi ancaman siber, dan praktik konfigurasi keamanan sistem operasi. Materi yang diberikan meliputi pengaturan firewall, penggunaan antivirus, pembaruan sistem, pengaturan hak akses pengguna, keamanan password, serta pengenalan ancaman siber seperti malware, phishing, dan ransomware. Hasil pelatihan menunjukkan adanya peningkatan kemampuan siswa dalam memahami dasar-dasar keamanan siber dan melakukan pengaturan keamanan sederhana pada komputer. Siswa mulai memahami pentingnya menjaga keamanan data pribadi, menggunakan password yang kuat, serta berhati-hati terhadap ancaman digital yang dapat menyerang perangkat komputer maupun akun pribadi. Metode praktik langsung dan pendampingan intensif terbukti efektif dalam meningkatkan keterampilan teknis serta kesadaran siswa terhadap pentingnya keamanan digital. Meskipun terdapat beberapa kendala seperti keterbatasan perangkat komputer dan minimnya pengalaman siswa dalam menggunakan Linux, secara keseluruhan pelatihan ini berhasil meningkatkan literasi digital serta kesiapan siswa dalam menghadapi ancaman siber.

Kata kunci: keamanan siber, sistem operasi Windows, sistem operasi Linux, pelatihan,

ABSTRACT

The objective of the Windows and Linux security configuration training for students of MTs Gintangan Blimbingsari is to improve students' understanding and skills in dealing with cyber threats in the digital era. The training was conducted using a hands-on practice method through several stages, namely coordination, material preparation, theoretical instruction, cyber threat simulation, and direct practice in configuring security settings on Windows and Linux operating systems. The materials covered firewall configuration, antivirus usage, system updates, user access management, password security, and an introduction to cyber threats such as malware, phishing, and ransomware. The results of the training indicate an improvement in students' ability to understand basic cybersecurity concepts and perform simple computer security configurations. Students began to understand the importance of protecting personal data, using strong passwords, and being cautious of digital threats that could attack computer devices or personal accounts. The

DOI: 10.64479/jtpm.v2i2.74

hands-on practice method and intensive mentoring proved effective in improving students' technical skills and awareness of digital security. Although there were several obstacles such as limited computer equipment and students' lack of experience in using Linux, overall the training successfully improved students' digital literacy and readiness in facing cyber threats.

Keyword: *cyber security, Windows operating system, Linux operating system, training.*

1. Pendahuluan

Kemajuan teknologi komputer memberikan pengaruh signifikan dalam berbagai bidang kehidupan, terutama melalui peran sistem operasi sebagai komponen vital dalam pengoperasian perangkat komputer(Ahmad Fahimurridho, Muhammad Irham Syakirin, 2025). dunia siber yang semakin pesat menuntut peningkatan kesiapan dan kesadaran keamanan digital sejak dini. Setiap orang menggunakan gadget untuk berkomunikasi dan mengakses berbagai informasi setiap hari (Rafrastara et al., 2024). Dalam dunia teknologi informasi dan komunikasi pada era digital memberikan pengaruh besar terhadap dunia pendidikan. Penggunaan komputer, internet, dan perangkat digital saat ini telah menjadi bagian penting dalam kegiatan belajar mengajar di sekolah(Wijayanto et al., 2026). Siswa tidak hanya dituntut untuk mampu menggunakan teknologi, tetapi juga harus memahami cara menjaga keamanan perangkat dan data pribadi agar terhindar dari ancaman siber. Ancaman siber seperti virus, malware, phishing, ransomware, dan pencurian data dapat menyerang siapa saja, termasuk siswa yang aktif menggunakan internet dan media digital dalam kehidupan sehari-hari(Godzali et al., 2025). Literasi digital merupakan Transformasi digital dalam institusi pendidikan telah meningkatkan ketergantungan pada teknologi informasi, termasuk dalam manajemen data, administrasi, dan proses pembelajaran daring. Namun, perkembangan ini juga memunculkan risiko signifikan terkait keamanan data dan ancaman siber yang mampu mengganggu operasional pendidikan secara menyeluruh(Septia, 2025). Selain kemampuan menggunakan teknologi, siswa juga perlu memahami pentingnya keamanan digital untuk melindungi data dan perangkat yang digunakan. Keamanan siber menjadi salah satu aspek penting dalam literasi digital karena berkaitan dengan perlindungan sistem komputer, jaringan, serta informasi dari berbagai ancaman yang dapat merugikan pengguna(Hermawan, Dani, 2025).

Sistem operasi Windows dan Linux merupakan dua sistem operasi yang banyak digunakan dalam dunia pendidikan maupun pekerjaan. Windows dikenal sebagai sistem operasi yang mudah digunakan dan banyak dipakai oleh pengguna umum namun Sistem operasi Windows menjadi salah satu target utama bagi para penyerang *cyber* karena popularitasnya di kalangan pengguna komputer (Sari et al., 2024), sedangkan *Linux* dikenal memiliki Keamanan siber (Hendrawansyah, Andi Irfan, 2025)terbaik sebagai distribusi Linux yang isu krusialnya dalam era digital saat ini, dengan meningkatnya kompleksitas dan frekuensi serangan yang menargetkan infrastruktur informasi (Prasetiyo et al., 2024). Dibalik maraknya penyebaran *malware*, tentu para ahli dibilang IT membuat sebuah sistem keamanan yang kuat untuk meminimalisir risiko terkena malware(Fajar & Lestari, 2025). Pada sistem keamanan windows, sudah banyak perangkat lunak yang diciptakan untuk mencegah ancaman malware, diantaranya Windows defender yang merupakan induk atau inti dari sistem keamanan windows, virus & *threat protection*, *real-time protection, firewall & network protection, account protection* (Rahman et al., 2024). respon yang dapat dilakukan yaitu meningkatkan intensitas dan kompleksitas serangan siber yang berpotensi mengganggu integritas, kerahasiaan, dan ketersediaan data pada berbagai sistem informasi modern (Misni, Misni, 2026). serangan siber juga yang berpotensi mengganggu integritas, kerahasiaan, dan ketersediaan data pada berbagai sistem informasi modern(Misni, Misni, 2026).

Oleh karena itu, pemahaman mengenai pengaturan keamanan pada kedua sistem operasi tersebut sangat penting untuk dikenalkan kepada siswa sejak dini. Namun pada kenyataannya, masih banyak siswa yang belum memahami cara mengamankan perangkat komputer yang digunakan. Sebagian siswa masih terdapat kekurangan dalam penerapan praktik terbaik, seperti penggunaan kata sandi yang kuat dan verifikasi keaslian email, jarang melakukan pembaruan sistem, serta belum memahami pentingnya penggunaan antivirus dan firewall(Prasetyo et al., 2024). Selain itu, dalam Program pelatihan keamanan siber kolaboratif bagi siswa-siswi masih banyak siswa yang belum mengetahui cara mengenali ancaman seperti email phishing, tautan berbahaya, maupun aplikasi yang berpotensi mengandung malware(Ahmadi et al., 2025). Kondisi tersebut

juga ditemukan pada siswa MTs Gintangan Blimbingsari, di mana sebagian besar siswa masih memiliki pemahaman yang terbatas mengenai keamanan digital dan pengamanan sistem operasi.

Berdasarkan permasalahan tersebut, diperlukan suatu kegiatan pelatihan yang dapat membantu siswa memahami dasar-dasar keamanan siber serta praktik pengaturan keamanan pada sistem operasi Windows dan Linux. Pelatihan ini bertujuan untuk memberikan pengetahuan dan keterampilan kepada siswa dalam menjaga keamanan perangkat komputer serta meningkatkan kesadaran terhadap ancaman siber yang dapat terjadi dalam kehidupan sehari-hari. Dampak positif dari kegiatan ini tidak hanya dirasakan oleh peserta secara individual, tetapi juga berkontribusi pada peningkatan budaya keamanan siber di lingkungan sekolah (Solehuddin et al., 2025). Melalui pelatihan ini, siswa diharapkan mampu memahami pentingnya keamanan digital, mengenali berbagai bentuk ancaman siber, serta mampu melakukan pengaturan keamanan dasar pada sistem operasi Windows dan Linux. Selain itu, pelatihan ini juga diharapkan dapat meningkatkan kesiapan siswa dalam menggunakan teknologi secara aman, bijak, dan bertanggung jawab di era digital.

2. Metode

Evaluasi dilakukan melalui observasi sederhana terhadap pemahaman siswa sebelum dan sesudah pelatihan, di mana siswa diajak untuk belajar sambil mempraktikkan setiap materi yang diberikan secara langsung pada sistem operasi Windows dan Linux(Bahri, 2026). Metode ini dipilih agar siswa tidak hanya memahami teori mengenai keamanan siber, tetapi juga mampu menerapkan pengaturan keamanan dasar pada komputer yang digunakan. Pelatihan ini dilaksanakan di MTs Gintangan Blimbingsari dengan melibatkan semua siswa kelas VII.

Kegiatan diawali dengan koordinasi antara tim pelaksana dengan pihak sekolah untuk menentukan jadwal pelaksanaan serta memastikan kesiapan tempat dan perangkat yang dibutuhkan selama kegiatan berlangsung. Setelah itu, dilakukan pengecekan awal untuk mengetahui tingkat pemahaman siswa mengenai penggunaan komputer dan keamanan digital(Islamey et al., 2025). Hal ini bertujuan agar materi pelatihan dapat disesuaikan dengan kemampuan dasar siswa sehingga proses pembelajaran menjadi lebih efektif dan mudah dipahami.

Sebelum pelatihan dimulai, tim pelaksana menyiapkan beberapa hal, yaitu:

a. Materi pelatihan yang berisi pengenalan keamanan siber, jenis-jenis ancaman siber, pengaturan keamanan pada Windows dan Linux, penggunaan antivirus, firewall, serta keamanan password
b. Menyiapkan perangkat komputer/laptop yang telah terpasang sistem operasi Windows dan Linux untuk kegiatan praktik
c. Menyiapkan contoh simulasi ancaman siber sederhana seperti phishing, malware, dan file berbahaya sebagai bahan pembelajaran siswa
d. Menyiapkan lembar evaluasi dan penilaian untuk mengetahui perkembangan kemampuan siswa setelah mengikuti pelatihan

2.1. Tahap Pertama

Tahap pertama adalah pemberian motivasi kepada siswa mengenai pentingnya menjaga keamanan digital di era perkembangan teknologi informasi. Pada tahap ini siswa dijelaskan mengenai berbagai ancaman siber yang sering terjadi serta dampaknya terhadap keamanan data dan perangkat komputer.

2.2. Tahap Kedua

Tahap kedua adalah penyampaian materi dasar mengenai keamanan sistem operasi Windows dan Linux. Pada tahap ini siswa dikenalkan dengan fitur-fitur keamanan dasar seperti pengaturan firewall, penggunaan antivirus, update sistem, pengaturan hak akses pengguna, serta pentingnya penggunaan password yang kuat dan aman. Penjelasan dilakukan secara langsung menggunakan proyektor sehingga siswa dapat mengikuti langkah-langkah yang dijelaskan oleh tim pelaksana dengan lebih mudah.

2.3. Tahap Ketiga

Tahap ketiga adalah praktik langsung. Siswa diminta untuk mencoba melakukan pengaturan keamanan pada perangkat komputer masing-masing, seperti mengaktifkan firewall Windows, melakukan update sistem operasi Linux, membuat password yang aman, serta melakukan pemindaian antivirus pada komputer. Selama praktik berlangsung, tim pelaksana memberikan bimbingan secara langsung agar siswa dapat memahami setiap langkah pengaturan keamanan dengan baik.

2.4. Tahap Keempat

Tahap keempat adalah simulasi ancaman siber sederhana. Pada tahap ini siswa diberikan contoh bentuk ancaman seperti email phishing, tautan berbahaya, serta file mencurigakan yang dapat mengandung malware. Kegiatan ini bertujuan agar siswa mampu mengenali ancaman siber dan memahami cara menghindarinya saat menggunakan perangkat digital maupun internet.

2.5. Tahap Kelima

Tahap terakhir adalah evaluasi. Tim pelaksana memberikan penilaian terhadap hasil praktik siswa, baik dari segi pemahaman materi maupun kemampuan dalam melakukan pengaturan keamanan pada sistem operasi Windows dan Linux. Dengan adanya evaluasi ini, siswa diharapkan dapat mengetahui kekurangan serta mampu meningkatkan kemampuan dalam menjaga keamanan perangkat dan data pribadi di masa mendatang.

3. Hasil Dan Pembahasan

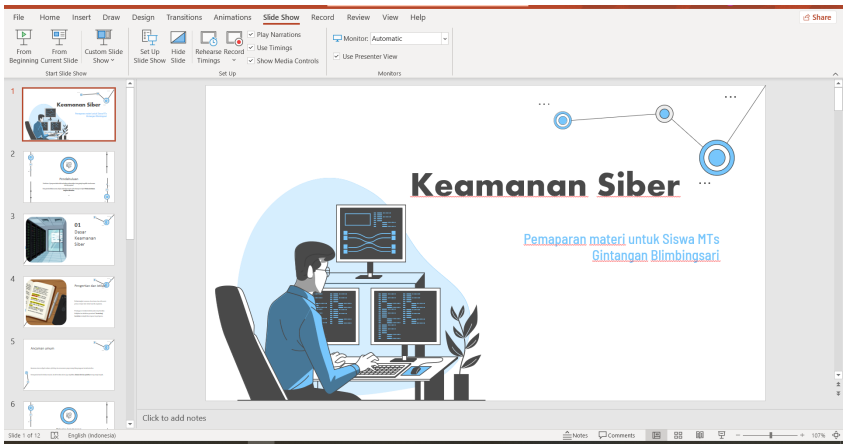
Siswa MTs Gintangan Blimbingsari mengikuti pelatihan pengaturan keamanan pada sistem operasi Windows dan Linux dengan baik dan penuh antusias. Berdasarkan hasil observasi dan evaluasi yang dilakukan oleh tim pelaksana, pelatihan ini memberikan dampak yang cukup signifikan terhadap peningkatan pemahaman siswa mengenai keamanan siber serta kemampuan siswa dalam melakukan pengaturan keamanan dasar pada komputer. Pada awal pelatihan, tim pelaksana melakukan pengujian awal untuk mengetahui tingkat pemahaman siswa mengenai keamanan digital dan penggunaan sistem operasi Windows maupun Linux. Sebagian besar siswa mulai memahami penggunaan firewall, antivirus, dan pentingnya penggunaan password yang kuat setelah mengikuti pelatihan. Berdasarkan hasil pengujian tersebut, sebagian besar siswa masih belum memahami pentingnya pengaturan keamanan komputer dan masih memiliki kebiasaan menggunakan password yang sederhana serta jarang melakukan pembaruan sistem operasi.

Setelah penyampaian materi, siswa mulai dikenalkan dengan konsep dasar keamanan siber serta berbagai jenis ancaman digital yang dapat menyerang perangkat komputer. Materi yang disampaikan meliputi pengenalan malware, ransomware, phishing, penggunaan firewall, antivirus, serta pentingnya melakukan update sistem secara berkala. Penyampaian materi dilakukan menggunakan metode demonstrasi dengan bantuan proyektor sehingga siswa dapat mengikuti setiap langkah pengaturan keamanan secara langsung. Selama proses penyampaian materi, siswa terlihat aktif memperhatikan dan mulai memahami pentingnya menjaga keamanan perangkat serta data pribadi. Selain itu, pelatihan ini juga memberikan pemahaman kepada siswa mengenai pentingnya menjaga keamanan akun dan data pribadi saat menggunakan internet. Siswa diberikan simulasi sederhana mengenai ancaman phishing melalui contoh email palsu dan tautan berbahaya yang sering digunakan untuk mencuri informasi pengguna. Setelah mengikuti simulasi tersebut, siswa mulai memahami ciri-ciri ancaman phishing serta pentingnya berhati-hati saat membuka tautan atau mengunduh file dari internet. Beberapa siswa juga mulai memahami pentingnya penggunaan password yang kuat dengan kombinasi huruf, angka, dan simbol untuk meningkatkan keamanan akun.

Analisis dari pelaksanaan pelatihan menunjukkan bahwa metode praktik langsung yang digunakan terbukti efektif dalam meningkatkan pemahaman siswa mengenai keamanan siber. Siswa dapat langsung mencoba setiap materi yang diberikan sehingga lebih mudah memahami cara kerja pengaturan keamanan pada sistem operasi Windows dan Linux. Selain itu, pelatihan ini juga meningkatkan motivasi dan kesadaran siswa terhadap pentingnya menjaga keamanan digital. Hal ini terlihat dari antusiasme siswa selama kegiatan berlangsung, di mana siswa aktif mencoba fitur-fitur keamanan yang dijelaskan serta tidak ragu bertanya ketika mengalami kesulitan.

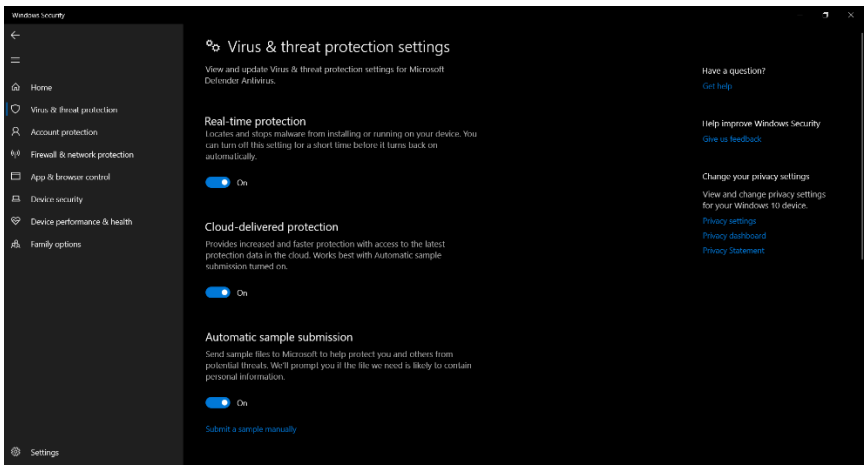
Meskipun pelatihan berjalan dengan baik, terdapat beberapa kendala yang dialami selama pelaksanaan kegiatan. Salah satu kendala utama adalah keterbatasan jumlah perangkat komputer/laptop sehingga beberapa siswa harus menggunakan perangkat secara bergantian saat praktik berlangsung. Selain itu, sebagian siswa masih belum terbiasa menggunakan sistem operasi Linux sehingga membutuhkan pendampingan yang lebih intensif dibandingkan penggunaan Windows. Namun demikian, kendala tersebut dapat diatasi oleh tim pelaksana melalui pendampingan secara langsung kepada siswa yang mengalami kesulitan. Pelatihan pengaturan keamanan pada sistem operasi Windows dan Linux ini berhasil meningkatkan kemampuan siswa

dalam memahami ancaman siber, melakukan pengaturan keamanan dasar, serta meningkatkan kesadaran terhadap pentingnya menjaga keamanan data dan perangkat digital. Pelatihan ini sangat bermanfaat dalam mendukung peningkatan literasi digital siswa di lingkungan sekolah. Oleh karena itu, pelatihan serupa dengan materi yang lebih mendalam sangat disarankan untuk dilaksanakan secara berkelanjutan agar kemampuan siswa dalam menghadapi ancaman siber semakin berkembang di masa mendatang.



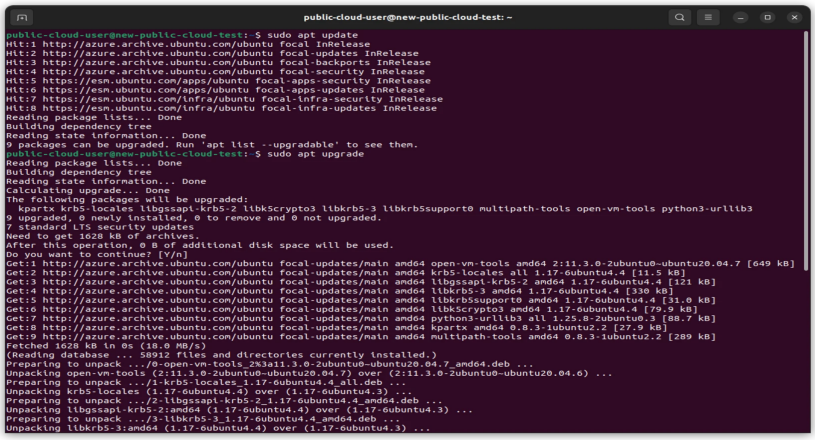
Gambar 3.1. Penyampaian materi keamanan siber kepada siswa

Gambar 3.1 menunjukkan proses penyampaian materi mengenai dasar-dasar keamanan siber oleh tim pelaksana kepada siswa. Materi disampaikan menggunakan laptop agar siswa dapat memahami penjelasan mengenai ancaman siber serta pengaturan keamanan pada Windows dan Linux dengan lebih mudah.



Gambar 3.2. Praktik pengaturan keamanan Windows

Gambar 3.2 menunjukkan kegiatan praktik siswa dalam melakukan pengaturan keamanan pada sistem operasi Windows. Pada tahap ini siswa mencoba mengaktifkan firewall, melakukan update sistem, serta menggunakan antivirus untuk melakukan pemindaian perangkat komputer.



Gambar 3.3. Praktik penggunaan Linux

Gambar 3.3 menunjukkan kegiatan siswa saat mempraktikkan penggunaan sistem operasi Linux. Siswa dikenalkan dengan penggunaan terminal sederhana untuk melakukan update sistem dan pengaturan keamanan dasar pada Linux.

Gambar 3.4. Simulasi ancaman siber

Gambar 3.4 memperlihatkan simulasi ancaman siber sederhana yang diberikan kepada siswa, seperti contoh email phishing dan tautan berbahaya. Kegiatan ini bertujuan untuk melatih siswa agar lebih waspada terhadap ancaman digital saat menggunakan internet.

Gambar 3.5. Dokumentasi kegiatan pelatihan

Gambar 3.5 menunjukkan dokumentasi kegiatan pelatihan berupa foto bersama antara pelaksana dan siswa setelah kegiatan selesai dilaksanakan. Dokumentasi ini menjadi bukti bahwa kegiatan pelatihan berjalan dengan baik dan diikuti secara aktif oleh seluruh peserta.

Gambar 3.6. Dokumentasi kegiatan

Gambar 3.6 menunjukkan dokumentasi tambahan kegiatan pelatihan yang telah dilaksanakan. Dokumentasi ini menggambarkan suasana kebersamaan dan partisipasi siswa selama mengikuti pelatihan presentasi PowerPoint.

4. Kesimpulan

Berdasarkan hasil pelatihan pengaturan keamanan pada sistem operasi Windows dan Linux yang dilaksanakan di MTs Gintangan Blimbingsari, dapat disimpulkan bahwa pelatihan ini berhasil meningkatkan pemahaman dan keterampilan siswa dalam menghadapi ancaman siber. Sebelum pelatihan dilaksanakan, sebagian besar siswa masih memiliki pemahaman yang terbatas mengenai keamanan digital dan belum mengetahui cara melakukan pengaturan keamanan pada perangkat komputer. Namun setelah mengikuti pelatihan, siswa mulai mampu memahami jenis-jenis ancaman siber, pentingnya menjaga keamanan data pribadi, serta cara melakukan pengaturan keamanan dasar pada sistem operasi Windows dan Linux. Pelatihan

serupa disarankan untuk dilaksanakan secara berkala guna meningkatkan kesiapan siswa dalam menghadapi ancaman siber di era digital.

5. Ucapan terima kasih

Penulis mengucapkan terima kasih kepada MTs Gintangan Blimbingsari, khususnya kepada Kepala Sekolah dan para guru yang telah memberikan izin serta dukungan sehingga kegiatan pelatihan ini dapat terlaksana dengan baik. Ucapan terima kasih juga disampaikan kepada seluruh siswa yang telah berpartisipasi aktif dan mengikuti kegiatan pelatihan dengan penuh antusias. Selain itu, penulis juga mengucapkan terima kasih kepada semua pihak yang telah membantu dan mendukung pelaksanaan kegiatan ini sehingga pelatihan dapat berjalan sesuai dengan tujuan yang diharapkan.

Referensi

Ahmad Fahimurridho, Muhammad Irham Syakirin, & Z. F. (2025). Pemahaman Dan Manfaat Dari Sistem Operasi Dalam Meningkatkan Kinerja Komputer : Studi Kasus Di Smk Mansyaul Huda Tegaldlimo Banyuwangi Pendahuluan Smk Mansyaul Huda. *Nuras : Jurnal Pengabdian Kepada Masyarakat*, *5*(3), 141–148.

Ahmadi, A., Akbar, T., Putra, H. M., Ahmad, R., & Dewi, I. K. (2025). Pelatihan Keamanan Siber Kolaboratif Bagi Siswa-Siswi Sma / Ma Guna Menumbuhkan Budaya Sadar Keamanan Informasi Sejak Dini. *J U R N A L S O L M A*, *14*(3), 5467–5475.

Bahri, S. (2026). Pendekatan Preventive Security Dalam Optimalisasi Keamanan Sistem Operasi Windows. *Remik: Riset Dan E-Jurnal Manajemen Informatika Komputer*, *10*, 376–384.

Fajar, R. Al, & Lestari, A. (2025). Analisis Perbandingan Sistem Operasi Windows 11 Dan Linux Ubuntu Menggunakan Metode Studi Literatur (Studi Kasus : Kinerja Sistem , Keamanan Dan Biaya). *Jurnal Bitwise*, *1*(2), 74–82.

Godzali, G. Al, Athallah, R. I., & Rivalni, E. (2025). Evaluasi Keamanan Autentikasi Pengguna Pada Sistem Operasi Windows Dan Linux. *Neptunus: Jurnal Ilmu Komputer Dan Teknologi Informasi*, *3*(1), 31–40.

Hendrawansyah, Andi Irfan, C. (2025). Pelatihan Instalasi Sistem Operasi Berbasis Windows 10 Bagi Dosen Dan Mahasiswa Di Kabupaten Soppeng. *Pendiamka: Jurnal Pengabdian Masyarakat Amika*, *2*(1), 27–36.

Hermawan, Dani, A. H. A. (2025). Keamanan Kernel Pada Sistem Operasi Modern. *Jati (Jurnal Mahasiswa Teknik Informatika)*, *9*(2), 2067–2069.

Islamey, A., Pamungkas, A. M., Wijaya, A., & Saputra, D. D. (2025). Pelatihan Sistem Operasi Windows Bagi Siswa Untuk Meningkatkan Keterampilan Teknologi Informasi. *Jriin : Jurnal Riset Informatika Dan Inovasi*, *2*(11), 2079–2083.

Misni, Misni, A. C. (2026). Pelatihan Dasar Keamanan Siber Untuk Mengelola Resiko Digital Di Pusat Data Dan Informasi Pangan – Badan Pangan Nasional Ri. *Jurnal Abdimas*, *5*(3), 59–68.

Prasetiyo, S. M., Ulu, S. F., Simatupang, H., & Kerwinto, J. (2024). Keamanan Siber Pada Distribusi Linux : Studi Kasus Dan Solusi Efektif. *(Biikma)Buletin Ilmiah Ilmu Komputer Dan Multimedia*, *2*(1), 72–76.

Prasetyo, H., Ibrahim, I., Milhan, M., & Moelyana, H. (2024). Keamanan Cyber Dalam Menghadapi Tantangan Ancaman Masa Depan Di Universitas Bhayangkara Jakarta Raya. *Journal Of Information And Information Security (Jiforty)*, *5*(2), 235–244.

Rafrastara, F. A., Ghozi, W., & Sani, R. R. (2024). Pelatihan Basic Cyber Security Untuk Siswa Ma / Sederajat Di Kabupaten Batang. *Jurnal Abdimasku*, *7*(3), 1058–1065.

Rahman, R., Ilyas, M. F., & Yusuf, M. A. (2024). Strategi Pengembangan Sistem Operasi Windows Untuk Memperkuat Proteksi Windows Terhadap Ancaman Malaware. *Jurnal Sistem Informasi Dan Ilmu Komputer*, *2*(2), 113–121.

Sari, S., Fadil, A., Informasi, J. S., & Habibie, I. T. B. J. (2024). Strategi Pengembangan Sistem Keamanan Terpadu Untuk Melindungi Sistem Operasi Windows Dari Ancaman Cyber. *Router : Jurnal Teknik Informatika Dan Terapan*, *2*(3), 122–136.

Septia. (2025). Kesiapan Organisasi Pendidikan Terhadap Risiko Teknologi Dan Keamanan Data. *Jurnal Media Akademik (Jma)*, *3*(12).

Solehuddin, M., Awaludin, D. T., Marasaoly, S., Rijal, S., & Milasari, L. A. (2025). Pelatihan Dasar Literasi Keamanan Siber Bagi Guru Dan Pelajar Dalam Meningkatkan Kesadaran Keamanan Data Pribadi. *Jipiti: Jurnal Pengabdian Kepada Masyarakat*, *2*(1), 27–32.

Wijayanto, A., , Muhammad Fahmi Abdillah , Aqilah Aulya Maulidah, A. M., , Ghina Nur Madina, A. W., Gerungan, R. A. C., Najha, N., Ahsani, A. Z., Ramadhan, S. M., Danu, R., Triwahyudi, & Zistafa, E. R.

(2026). Peningkatan Kesadaran Keamanan Siber Siswa Smk Melalui Pelatihan Dan Simulasi Serangan Dalam Lingkungan Virtual. *Jurnal Pengabdian Kepada Masyarakat*, *3*(3), 276–283.