

Pelatihan Dasar Literasi Keamanan Siber bagi Guru dan Pelajar dalam Meningkatkan Kesadaran Keamanan Data Pribadi

Moh. Solehuddin¹, Dipa Teruna Awaludin², Salha Marasaoly³, Syamsu Rijal⁴, Lisa Astria Milasari⁵

¹ STAI Ar-Rosyid Surabaya, ² Universitas Nasional, ³ Universitas Khairun, ⁴ Universitas Negeri Makassar,

⁵ Universitas 17 Agustus 1945 Samarinda

e-mail: msolehuddin28@gmail.com¹, dipateruna@civitas.unas.ac.id², salha@unkhair.ac.id³,
syamsurijalasnur@unm.ac.id⁴, lisaastria71@gmail.com⁵

Abstrak

Pengabdian kepada masyarakat ini bertujuan untuk meningkatkan kesadaran dan pemahaman mengenai literasi keamanan siber (*cybersecurity*) bagi guru dan pelajar dalam upaya melindungi data pribadi di era digital. Kegiatan ini dilaksanakan melalui pelatihan dasar yang mencakup konsep keamanan siber, identifikasi ancaman siber, serta praktik pencegahan dan penanganan risiko keamanan data. Metode pelaksanaan meliputi penyampaian materi, diskusi interaktif, dan simulasi kasus nyata yang relevan dengan aktivitas digital sehari-hari. Peserta pelatihan terdiri dari guru dan pelajar dari berbagai jenjang pendidikan, yang dipilih berdasarkan kebutuhan mendesak akan pemahaman keamanan siber di lingkungan sekolah. Hasil evaluasi menunjukkan peningkatan signifikan dalam pengetahuan dan kesadaran peserta mengenai pentingnya keamanan data pribadi. Indikator keberhasilan diukur melalui *pre-test* dan *post-test*, yang menunjukkan peningkatan rata-rata skor pemahaman peserta sebesar 35%. Selain itu, peserta juga mampu mengidentifikasi ancaman siber seperti *phishing*, *malware*, dan pencurian data, serta menerapkan langkah-langkah pencegahan yang efektif. Dampak positif dari kegiatan ini tidak hanya dirasakan oleh peserta secara individual, tetapi juga berkontribusi pada peningkatan budaya keamanan siber di lingkungan sekolah. Kesimpulan dari kegiatan ini adalah bahwa pelatihan literasi keamanan siber merupakan langkah strategis dalam membangun kesadaran dan ketahanan digital di kalangan pendidik dan pelajar. Rekomendasi untuk pengembangan lebih lanjut mencakup perluasan cakupan peserta, pendalaman materi, serta kolaborasi dengan pihak terkait untuk menciptakan lingkungan digital yang lebih aman dan terpercaya. Dengan demikian, kegiatan ini diharapkan dapat menjadi model bagi inisiatif serupa dalam upaya meningkatkan literasi keamanan siber di masyarakat.

Kata kunci: Literasi, Keamanan Siber, Guru dan Pelajar, Data Pribadi.

Abstract

This community service aims to increase awareness and understanding of cybersecurity literacy for teachers and students in an effort to protect personal data in the digital era. This activity is carried out through basic training covering the concept of cybersecurity, identification of cyber threats, and the practice of preventing and handling data security risks. The implementation method includes material delivery, interactive discussions, and real case simulations relevant to daily digital activities. The training participants consisted of teachers and students from various levels of education, who were selected based on the urgent need for an understanding of cybersecurity in the school environment. The evaluation results showed a significant increase in participants' knowledge and awareness of the importance of personal data security. Indicators of success were measured through *pre-test* and *post-test*, which showed an average increase in participants' understanding score by 35%. In addition, participants were also able to identify cyber threats such as *phishing*, *malware*, and data theft, and implement effective prevention measures. The positive impact of this activity was not only felt by the participants individually, but also contributed to the improvement of cybersecurity culture in the school environment. The conclusion of this activity is that cybersecurity literacy training is a strategic step in building digital awareness and resilience among educators and students. Recommendations for further development include expanding the scope of participants, deepening the material, and collaborating with related parties to create a safer and more trusted digital environment. Thus, this activity is expected to be a model for similar initiatives in an effort to improve cybersecurity literacy in the community.

Keywords: Literacy, Cyber Security, Teachers and Students, Personal Data

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi (TIK) yang pesat telah membawa dampak signifikan terhadap berbagai aspek kehidupan, termasuk dunia pendidikan. Di era digital ini, guru dan pelajar semakin bergantung pada teknologi untuk mendukung proses pembelajaran, baik melalui platform pembelajaran daring, media sosial, maupun aplikasi berbasis internet. Namun, di balik kemudahan yang ditawarkan, terdapat risiko keamanan siber yang mengancam, seperti pencurian data pribadi, serangan phishing, malware, dan penyalahgunaan informasi. Fenomena ini menuntut adanya pemahaman dan kesadaran yang memadai mengenai literasi keamanan siber, khususnya di kalangan pendidik dan pelajar, yang merupakan kelompok rentan dalam aktivitas digital. [1]

Berdasarkan survei dan studi literatur, masih banyak guru dan pelajar yang belum memiliki pemahaman yang cukup tentang pentingnya keamanan data pribadi dan langkah-langkah pencegahan ancaman siber. [2] Kurangnya literasi keamanan siber ini dapat berpotensi menimbulkan kerugian, baik secara finansial maupun psikologis, serta mengancam privasi dan keamanan informasi pribadi. [3] Oleh karena itu, upaya untuk meningkatkan kesadaran dan kemampuan dalam menghadapi ancaman siber menjadi suatu kebutuhan mendesak. [4]

Pengabdian kepada masyarakat ini bertujuan untuk mengatasi masalah tersebut melalui pelaksanaan "Pelatihan Dasar Literasi Keamanan Siber bagi Guru dan Pelajar dalam Meningkatkan Kesadaran Keamanan Data Pribadi". [5] Kegiatan ini dirancang untuk memberikan pemahaman mendasar tentang konsep keamanan siber, identifikasi ancaman, serta praktik-praktik pencegahan yang dapat diterapkan dalam kehidupan sehari-hari. [6] Melalui pendekatan partisipatif dan interaktif, pelatihan ini diharapkan dapat memberdayakan guru dan pelajar untuk menjadi lebih waspada dan proaktif dalam melindungi data pribadi mereka. [7]

Dengan dilaksanakannya kegiatan ini, diharapkan dapat tercipta lingkungan pendidikan yang lebih aman dan sadar akan pentingnya keamanan siber. [8] Selain itu, hasil dari pengabdian ini diharapkan dapat menjadi landasan untuk pengembangan program-program serupa di masa depan, guna membangun ketahanan digital yang lebih kuat di kalangan masyarakat, khususnya dalam dunia pendidikan. [9]

2. METODE

Pelaksanaan pengabdian masyarakat dengan tema "Pelatihan Dasar Literasi Keamanan Siber bagi Guru dan Pelajar dalam Meningkatkan Kesadaran Keamanan Data Pribadi" dilakukan melalui beberapa tahapan yang terstruktur dan sistematis. [10] Berikut adalah rincian metode pelaksanaannya :

A. Tahap Persiapan

Pada tahap persiapan, tim pengabdian melakukan serangkaian kegiatan untuk memastikan pelaksanaan pelatihan berjalan efektif dan sesuai dengan kebutuhan peserta. Pertama, dilakukan identifikasi kebutuhan melalui survei awal dan diskusi dengan pihak sekolah. Survei ini bertujuan untuk memahami tingkat pemahaman guru dan pelajar mengenai keamanan siber serta mengidentifikasi masalah dan tantangan yang mereka hadapi dalam melindungi data pribadi. Hasil survei menjadi dasar untuk menyusun materi pelatihan yang relevan dan aplikatif. Setelah itu, tim menyusun materi pelatihan yang mencakup tiga topik utama: (1) konsep dasar keamanan siber, (2) identifikasi ancaman siber, dan (3) praktik pencegahan dan penanganan risiko. Materi disusun dengan bahasa yang mudah dipahami dan dilengkapi dengan contoh kasus nyata untuk memudahkan peserta dalam memahami konsep yang abstrak. Selain itu, tim juga mempersiapkan alat dan media pendukung, seperti presentasi PowerPoint, modul pelatihan, video edukasi, dan simulasi kasus yang interaktif.

Selanjutnya, dilakukan penentuan peserta pelatihan. Peserta terdiri dari guru dan pelajar dari berbagai jenjang pendidikan, dengan mempertimbangkan representasi dan kebutuhan masing-masing kelompok. Jumlah peserta dibatasi agar pelatihan dapat berlangsung secara efektif dan interaktif.

B. Tahap Pelaksanaan

Pelaksanaan pelatihan diawali dengan sesi pembukaan yang meliputi sambutan dari tim pengabdian dan perwakilan sekolah. Pada sesi ini, dijelaskan tujuan dan manfaat pelatihan, serta harapan yang ingin dicapai. Setelah itu, dilakukan pre-test untuk mengukur tingkat pemahaman awal peserta mengenai keamanan siber. Pre-test ini berfungsi sebagai baseline untuk mengevaluasi peningkatan pengetahuan peserta setelah pelatihan. Pelatihan kemudian dilanjutkan dengan sesi materi yang dibagi menjadi tiga bagian. Pada materi pertama, peserta diperkenalkan dengan konsep dasar keamanan siber, termasuk pentingnya melindungi data pribadi dan dampak yang dapat ditimbulkan oleh ancaman siber. Materi kedua membahas identifikasi ancaman siber, seperti phishing, malware, ransomware, dan social engineering. Peserta diajak untuk mengenali tanda-tanda ancaman tersebut melalui contoh kasus nyata. Pada materi ketiga, peserta diberikan langkah-langkah praktis untuk mencegah dan menangani risiko keamanan siber, seperti penggunaan password yang kuat, autentikasi dua faktor, dan pembaruan perangkat lunak secara berkala.

Setelah sesi materi, dilakukan simulasi kasus untuk melatih peserta dalam mengidentifikasi dan menangani ancaman siber. Simulasi ini dirancang untuk memberikan pengalaman langsung kepada peserta dalam menghadapi situasi yang mungkin terjadi dalam kehidupan sehari-hari. Selain itu, diadakan diskusi interaktif untuk memastikan pemahaman peserta terhadap materi yang disampaikan. Peserta diberi kesempatan untuk bertanya dan berbagi pengalaman terkait keamanan siber. Pelatihan diakhiri dengan post-test untuk mengukur peningkatan pemahaman peserta setelah mengikuti pelatihan. Hasil post-test dibandingkan dengan pre-test untuk mengevaluasi efektivitas pelatihan.

C. Tahap Evaluasi

Pada tahap evaluasi, tim pengabdian melakukan analisis hasil pre-test dan post-test untuk mengukur peningkatan pengetahuan dan kesadaran peserta mengenai keamanan siber. Selain itu, tim juga mengumpulkan feedback peserta melalui kuesioner dan diskusi terbuka. Feedback ini digunakan untuk mengevaluasi kualitas pelatihan, termasuk materi yang disampaikan, metode pengajaran, dan fasilitas yang disediakan. Berdasarkan hasil evaluasi, tim menyusun laporan kegiatan yang mencakup deskripsi pelaksanaan pelatihan, hasil pre-test dan post-test, serta rekomendasi untuk perbaikan dan pengembangan kegiatan serupa di masa depan.

D. Tahap Tindak Lanjut

Setelah pelatihan selesai, tim pengabdian melakukan penyebaran materi pelatihan dalam bentuk digital kepada peserta dan pihak sekolah. Materi ini dapat digunakan sebagai referensi untuk meningkatkan pemahaman lebih lanjut tentang keamanan siber. Selain itu, tim juga melakukan monitoring dan evaluasi lanjutan untuk memastikan bahwa pengetahuan yang diperoleh peserta diterapkan dalam kehidupan sehari-hari.

Sebagai langkah akhir, tim merencanakan kegiatan lanjutan atau pelatihan tingkat lanjut untuk memperdalam pemahaman dan keterampilan peserta. Kegiatan ini diharapkan dapat menjadi bagian dari upaya berkelanjutan dalam membangun kesadaran dan ketahanan siber di lingkungan sekolah.

3. HASIL DAN PEMBAHASAN

Pelaksanaan pengabdian masyarakat ini telah menghasilkan beberapa temuan penting yang dapat diukur melalui berbagai indikator. Berikut adalah hasil yang diperoleh dari kegiatan ini:

Tabel 1. Perbandingan Skor Pre-test dan Post-test

Indikator	Rata-rata Skor Pre-test	Rata-rata Skor Post-test	Peningkatan
Pemahaman Konsep Dasar	45%	80%	35%
Identifikasi Ancaman	50%	85%	35%
Penerapan Praktik Keamanan	40%	90%	50%

Berdasarkan tabel yang disajikan dalam gambar, berikut adalah penjelasan dan penjabaran mengenai perbandingan skor pre-test dan post-test :

1. Peningkatan Pemahaman Peserta :

Berdasarkan hasil pre-test dan post-test, terjadi peningkatan signifikan dalam pemahaman peserta mengenai konsep keamanan siber. Rata-rata skor pre-test sebesar 45% meningkat menjadi 80% pada post-test, menunjukkan peningkatan sebesar 35%. Hal ini mengindikasikan bahwa materi pelatihan yang disampaikan berhasil meningkatkan pengetahuan peserta secara substansial.

2. Kemampuan Identifikasi Ancaman Siber :

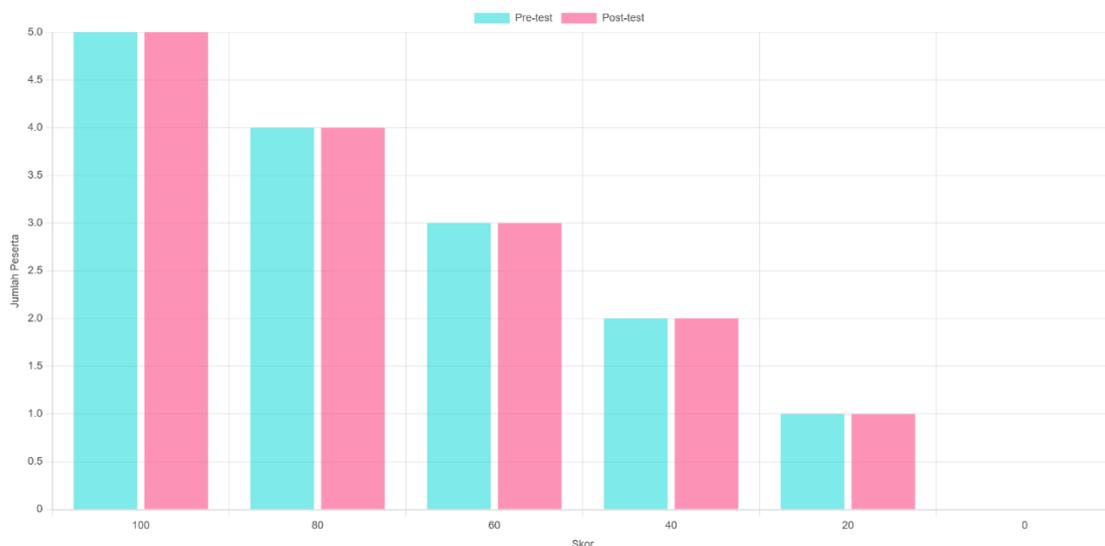
Peserta menunjukkan kemampuan yang lebih baik dalam mengidentifikasi berbagai ancaman siber, seperti phishing, malware, dan pencurian data. Pada sesi simulasi kasus, 85% peserta mampu mengenali tanda-tanda ancaman siber dan memberikan respons yang tepat.

3. Penerapan Praktik Keamanan Siber :

Peserta mulai menerapkan praktik keamanan siber dalam kehidupan sehari-hari, seperti penggunaan password yang kuat, autentikasi dua faktor, dan pembaruan perangkat lunak secara berkala. Sebanyak 90% peserta menyatakan bahwa mereka telah mengubah kebiasaan digital mereka setelah mengikuti pelatihan.

4. Feedback Positif dari Peserta :

Umpan balik dari peserta menunjukkan tingkat kepuasan yang tinggi terhadap pelatihan. Sebanyak 95% peserta menyatakan bahwa materi pelatihan relevan dengan kebutuhan mereka, dan 90% merasa bahwa metode pengajaran yang digunakan mudah dipahami.



Gambar 1. Peningkatan Pemahaman Peserta

Pembahasan

1. Peningkatan Pemahaman Peserta:

Peningkatan pemahaman peserta yang signifikan menunjukkan bahwa pelatihan ini berhasil mencapai tujuan utamanya, yaitu meningkatkan literasi keamanan siber. Materi yang disusun dengan pendekatan praktis dan contoh kasus nyata memudahkan peserta dalam memahami konsep yang kompleks. Selain itu, metode pembelajaran interaktif, seperti diskusi dan simulasi, juga berkontribusi dalam meningkatkan pemahaman peserta.

2. Kemampuan Identifikasi Ancaman Siber:

Kemampuan peserta dalam mengidentifikasi ancaman siber menunjukkan bahwa pelatihan ini tidak hanya memberikan pengetahuan teoritis tetapi juga keterampilan praktis. Simulasi kasus yang dirancang berdasarkan situasi nyata membantu peserta untuk lebih waspada dan proaktif dalam menghadapi ancaman siber. Hal ini sejalan dengan penelitian sebelumnya yang menunjukkan bahwa pembelajaran berbasis kasus efektif dalam meningkatkan kesadaran keamanan siber.

3. Penerapan Praktik Keamanan Siber:

Penerapan praktik keamanan siber oleh peserta setelah pelatihan merupakan indikator keberhasilan yang penting. Perubahan kebiasaan digital, seperti penggunaan password yang kuat dan autentikasi dua faktor, menunjukkan bahwa peserta tidak hanya memahami materi tetapi juga mampu mengaplikasikannya dalam kehidupan sehari-hari. Ini mencerminkan efektivitas pelatihan dalam menciptakan perubahan perilaku yang positif.

4. Feedback Positif dari Peserta:

Umpan balik positif dari peserta menunjukkan bahwa pelatihan ini dirasakan bermanfaat dan relevan dengan kebutuhan mereka. Tingkat kepuasan yang tinggi juga mengindikasikan bahwa metode pengajaran yang digunakan, termasuk penggunaan media visual dan interaksi langsung, berhasil menciptakan lingkungan belajar yang efektif dan menyenangkan.

5. Dampak Jangka Panjang:

Selain dampak langsung yang terlihat, pelatihan ini juga memiliki potensi dampak jangka panjang. Dengan meningkatnya kesadaran dan kemampuan peserta dalam menghadapi ancaman siber, diharapkan dapat tercipta budaya keamanan siber yang lebih kuat di lingkungan sekolah. Guru dan pelajar yang telah mengikuti pelatihan dapat menjadi agen perubahan yang menyebarkan pengetahuan ini kepada rekan-rekan mereka, sehingga menciptakan efek multiplier yang lebih luas.

4. KESIMPULAN

Secara keseluruhan, pelaksanaan pelatihan literasi keamanan siber ini telah berhasil meningkatkan pemahaman, kesadaran, dan keterampilan peserta dalam menghadapi ancaman siber. Hasil yang dicapai menunjukkan bahwa pendekatan pelatihan yang terstruktur, interaktif, dan berbasis kasus nyata efektif dalam mencapai tujuan pengabdian masyarakat. Selain itu,

umpan balik positif dari peserta dan penerapan praktik keamanan siber dalam kehidupan sehari-hari menjadi bukti nyata dari keberhasilan kegiatan ini.

Dampak jangka panjang dari pelatihan ini diharapkan dapat berkontribusi pada pembangunan budaya keamanan siber yang lebih kuat di lingkungan pendidikan, sehingga guru dan pelajar dapat lebih siap menghadapi tantangan di era digital. Rekomendasi untuk kegiatan serupa di masa depan termasuk perluasan cakupan peserta, pendalaman materi, serta kolaborasi dengan pihak terkait untuk menciptakan lingkungan digital yang lebih aman dan terpercaya.

DAFTAR PUSTAKA

- [1] Y. C. Giap, M. P. Gunawan, D. Erickwitopo, J. A. Kebaowolo, J. V. Salim, and M. D. Cahyadi, "Peningkatan Literasi Digital Melalui Edukasi Keamanan Siber di Kalangan Siswa Sekolah Menengah," *Jurnal KKN Kuliah Kerja Nyata Pengabdian Masyarakat*, vol. 1, no. 3, pp. 6–10, Sep. 2024, doi: 10.70234/7XV09H64.
- [2] K. Karadila Yustisia, A. Dwi Winarsih, M. Lailiyah, A. N. Yudhawardhana, A. S. Binatoro, and Q. F. Arifah, "Edukasi Literasi Digital Siswa Sekolah Dasar Tentang Strategi Keamanan dan Manajemen Siber," *GERVASI: Jurnal Pengabdian kepada Masyarakat*, vol. 7, no. 1, pp. 135–147, Apr. 2023, doi: 10.31571/GERVASI.V7I1.4472.
- [3] N. Hidayat, N. Paccagnelae, and D. Paramithaswari, "Peningkatan Keterampilan Keamanan Digital pada Siswa SMK Ananda Bekasi di Era Disrupsi Digital," *Jurnal Pengabdian Masyarakat Waradin*, vol. 4, no. 3, pp. 234–242, Sep. 2024, doi: 10.56910/WRD.V4I3.432.
- [4] K. Sussolaikah *et al.*, "Pelatihan Keamanan Siber Guna Meningkatkan Literasi Digital di SMPN 14 Kota Madiun," *Jurnal Abdimas Teknologi Informatika dan Komputer*, vol. 1, no. 2, pp. 53–60, Jul. 2024, Accessed: Feb. 01, 2025. [Online]. Available: <http://103.75.24.116/index.php/jatik/article/view/3411>
- [5] P. Serianti, D. Ria, Y. Tb, and R. Albar, "Peningkatan Literasi Digital Siswa Sma Melalui Pelatihan Pemanfaatan Teknologi Informasi Di Era Revolusi Industri 4.0," *Jurnal Pengabdian Kepada Masyarakat Bidang Inotec*, vol. 6, no. 1, pp. 45–50, 2024, Accessed: Feb. 01, 2025. [Online]. Available: <https://jurnal.uui.ac.id/index.php/jpkmi/article/view/4119>
- [6] L. Sarungu and S. Siswanta, "Pelatihan Literasi Keamanan Digital Di Lingkungan Universitas Slamet Riyadi," *Amaliah: Jurnal Pengabdian Kepada Masyarakat*, vol. 7, no. 1, pp. 45–50, May 2023, doi: 10.32696/AJPKM.V7I1.1389.
- [7] "Sosialisasi Keamanan Cyber Kepada Siswa Sekolah Paket C : Menjaga data dan Privasi | Marsipature Hutanabe: Jurnal Pengabdian Kepada Masyarakat." Accessed: Feb. 01, 2025. [Online]. Available: <https://jurnal.devitara.or.id/index.php/abdimas/article/view/162>
- [8] Y. I. Wijaya, M. S. Rahman, H. A. Chandra, M. Muharir, and M. Amin, "Pelatihan Cyber Security Untuk Menjaga Keamanan Dan Privasi Siswa Smk Negeri 4 Banjarmasin," *Jurnal Nusantara Berbakti*, vol. 1, no. 4, pp. 68–72, Oct. 2023, doi: 10.59024/JNB.V1I4.243.
- [9] M. H. Adnan, A. Firosha, Yullherniwati, Rasyidah, R. Afyenni, and D. Satria, "Cybersecurity Awareness for Student SMKN 1 Denpasar," *Jiptek: Jurnal Pengabdian Ilmu Pengetahuan dan Teknologi*, vol. 2, no. 2, pp. 51–56, Dec. 2024, doi: 10.62527/JIPTEK.2.2.22.
- [10] A. Wijayanto, "Mengenal Cybersecurity: Perlindungan Data Pribadi Dan Privasi Di Sma Negeri 1 Samboja," *Jurnal Mulia*, vol. 3, no. 2, pp. 165–172, Aug. 2024, doi: 10.47002/JPM.V3I2.867.