AMMA : Jurnal Pengabdian Masyarakat
Volume 2, No.4 Mei (2023)
ISSN 2828-6634 (media online)
Hal 528-533

Pelatihan Keamanan Siber Dasar Untuk Pelajar Dan Guru Di Sekolah Menengah

Tati Suprapti[1*], Umi Hayati[2], Alwan Azhar[3], Andi Ardiansyah[4]

[1,2,3,4]Program Studi Teknik Informatika, STMIK IKMI Cirebon, Cirebon, Indonesia
Email: [1*]tatsuprapti.ikmi@gmail.com, [2]umihayati.ikmi@gmail.com, [3]alwanazhari.ikmi@gmail.com, [4]andiardiansyah.ikmi@gmail.com
(* : tatsuprapti.ikmi@gmail.com)

Abstrak − Keamanan siber merupakan upaya yang bertujuan untuk melindungi sistem komputer, jaringan, perangkat lunak, serta data dari berbagai ancaman digital seperti peretasan, malware, phishing, ransomware, dan serangan lainnya yang dapat menyebabkan kerugian baik secara material maupun non-material. Dalam era digital yang semakin berkembang pesat, khususnya di lingkungan pendidikan seperti sekolah menengah, kesadaran akan pentingnya keamanan siber menjadi hal yang sangat krusial. Pelajar dan guru yang menggunakan perangkat digital dalam proses belajar mengajar sering kali menjadi sasaran empuk bagi para pelaku kejahatan siber yang mencari celah untuk mengeksploitasi kerentanan keamanan. Pemahaman dasar mengenai keamanan siber perlu ditanamkan kepada pelajar dan guru agar mereka dapat mengidentifikasi ancaman potensial serta menerapkan langkah-langkah pencegahan yang tepat. Artikel ini bertujuan untuk memberikan panduan praktis dalam mengenali berbagai jenis ancaman siber yang umum terjadi, seperti serangan phishing yang menyamar sebagai situs atau pesan yang sah, malware yang menyusup melalui perangkat lunak yang terinfeksi, serta serangan ransomware yang mengenkripsi data untuk mendapatkan tebusan. Selain itu, artikel ini juga menguraikan sejumlah strategi pencegahan yang dapat diterapkan oleh pelajar dan guru, termasuk penggunaan kata sandi yang kuat, pembaruan perangkat lunak secara rutin, serta pengelolaan privasi di media sosial. Dengan memahami konsep dasar keamanan siber dan mengadopsi praktik terbaik dalam melindungi data serta perangkat digital, diharapkan pelajar dan guru dapat mengurangi risiko yang mungkin timbul dari aktivitas digital yang tidak aman. Lebih jauh lagi, penerapan keamanan siber yang efektif dapat menciptakan lingkungan belajar yang lebih aman dan kondusif bagi seluruh pihak yang terlibat.

Kata Kunci: Keamanan Siber, Pelajar, Guru, Sekolah Menengah, Perlindungan Data, Ancaman Digital, Pencegahan

Abstract − *Cybersecurity is an effort that aims to protect computer systems, networks, software, and data from various digital threats such as hacking, malware, phishing, ransomware, and other attacks that can cause both material and non-material losses. In the rapidly growing digital era, especially in educational environments such as secondary schools, awareness of the importance of cybersecurity is crucial. Students and teachers who use digital devices in the teaching and learning process are often easy targets for cyber criminals who are looking for loopholes to exploit security vulnerabilities. A basic understanding of cybersecurity needs to be instilled in students and teachers so that they can identify potential threats and implement appropriate preventive measures. This article aims to provide practical guidance in recognizing common types of cyber threats, such as phishing attacks that masquerade as legitimate sites or messages, malware that infiltrates through infected software, and ransomware attacks that encrypt data for ransom. In addition, the article also outlines a number of prevention strategies that students and teachers can implement, including the use of strong passwords, regular software updates, and managing privacy on social media. By understanding the basic concepts of cybersecurity and adopting best practices in protecting digital data and devices, it is hoped that students and teachers can reduce the risks that may arise from unsafe digital activities. Furthermore, effective cybersecurity implementation can create a safer and more conducive learning environment for all parties involved.*

Keywords*: Cybersecurity, Students, Teachers, Secondary Schools, Data Protection, Digital Threats, Prevention.*

1. PENDAHULUAN

1.1 Analisis Situasi

Di era digital saat ini, penggunaan teknologi informasi dan internet di lingkungan sekolah semakin meningkat. Pelajar dan guru di sekolah menengah sering menggunakan perangkat digital seperti komputer, laptop, dan ponsel pintar untuk mengakses informasi, belajar daring, serta berkomunikasi melalui berbagai platform. Namun, minimnya kesadaran akan keamanan siber menyebabkan mereka rentan terhadap berbagai ancaman digital seperti phishing, malware,

pencurian data, dan peretasan akun. Berdasarkan data dari **Badan Siber dan Sandi Negara (BSSN)**, serangan siber di Indonesia meningkat signifikan dalam beberapa tahun terakhir, dengan sektor pendidikan menjadi salah satu target utama. Studi juga menunjukkan bahwa banyak siswa dan guru belum memiliki pemahaman yang cukup mengenai praktik keamanan siber yang baik, seperti pentingnya kata sandi yang kuat, pengamanan data pribadi, serta cara mengidentifikasi ancaman siber. Oleh karena itu, kegiatan pengabdian ini diperlukan untuk meningkatkan literasi keamanan siber di kalangan pelajar dan tenaga pendidik di sekolah menengah.

1.2 Permasalahan Mitra

Mitra dalam kegiatan ini, yaitu sekolah menengah, menghadapi beberapa permasalahan utama terkait keamanan siber, antara lain:

1. **Kurangnya Kesadaran dan Edukasi** – Banyak pelajar dan guru tidak memahami pentingnya menjaga keamanan data dan belum terbiasa menerapkan langkah-langkah proteksi dasar.
2. **Rentan terhadap Serangan Siber** – Banyak akun sekolah dan pribadi telah menjadi sasaran peretasan akibat penggunaan kata sandi yang lemah dan berbagi informasi sensitif secara sembarangan.
3. **Minimnya Kebijakan Keamanan Digital di Sekolah** – Sekolah umumnya belum memiliki regulasi atau panduan resmi terkait keamanan siber, sehingga belum ada standar perlindungan yang diterapkan secara sistematis.
4. **Penggunaan Internet yang Tidak Aman** – Beberapa siswa dan guru sering mengakses situs yang tidak aman atau mengunduh file dari sumber yang tidak terpercaya, yang dapat menyebabkan infeksi malware atau pencurian data.

Permasalahan ini tidak hanya menghambat proses pembelajaran digital yang aman tetapi juga berisiko membahayakan data pribadi serta informasi akademik yang penting.

1.3 Tujuan Kegiatan

Kegiatan pengabdian ini bertujuan untuk:

1. **Meningkatkan Kesadaran Keamanan Siber** – Memberikan pemahaman dasar kepada pelajar dan guru mengenai pentingnya keamanan siber dalam aktivitas digital sehari-hari.
2. **Melatih Praktik Keamanan Digital** – Mengajarkan cara mengamankan akun, menggunakan kata sandi yang kuat, serta mengidentifikasi dan menghindari ancaman siber seperti phishing dan malware.
3. **Membantu Sekolah Menyusun Kebijakan Keamanan Siber** – Memberikan rekomendasi untuk sekolah dalam merancang kebijakan terkait keamanan digital guna melindungi data siswa dan guru.
4. **Menciptakan Lingkungan Digital yang Aman di Sekolah** – Mendorong penggunaan teknologi secara aman dan bertanggung jawab untuk mendukung proses pembelajaran yang lebih efektif.

1.4 Manfaat Kegiatan

Pelaksanaan kegiatan ini akan memberikan berbagai manfaat bagi mitra dan pihak terkait, di antaranya:

1. **Bagi Pelajar** – Mereka akan lebih sadar akan pentingnya menjaga keamanan data pribadi dan akun mereka, serta mampu menghindari ancaman siber yang sering terjadi.
2. **Bagi Guru dan Staf Sekolah** – Guru akan memiliki pengetahuan lebih baik dalam membimbing siswa terkait keamanan digital dan dapat melindungi data akademik sekolah dengan lebih efektif.
3. **Bagi Sekolah** – Dengan adanya pelatihan ini, sekolah dapat meningkatkan sistem keamanan digital mereka serta mengurangi risiko kebocoran data atau serangan siber.

AMMA : Jurnal Pengabdian Masyarakat
Volume 2, No.4 Mei (2023)
ISSN 2828-6634 (media online)
Hal 528-533

4. **Bagi Masyarakat** – Kesadaran keamanan siber yang meningkat di lingkungan sekolah akan berdampak pada pola penggunaan internet yang lebih aman di kehidupan sehari-hari.

2. METODE PELAKSANAAN

Untuk memastikan keberhasilan kegiatan pengabdian kepada masyarakat ini, metode pelaksanaan dirancang secara sistematis dengan beberapa tahapan utama, yaitu:

1. Persiapan dan Perencanaan

a) Melakukan analisis kebutuhan di sekolah mitra untuk memahami tingkat pemahaman siswa dan guru tentang keamanan siber.

b) Menyusun materi pelatihan berupa modul, presentasi, dan studi kasus terkait keamanan digital.

c) Mempersiapkan alat dan sarana yang dibutuhkan, seperti perangkat komputer, jaringan internet, dan platform e-learning jika diperlukan.

d) Berkoordinasi dengan pihak sekolah untuk menentukan jadwal pelaksanaan kegiatan.

2. Pelaksanaan Kegiatan

Kegiatan pelatihan keamanan siber akan dilakukan melalui beberapa metode berikut:

a) Workshop dan Seminar – Penyampaian materi tentang keamanan siber dasar, termasuk cara membuat kata sandi yang kuat, mengenali serangan phishing, serta menjaga keamanan perangkat digital.

b) Praktik Langsung dan Simulasi – Peserta akan diberikan simulasi serangan siber seperti phishing email atau pencurian data, kemudian diajarkan cara mengatasinya.

c) Diskusi Interaktif – Guru dan siswa akan diberi kesempatan untuk bertanya dan berbagi pengalaman terkait keamanan digital yang pernah mereka hadapi.

d) Evaluasi dan Post-Test – Dilakukan untuk mengukur peningkatan pemahaman peserta setelah pelatihan.

3. Implementasi dan Pendampingan

a) Mendorong sekolah untuk menerapkan kebijakan keamanan siber yang telah disusun dalam kegiatan.

b) Memberikan pendampingan bagi guru dalam mengintegrasikan konsep keamanan digital ke dalam kegiatan belajar mengajar.

c) Menyediakan sesi konsultasi jika ada kendala atau pertanyaan dari siswa dan guru terkait keamanan siber.

4. Evaluasi dan Tindak Lanjut

a) Melakukan survei dan wawancara untuk mengukur dampak pelatihan terhadap peningkatan kesadaran keamanan siber di sekolah.

b) Menyusun laporan hasil kegiatan yang mencakup tingkat pemahaman peserta sebelum dan sesudah pelatihan.

c) Memberikan rekomendasi untuk keberlanjutan program agar sekolah dapat terus meningkatkan keamanan digitalnya.

AMMA : Jurnal Pengabdian Masyarakat
Volume 2, No.4 Mei (2023)
ISSN 2828-6634 (media online)
Hal 528-533

3. HASIL DAN PEMBAHASAN

3.1 Hasil

Hasil dari pelaksanaan program Keamanan Siber Dasar untuk Pelajar dan Guru di Sekolah Menengah:

Hasil Pelaksanaan Program

Program *Keamanan Siber Dasar untuk Pelajar dan Guru di Sekolah Menengah* telah berhasil mencapai tujuan yang telah ditetapkan. Beberapa hasil utama dari pelaksanaan program ini adalah:

1. **Peningkatan Kesadaran Keamanan Siber**
   a) Pelajar dan guru kini lebih memahami pentingnya keamanan siber dalam aktivitas digital mereka.
   b) Mereka telah mengenali berbagai ancaman siber seperti phishing, malware, pencurian data, dan metode untuk menghindarinya.
2. **Penerapan Praktik Keamanan Digital**
   a) Peserta mulai menerapkan kebiasaan yang lebih aman, seperti menggunakan kata sandi yang kuat, mengaktifkan autentikasi dua faktor, dan berhati-hati dalam membagikan informasi pribadi secara daring.
   b) Guru lebih proaktif dalam mengajarkan keamanan digital kepada siswa dalam pembelajaran sehari-hari.
3. **Pengurangan Risiko Serangan Siber di Sekolah**
   a) Setelah pelatihan, terjadi penurunan kasus akun siswa atau guru yang diretas akibat kesalahan dasar seperti penggunaan kata sandi yang lemah.
   b) Sekolah mulai menerapkan kebijakan dasar terkait keamanan digital, seperti penggunaan perangkat yang lebih aman dan pembatasan akses ke situs yang berisiko.
4. **Dampak Positif bagi Mitra**
   a) Guru dan siswa merasa lebih percaya diri dalam menggunakan teknologi secara aman.
   b) Sekolah mulai mempertimbangkan penerapan regulasi yang lebih ketat dalam perlindungan data akademik dan penggunaan teknologi di lingkungan pendidikan.

3.2 Pembahasan

Sebagai hasil dari pelaksanaan program ini, beberapa luaran konkret yang telah dihasilkan antara lain:

1. **Modul Pelatihan Keamanan Siber**

   Sebuah modul pembelajaran yang mencakup dasar-dasar keamanan siber, contoh ancaman digital, serta langkah-langkah pencegahan yang dapat diterapkan oleh guru dan siswa.

2. **Workshop dan Simulasi**

   Kegiatan pelatihan interaktif yang memberikan pengalaman langsung kepada peserta dalam menghadapi ancaman siber dan cara mengatasinya.

3. **Peningkatan Keterampilan Digital**

   Guru dan siswa kini memiliki keterampilan praktis dalam mengamankan akun mereka, mengenali ancaman digital, serta memahami kebijakan privasi dalam menggunakan teknologi.

4. **Rekomendasi Kebijakan Keamanan Digital untuk Sekolah**

   Usulan kebijakan kepada pihak sekolah mengenai strategi pengelolaan keamanan siber, termasuk pedoman bagi siswa dan guru dalam menggunakan perangkat digital secara aman.

AMMA : Jurnal Pengabdian Masyarakat
Volume 2, No.4 Mei (2023)
ISSN 2828-6634 (media online)
Hal 528-533

Dengan adanya hasil dan luaran ini, diharapkan sekolah dapat terus mengembangkan program keamanan siber secara berkelanjutan untuk melindungi data dan aktivitas digital mereka.

Foto Kegiatan.

Gambar 1. Foto Kegiatan

4. KESIMPULAN

Kegiatan *Keamanan Siber Dasar untuk Pelajar dan Guru di Sekolah Menengah* telah memberikan dampak positif dalam meningkatkan kesadaran serta keterampilan dalam menjaga keamanan digital. Beberapa kesimpulan utama dari program ini adalah:

1. **Peningkatan Kesadaran Keamanan Siber**
   a) Pelajar dan guru kini lebih memahami pentingnya menjaga keamanan data pribadi dan akun digital mereka.
   b) Mereka telah belajar mengenali ancaman siber seperti phishing, malware, dan serangan peretasan.
2. **Implementasi Kebiasaan Digital yang Lebih Aman**

   Setelah pelatihan, peserta mulai menerapkan praktik keamanan seperti penggunaan kata sandi yang kuat, autentikasi dua faktor, serta berhati-hati dalam membagikan informasi di internet.
3. **Pentingnya Kebijakan Keamanan Digital di Sekolah**

   Sekolah mulai menyadari perlunya kebijakan dan regulasi terkait keamanan siber guna melindungi data akademik dan aktivitas digital siswa serta tenaga pendidik.
4. **Kebutuhan akan Pelatihan Berkelanjutan**

   Mengingat perkembangan ancaman siber yang terus berubah, penting bagi sekolah untuk terus mengadakan pelatihan dan pembaruan pengetahuan terkait keamanan digital.

Dari program ini, terdapat beberapa pelajaran penting yang dapat diterapkan untuk kegiatan serupa di masa depan:

Pentingnya Edukasi Dini

a) Keamanan siber harus diperkenalkan sejak dini kepada pelajar untuk membentuk kebiasaan digital yang aman sejak awal.

Pendekatan Praktis Lebih Efektif

a) Simulasi dan studi kasus nyata membantu peserta lebih memahami dan mengingat materi pelatihan dibandingkan sekadar teori.

Dukungan Pihak Sekolah Sangat Penting

a) Keberhasilan program ini tidak hanya bergantung pada peserta, tetapi juga pada dukungan sekolah dalam menerapkan kebijakan yang mendukung keamanan digital.

Rekomendasi untuk Keberlanjutan Program

Agar program ini dapat terus memberikan manfaat jangka panjang, beberapa rekomendasi yang dapat diterapkan adalah:

1. **Pelatihan Berkelanjutan**

   Mengadakan pelatihan rutin setiap tahun agar guru dan siswa selalu mendapatkan informasi terbaru mengenai ancaman siber dan cara mengatasinya.

2. **Pembuatan Panduan Keamanan Digital Sekolah**

   Menyusun pedoman resmi terkait kebijakan keamanan digital yang harus diterapkan oleh seluruh warga sekolah.

3. **Kolaborasi dengan Ahli Keamanan Siber**

   Menggandeng pakar keamanan siber atau lembaga terkait untuk memberikan pelatihan yang lebih mendalam dan sesuai dengan perkembangan terbaru.

4. **Monitoring dan Evaluasi**

   Melakukan evaluasi berkala untuk mengukur efektivitas program dan memperbaiki aspek yang masih perlu ditingkatkan.

Dengan adanya kesadaran yang lebih tinggi serta penerapan kebijakan yang lebih baik, diharapkan sekolah-sekolah dapat menjadi lingkungan digital yang lebih aman dan terlindungi dari berbagai ancaman siber.

DAFTAR PUSTAKA

Anderson, R. (2008). Security Engineering: A Guide to Building Dependable Distributed Systems (2nd ed.). Wiley.
Bishop, M. (2005). Introduction to Computer Security. Addison-Wesley.
Laudon, K. C., & Laudon, J. P. (2016). Management Information Systems: Managing the Digital Firm (14th ed.). Pearson.
Pfleeger, C. P., & Pfleeger, S. L. (2007). Security in Computing (4th ed.). Prentice Hall.
Schneier, B. (2015). Applied Cryptography: Protocols, Algorithms, and Source Code in C (20th Anniversary ed.). Wiley.
Stallings, W. (2017). Cryptography and Network Security: Principles and Practice (7th ed.). Pearson.
Whitman, M. E., & Mattord, H. J. (2018). Principles of Information Security (6th ed.). Cengage Learning.
McAfee, Inc. (2020). Cybersecurity Report: The Hidden Costs of Cybercrime. McAfee.
Kaspersky Lab. (2021). Global IT Security Risks Survey. Kaspersky Lab.
NIST. (2020). Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1). National Institute of Standards and Technology.