APPA : Jurnal Pengabdian kepada Masyarakat
Volume 2, No. 4 Desember 2024
ISSN 3025-0889 (media online)
Hal 295-301

Pentingnya Keamanan Data Di Era Digital

Muhammad Satriaji[1*], Fahriza Abdul Ghani[2], Agus Rachmat[3], Ajie Nugroho[4], Nixon C.[5], Pramudiya[6], Taufik Afrizal[7], Haiqal Aqmal Suryanto[8], Gilang Hari Saputra[9], Muhammad Miftahul Habaib[10]

[1-10]Fakultas Ilmu Komputer, Teknik Informatika, Universitas Pamulang, Jl. Raya Puspiptek No. 46, Kel. Buaran, Kec. Serpong, Kota Tangerang Selatan. Banten 15310, Indonesia
Email: [1*]muhammadsatriaji28@email.com, [2]ghanifahriza@email.com , [3]arachmat2312@gmail.com, [4]ajenugroho277@gmail.com, [5]nixonclementius@gmail.com , [6]pramudiapram826@gmail.com, [7]taufikganteng0881@gmail.com, [8]haiqalaqmal.s@gmail.com , [9]gilangghs03@gmail.com, [10]miftahulhabaib@gmail.com
(* : coressponding author)

Abstrak−Era digital membawa berbagai peluang sekaligus tantangan, terutama dalam hal keamanan data, salah satu isu utama yang dihadapi adalah ancaman siber, seperti phising, malware, dan pencurian identitas, yang dapat merugikan individu maupun organisasi. Sayangnya, kesadaran akan pentingnya keamanan data, khususnya di kalangan siswa SMK, masih sangat rendah. Padahal, sebagai generasi muda yang aktif menggunakan teknologi, mereka rentan terhadap serangan siber. Kegiatan pengabdian masyarakat ini bertujuan untuk meningkatkan literasi digital siswa SMK Muara Ilmu di Bojongsari, Depok, melalui sosialisasi dan workshop interaktif tentang keamanan data. Kegiatan ini memanfaatkan fasilitas yang tersedia, seperti laboratorium komputer, untuk memberikan pengalaman langsung dalam memahami dan menerapkan langkah-langkah preventif terhadap ancaman siber. Materi yang disampaikan mencakup pengenalan dasar *cybersecurity*, identifikasi jenis-jenis ancaman siber, dan strategi perlindungan data pribadi. Melalui pendekatan yang terstruktur dan melibatkan simulassi praktis, kegiatan ini diharapkan dapat menciptakan budaya keamanan digital dikalangan siswa. Selain itu, siswa diharapkan mampu menjadi agen perubahan yang menyebarkan kesadaran akan pentingnya menjaga keamanan data kepada teman dan komunitas mereka. Luaran yang dihasilkan meliputi peningkatan kesadaran akan keamanan data, keterampilan praktis dalam menghadapi ancaman siber, dan pembentukan generasi muda yang lebih bijak dalam memanfaatkan teknologi.

Kata Kunci: Keamanan Data, Ancaman Siber, *Cybersecurity*, Literasi Digital, Siswa SMK, Budaya Keamanan Digital, Workshop Keamanan Data

Abstract−*The digital era presents both opportunities and challenges, particularly in the realm of data security. One of the primary issues is cyber threats, such as phishing, malware, and identity theft, which can harm individuals and organizations alike. Unfortunately, awareness of the importance of data security, especially among vocational high school (SMK) students, remains low. As active technology users, they are highly vulnerable to cyberattacks. This community service program aims to enhance the digital literacy of SMK Muara Ilmu students in Bojongsari, Depok, through interactive socialization and workshops on data security. Utilizing available facilities such as computer laboratories, the program provides hands-on experience to help students understand and implement preventive measures against cyber threats. The materials cover the basics of cybersecurity, identification of different types of cyber threats, and strategies for personal data protection. Through a structured approach involving practical simulations, this activity is expected to foster a culture of digital security among students. Moreover, students are encouraged to become agents of change by raising awareness about data security among their peers and community. The expected outcomes include increased awareness of data security, practical skills for mitigating cyber threats, and the formation of a generation that uses technology more wisely.*

Keywords*: Data Security, Cyber Threats, Cybersecurity, Digital Literacy, Vocational Students, Digital Security Culture, Data Security Workshop*

1. PENDAHULUAN

Keamanan siber merupakan sebuah rangkaian aktivitas yang diarahkan untuk melindungi dari ancaman, gangguan, serangan jaringan komputer (perangkat keras dan perangkat lunak), terkait informasi di dalamnya, dan elemen-elemen ruang siber lainnya. Keamanan siber dapat digunakan sebagai sarana melindungi terhadap pengawasan yang tidak diinginkan, seperti kegiatan intelijen. Dengan demikian, keamanan siber adalah semua mekanisme perlindungan yang digunakan untuk meminimalisir gangguan pada ketersediaan (availability), integritas (integrity), dan kerahasiaan (confidentiality) dari sebuah informasi.1 Kerahasiaan data merujuk pada akses yang disetujui

APPA : Jurnal Pengabdian kepada Masyarakat
Volume 2, No. 4 Desember 2024
ISSN 3025-0889 (media online)
Hal 295-301

terhadap sebuah data, yang berarti hanya pihak yang memiliki akses saja yang dapat membukanya. Usaha untuk mendapatkan akses dengan cara mencuri informasi diartikan sebagai tindakan membahayakan kerahasiaan data (Aji, 2022).

Di era digital yang semakin berkembang, ancaman *cyber* menjadi salah satu isu yang mendesak untuk diperhatikan. Siswa, sebagai generasi muda yang aktif menggunakan teknologi, sering kali memhami risiko yang mengintai di dunia maya. *Cybersecurity* mencakup berbagai teknologi, prosedur, dan praktik yang dirancang untuk melindungi sistem dan data dari serangan siber. *Cybercrime* adalah serangan yang dilakukan melalui teknologi internet. Serangan cyber juga menjadi salah satu serangan yang sering terjadi di dunia (Nasution, 2023).

Seiring perkembangan zaman, teknologi menimbulkan dampak yang besar bagi kehidupan manusia. Kehadirannya membawa perubahan dalam bentuk perilaku dan pola kehidupan masyarakat, serta menyebabkan perubahan ekonomi, budaya, sosial dan penegakan hukum. Perkembangan ini telah memasuki revolusi industri 4.0 yang ditandai dengan meningkatnya pemakaian teknologi informasi. Dengan meningkatnya penggunaan internet, penting bagi siswa untuk memiliki pengetahuan dasar tentang cara melindungi diri mereka dari berbagai ancaman.

Di era digital saat ini, ancaman siber menjadi isu yang sangat penting, terutama bagi generasi muda yang aktif menggunakan teknologi. Siswa, sebagai pengguna utama teknologi, sering kali kurang memahami risiko yang ada di dunia maya. *Cybersecurity* mencakup berbagai langkah dan praktik yang dirancang untuk melindungi sistem dan data dari serangan siber. Hal ini menjadi krusial mengingat banyaknya kasus pencurian identitas dan penipuan online yang terjadi.

2. METODE PELAKSANAAN

2.1 Rencana Kegiatan

Dalam kegiatan pengabdian masyarakat ini, metode yang digunakan terdiri dari beberapa tahapan yang dirancang untuk memastikan transfer pengetahuan secara efektif dan berdampak. Berikut adalah metode yang digunakan.

1. **Persiapan Materi dan Peralatan**
   a. Membuat materi presentasi interaktif yang mencakup dasar-dasar keamanan data, jenis-jenis ancaman siber (*phising*, *malware*, *trojan*, dll), serta langkah-langkah preventif untuk melindungi data pribadi.
   b. Menyiapkan alat bantu seperti laptop, proyektor, tripod, kamera dan perangkat pendukung lainnya.
2. **Sosialisasi**
   a. Melalui sesi presentasi di kelas, siswa diberikan pengenalan dasar tentang konsep keamanan digital dan pentingnya melindungi data pribadi di era digital.
   b. Penyampaian materi dilakukan menggunakan pendekatan interaktif untu meningkatkan pemahaman dan keterlibatan siswa.
3. **Workshop dan Simulasi Praktis**
   a. Simulasi ancaman siber seperti *phising* atau serangan *malware*, sehingga siswa dapat memahami cara kerja ancaman tersebut dan bagaimana cara menghindarinya.
4. **Diskusi dan Tanya Jawab**
   a. Sesi diskusi diadakan untuk membahas kasus-kasus nyata tentang pelanggaran data dan cara mengatasinya.
   b. Siswa diajak berpartisipasi aktif dengan mengajukan pertanyaan atau berbagi pengalaman pribadi terkait penggunaan internet.
5. **Monitoring dan Evaluasi**
   a. Pemantauan dilakukan selama kegiatan untuk memastikan efektivitas penyampaian materi.
   b. Evaluasi dilakukan melalui survei singkat atau kuis untuk mengukur sejauh mana siswa memahami materi yang disampaikan.
6. **Penyusunan Laporan Akhir**
   a. Hasil dari kegiatan, termasuk dokumentasi, umpan balik peserta, dan hasil evaluasi, disusun dalam bentuk laporan akhir sebagai bukti pelaksanaan kegiatan.

APPA : Jurnal Pengabdian kepada Masyarakat
Volume 2, No. 4 Desember 2024
ISSN 3025-0889 (media online)
Hal 295-301

Metode ini dirancang agar siswa tidak hanya memahami pentingnya keamanan data secara teori tetapi juga mampu mengimplentasikannya dalam kehidupan sehari-hari.

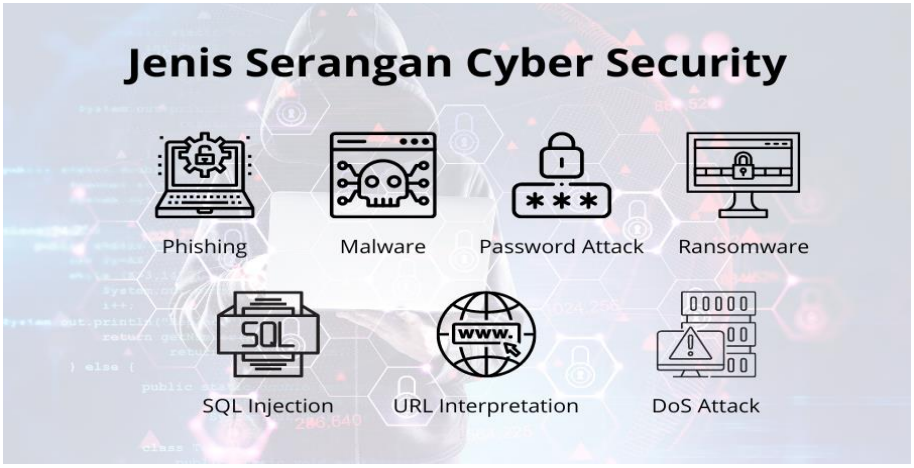
2.2 *Cybersecurity*

Cybersecurity adalah (Ghernaouti-Helie (2009)) mekanisme untuk melindungi sumber daya teknologi informasi, baik yang bersifat material maupun imaterial, dari potensi bahaya yang dapat merusak, menghancurkan, atau mengganggu kerahasiaan (*confidentiality*), integritas (*Integrity*), dan ketersediaan (*availability*) infromasi.

Berikut adalah daftar jenis-jenis *Cybersecurity* dalam tabel 1 dan jenis-jenis serangan *Cybersecurity* ada pada Gambar 1.

Tabel 1. Jenis-Jenis *Database*

Jenis *Cybersecurity*	Deskripsi Singkat	Contoh Penerapan
Network Security	Melindungi jaringan dari akses tidak sah.	Firewall, VPN
Application Security	Melindungi aplikasi dari kerentanan.	Patch Software
Cloud Security	Mengamankan data dan aplikasi di cloud.	Enkripsi, IAM
IoT Security	Mengamankan perangkat Internet of Things.	Auntentikasi perangkat
Endpoint Security	Melindungi perangkat pengguna akhir.	Antivirus, EDR



Gambar 1. Jenis Serangan *Cybersecurity*

3. ANALISA DAN PEMBAHASAN

3.1 Kegiatan PKM

Kegiatan pengabdian kepada masyarakat ini sudah dilaksanakan di SMK Muara Ilmu, Bojongsari, Depok, dengan serangkaian aktivitas yang dirancang untuk memberikan pengalaman edukatif, interaktif, dan menyenangkan kepada para siswa. Berikut adalah kegiatan utama yang telah dilaksanakan:

3.1.1 *Ice Breaking*

Untuk mencairkan suasana dan meningkatkan interaksi antara siswa dan tim, kegiatan ini dimulai dengan permianan tebak gambar interaktif dengan tema keamanan digital. Gambar-gambar tersebut dapat berupa ilustrasi ancaman siber (seperti phising atau malware) atau simbol keamanan (seperti kunci, gembok, firewall). Siswa diajak untuk menebak dan berdiskusi, sambil memperkenalkan konsep dasar keamanan data dengan cara yang menyenangkan dan memotivasi.

APPA : Jurnal Pengabdian kepada Masyarakat
Volume 2, No. 4 Desember 2024
ISSN 3025-0889 (media online)
Hal 295-301

Gambar 2. *Ice Breaking*

3.1.2 Sosialisai Inspiratif

Setelah *ice breaking*, siswa diperkenalkan pada pentingnya keamanan data di era digital. Dalam sesi ini, berbagai ancaman siber, seperti phising, malware dan pencurian data, dijelaskan secara menarik melalui cerita dan contoh nyata.

Gambar 3. Sosialisai Inspiratif

3.1.3 Workshop Praktis

Melalui pelatihan langsung, siswa akan mempelajari langkah-langkah konkret untuk melindungi diri dari serangan siber. Aktivitas ini dilengkapi dengan simulasi penggunaan alat keamanan digital. Seperti antivirus, enkripsi, dan pengaturan kata sandi yang kuat, sehingga siswa dapat langsung menerapkannya.

Gambar 4. *Workshop* Praktis

3.1.4 Diskusi Interaktif

Dalam sesi ini, siswa diajak untuk berbagi pengalaman dan pandangan mereka tentang keamanan digital. Dengan suasana yang santai namun edukatif, diskusi ini memfasilitasi pemahaman lebih dalam tentang pentingnya keamanan di dunia maya.

3.1.5 Simulasi Serangan Siber

APPA : Jurnal Pengabdian kepada Masyarakat
Volume 2, No. 4 Desember 2024
ISSN 3025-0889 (media online)
Hal 295-301

aktivitas simulasi memberikan pengalaman langsung tentang bagaimana serangan siber bekerja dan langkah-langkah untuk mengatasinya. Siswa akan belajar melalui skenario praktis, seperti mendeteksi email phising atau menangani malware, yang dirancang untuk mempersiapkan mereka menghadapi ancaman nyata.

Dengan tambahan kegiatan *ice breaking*, suasana kegiatan menjadi lebih santai dan menyenangkan sehingga siswa lebih antusias untuk mengikuti rangkaian acara. Kegiatan ini diharapkan mampu meningkatkan pemahaman siswa, menciptakan budaya keamanan digital, dan melahirkan generasi muda yang lebih sadar akan pentingnya menjaga privasi dan data di era digital.

3.2 Analisis Dampak

Kegiatan pengabdian kepada masyarakat bertema "**Sosialisasi Pentingnya Keamanan Data di Era Digital"** di SMK Muara Ilmu diharapkan membawa dampak positif yang berkelanjutan, tidak hanya bagi siswa, tetapi juga bagi sekolah dan masyarakat luas. Berikut adalah dampak yang diharapkan dari kegiatan ini:

a. Meningkatkan Kesadaran Siswa

Siswa akan lebih memahami pentingnya menjaga keamanan data pribadi dan bahaya yang dapat timbul dari ancaman siber seperti phising, malware, atau pencurian identitas. Dengan sepengetahuan ini, mereka akan lebih bijak dalam menggunakan teknologi, sehingga dapat melindungi diri dari risiko kejahatan digital.

b. Penguasaan Keterampilan Praktis

Melalui pelatihan langsung dalam workshop dan simulasi, siswa akan mempelajari langkah-langkah praktis untuk mengidentifikasi dan menangani ancaman siber. Keterampilan ini sangat relevan untuk menghadapi tantangan dunia digital saat ini, baaik dikehidupan sehari-hari maupun di lingkungan kerja dimasa depan.

c. Membangun Budaya Keamanan Digital

Dengan meningkatnya pemahaman siswa tentang keamanan siber, terciptalah budaa digital yang lebih aman dan bertanggung jawab. Siswa tidak hanya melindungi di

d. Dampak Positif untuk Sekolah

Kegiatan ini akan memperkuat reputasi SMK Muara Ilmu sebagai institusi yang tanggap terhadap isu-isu terkini, seperti keamanan siber. Sekolah akan dikenal sebagai tempat yang tidak hanya mendidik siswa secara akademis, tetapi juga mempersiapkan mereka untuk menghadapi tantangan era digital. Ini dapat menjadi daya tarik tambahan bagi calon siswa dan orang tua.

e. Kontribusi ke Masyarakat

Dampak jangka panjang dari kegiatan ini adalah peningkatkan **literasi digital** di lingkungan masyarakat sekitar. Siswa yang memahami pentingnya keamanan data dapat berkontribusi dalam meningkatkan kesadaran digital masyarakat, sehingga menciptakan komunitas yang lebih aman dan siap menghadapi ancaman siber.

f. Evaluasi dan Inovasi Program

Kegiatan ini juga menjadi peluang untuk mengevaluasi efektivitas program pengabdian masyarakat. Feedback dari peserta akan menjadi masukan penting untuk pengembangan materi dan metode yang lebih inovatif di masa mendatang. Dengan begitu program serupa dapat dilaksanakan dengan dampak yang lebih luas dan signifikan.

3.3 Kesadaran Terhadap *Cybersecurity*

Memahami *cybersecurity* adalah langkah awal untuk menjaga diri dan data pribadi dari berbagai ancaman siber. Dengan memahami konsep keamanan digital, siswa dapat:

a. Melindungi privasi dan data pribasi dari penyalahgunaan.
b. Mengenali ancaman siber yang sering terjadi, seperti phising, malware, ransomware, dan lainnya.
c. Menerapkan tindakan preventif untuk menjaga keamanan data saat menggunakan internet.

3.4 Jenis-Jenis Ancaman

Beberapa ancaman siber utama yang perlu diwaspadai, antara lain:

a. Phising, serangan yang berusaha mencuri informasi sensitif melalui pesan palsu.

APPA : Jurnal Pengabdian kepada Masyarakat
Volume 2, No. 4 Desember 2024
ISSN 3025-0889 (media online)
Hal 295-301

b. Malware, perangkat lunak berbahaya yang dapat merusak sistem atau mencuri data.
c. Ransomware, serangan yang mengenkripsi data korban dan meminta tebusan.
d. Social Engineering, manipulasi psikologis untuk mendapatkan akses ke informasi atau sistem.

Dengan memahami jenis-jenis ancaman ini, siswa dapat mengenali tanda-tanda serangan dan mengambil langkah preventif, seperti:

1. Menghindari membuka tautan atau lampiran dari sumber yang tidak dikenal.
2. Menggunakan kata sandi yang kuat dan unik.
3. Mengaktifkan firewall serta mempebarui perangkat lunak secara berkala.

4. KESIMPULAN

Kegiatan pengabdian kepada masyarakat ini dirancang untuk memberikan edukasi dan kesadaran kepada siswa SMK Muara Ilmu mengenai pentingnya keamanan data di era digital. Dalam rangkaian kegiatan yang interaktif dan menarik, siswa tidak hanya memperoleh pemahaman tentang ancaman siber seperti phishing, malware, dan ransomware, tetapi juga mempelajari langkah-langkah praktis untuk melindungi diri dari ancaman tersebut.

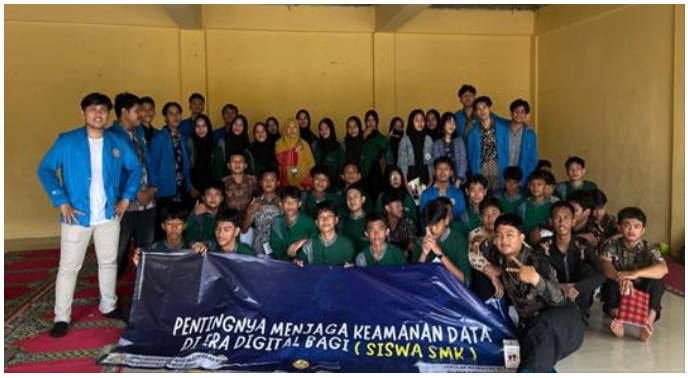
Melalui kegiatan sosialisasi, workshop, diskusi interaktif, simulasi, dan ice breaking, siswa diajak untuk lebih proaktif dalam menjaga keamanan data pribadi mereka. Dampak yang diharapkan meliputi peningkatan kesadaran, penguasaan keterampilan praktis, pembentukan budaya keamanan digital yang lebih baik, dan kontribusi positif terhadap literasi digital masyarakat. Tidak hanya bermanfaat bagi siswa, kegiatan ini juga membawa nilai tambah bagi SMK Muara Ilmu dengan memperkuat citra sebagai institusi pendidikan yang responsif terhadap tantangan zaman. Dalam jangka panjang, kegiatan ini diharapkan menjadi langkah awal dalam menciptakan generasi muda yang lebih sadar, tanggap, dan bertanggung jawab dalam menghadapi tantangan dunia digital yang semakin kompleks.

Kegiatan ini menegaskan pentingnya kolaborasi antara pendidikan formal dan nonformal untuk membangun komunitas digital yang aman, sekaligus membuka peluang untuk inovasi program-program serupa di masa depan.

UCAPAN TERIMA KASIH

1. Dosen pendamping: Ibu Kasih, S.Pd., M.Pd, atas bimbingan dan dukungan serta arahan yang telah diberikan selama proses penyusunan proposal dan pelaksanaan kegiatan ini.
2. Pihak SMK Muara Ilmu: terima kassih kepada Kepala Sekolah, Bapak Nuryadi dan seluruh Staf serta Siswa yang telah menerima dan berpartisipassi aktif dalam kegiatan sosialisasi ini.
3. Tim Pengabdi: rekan-rekan yang terlibat dalam kegiatan ini atas kerjasama, dedikasi dan komitmen yang tinggi untuk menyukseskan program ini.
4. Universitas Pamulang: atas dukungan dan fasilitass yang telah disediakan dalam rangka pelaksanaan kegiatan pengabdian kepada masyarakat ini.

Semoga kolaborasi yang telah terjalin dapat terus berlanjut dan memberikan manfaat bagi masyarakat, khususnya siswa SMK Muara Ilmu.



APPA : Jurnal Pengabdian kepada Masyarakat
Volume 2, No. 4 Desember 2024
ISSN 3025-0889 (media online)
Hal 295-301

REFERENCES

Digital Literacy Initiatives. *Improving Cybersecurity Awareness through Education Programs.*

Ghernaouti-Helie, S. (2009). *Cybersecurity, and Cyberwarfare: What Everyone Needs to Know.* Intenasional Telecommunication Union.

ISO/IEC 27032 (2012). *Guidelines for Cybersecurity.* International Organization for Standardization.

Kaspersky Lab. *Types of Cyber Threats.* Retrieved from https://www.kaspersky.com.

Microsoft Security Blog. *Phising Attacks and How to Prevent Them.* Retrieved from https://www.microsoft.com.

National Institute of Standards and Technology (NIST). (2014). *Framework for Improving Critical Infrastructure Cybersecurity.*

Stallings, W., & Brown, L. (2015). *Compuer Security: Principles and Practice.* Pearson.

Symantec Corporation. *The Internet security Threats Report.*

Verizon Data Breach Investigations Report (2021). *Cybersecurity Threats and Responses.*