

## **SOSIALISASI DAN EDUKASI KEAMANAN CYBER UNTUK SISWA CERDAS MENGELOLA DATA PRIBADI DI DUNIA MAYA**

### ***CYBER SECURITY AWARENESS AND EDUCATION FOR STUDENTS TO WISELY MANAGE PERSONAL DATA IN THE DIGITAL WORLD***

<sup>1</sup>Ari Putra, <sup>2</sup>Andri Fahmi, <sup>3</sup>Galuh Oka Safitri, <sup>4</sup>Raihan Pratama, <sup>5</sup>Fanza Yovian, <sup>6</sup>Hairia Sarfan, <sup>7</sup>Abdul Halim, <sup>8</sup>Mudiah Salsabella

<sup>1,2,3,4,5,6,7,8</sup>*Sistem Informasi, Fakultas Ilmu Komputer, Universitas Pamulang*

*email : dosen02815@unpam.ac.id, dosen02816@unpam.ac.id, dosen02818@unpam.ac.id, skwraihan123@gmail.com, fanzayovian06@gmail.com, riasarfan02@gmail.com, halim43201@gmail.com, mudiahsalsabella.s@gmail.com*

#### **ABSTRAK**

Pengabdian kepada masyarakat merupakan bentuk implementasi Tri Dharma Perguruan Tinggi. Di era digital saat ini, siswa sekolah menengah semakin aktif dalam penggunaan internet namun kurang memahami ancaman keamanan digital seperti phishing, malware, dan pencurian identitas. Kegiatan ini bertujuan memberikan edukasi dan sosialisasi keamanan siber kepada siswa-siswi Yayasan Maleo melalui seminar interaktif, praktik keamanan digital, dan diskusi kelompok. Hasil kegiatan menunjukkan peningkatan pemahaman siswa dalam mengelola data pribadi dan penggunaan teknologi digital secara aman. Kegiatan ini diharapkan menjadi langkah awal dalam membangun budaya literasi digital di kalangan pelajar.

**Kata Kunci:** Keamanan Siber, Edukasi Digital, Data Pribadi Siswa

#### **ABSTRACT**

*Community service is one form of implementing the Tri Dharma of Higher Education. In today's digital era, secondary school students are increasingly active in using the internet but lack awareness of digital security threats such as phishing, malware, and identity theft. This activity aims to provide cyber security education and awareness to Yayasan Maleo students through interactive seminars, digital security practices, and group discussions. The results show increased student understanding in managing personal data and using digital technology safely. This activity is expected to be an initial step in building a digital literacy culture among students.*

**Keywords:** Cyber Security, Digital Education, Personal Data Students

## **I. PENDAHULUAN**

Di era digital saat ini, internet telah menjadi bagian yang tidak terpisahkan dari kehidupan sehari-hari, terutama bagi generasi muda yang tumbuh dan berkembang bersamaan dengan kemajuan teknologi informasi. Siswa sekolah menengah semakin aktif dalam menggunakan berbagai platform digital, seperti media sosial, aplikasi perpesanan, platform pembelajaran online, dan game online. Namun, di balik kemudahan akses informasi dan komunikasi yang ditawarkan oleh teknologi digital, terdapat berbagai ancaman siber yang dapat membahayakan keamanan data pribadi, seperti pencurian identitas, peretasan akun, penyebaran hoaks, cyberbullying, penipuan online, malware, ransomware, hingga eksploitasi data pribadi untuk kepentingan komersial yang merugikan. Perkembangan teknologi

informasi yang pesat menuntut generasi muda untuk memahami serta waspada terhadap potensi ancaman siber ini. Yayasan Maleo, sebagai institusi pendidikan yang berlokasi di Jl. Palem Puri, Kampung Rawa Barat RT 004/RW 05 Kelurahan Pondok Pucung, Kecamatan Pondok Aren, Tangerang Selatan, menghadapi tantangan yang signifikan dalam memberikan pemahaman kepada siswanya mengenai pentingnya keamanan siber. Berdasarkan hasil observasi di Yayasan Maleo, ditemukan rendahnya pemahaman siswa terhadap keamanan data pribadi, lemahnya pengelolaan kata sandi, serta tingginya aktivitas media sosial tanpa pengamanan yang memadai. Ancaman seperti phishing, malware, cyberbullying, dan pencurian identitas menjadi isu nyata yang perlu ditangani dengan pendekatan edukatif.

Kondisi problematik ini menciptakan berbagai risiko serius yang dapat membahayakan siswa, baik dalam jangka pendek maupun jangka panjang. Dalam jangka pendek, siswa dapat menjadi korban penipuan online, kehilangan data pribadi, mengalami cyberbullying, atau bahkan menjadi target predator online. Dalam jangka panjang, kurangnya literasi keamanan siber dapat membuat mereka tidak siap menghadapi tantangan dunia kerja di era digital. Oleh karena itu, kegiatan pengabdian kepada masyarakat ini dirancang untuk menanamkan kesadaran akan pentingnya keamanan cyber sekaligus membekali siswa Yayasan Maleo dengan keterampilan praktis dalam menggunakan teknologi digital secara aman dan bertanggung jawab.

## **II. METODE PELAKSANAAN**

### **A. KERANGKA PEMECAHAN MASALAH**

Kerangka pemecahan masalah pada kegiatan ini dirancang secara sistematis untuk menjawab permasalahan rendahnya literasi keamanan digital di kalangan siswa. Tahapan yang dilakukan meliputi:

1. Analisis kebutuhan siswa dilakukan melalui observasi dan wawancara dengan pihak sekolah untuk mengidentifikasi sejauh mana pemahaman siswa terhadap ancaman digital dan praktik keamanan data pribadi.
2. Penyusunan materi edukasi berdasarkan hasil analisis, disesuaikan dengan kondisi dan tingkat pemahaman siswa, mencakup pengenalan cyber security, jenis ancaman siber, dan langkah perlindungan data pribadi.

3. Implementasi kegiatan berupa seminar, pelatihan teknis, dan diskusi interaktif guna menyampaikan materi secara menyeluruh sekaligus memberikan pengalaman langsung kepada siswa.
4. Evaluasi pasca kegiatan dilakukan untuk mengukur pemahaman siswa dan dampak kegiatan terhadap peningkatan kesadaran serta perubahan perilaku digital yang lebih aman.

## **B. REALISASI PEMECAHAN MASALAH**

Realisasi dari kerangka pemecahan masalah diwujudkan dalam bentuk kegiatan langsung yang menasar peningkatan kesadaran dan keterampilan siswa terkait keamanan digital. Kegiatan ini dilaksanakan dengan pendekatan partisipatif dan berorientasi pada praktik nyata, yang dijabarkan melalui tahapan berikut:

1. Pelaksanaan kegiatan Pengabdian Kepada Masyarakat dilaksanakan pada tanggal 27 Mei 2025 di Yayasan Maleo. Seminar ini menjadi sarana awal penyampaian materi secara umum kepada siswa.
2. Penyampaian materi dilakukan secara interaktif oleh tim narasumber yang terdiri dari dosen Universitas Pamulang dan mahasiswa, dengan pendekatan visual dan komunikasi dua arah agar mudah dipahami oleh peserta.
3. Pelatihan teknis diberikan kepada siswa, seperti praktik membuat kata sandi yang kuat, mengaktifkan autentikasi dua faktor (2FA), serta mengatur ulang pengaturan privasi pada akun media sosial.
4. Sesi diskusi interaktif diselenggarakan sebagai penutup kegiatan, yang memberi ruang bagi siswa untuk bertanya, berbagi pengalaman, dan mengeksplorasi lebih lanjut praktik keamanan digital dalam kehidupan sehari-hari.

## **C. SASARAN MASYARAKAT**

Khalayak sasaran dalam kegiatan Pengabdian Kepada Masyarakat ini adalah siswa-siswi Yayasan Maleo jenjang pendidikan menengah usia 13–18 tahun, yang aktif dalam penggunaan internet namun masih rentan terhadap ancaman siber. Meskipun sebagian besar sudah terbiasa menggunakan perangkat seperti smartphone dan laptop serta mengakses platform digital seperti Instagram, TikTok, dan WhatsApp, tingkat literasi keamanan digital mereka masih rendah, ditandai dengan minimnya pemahaman terhadap risiko siber dan kurangnya pengetahuan tentang perlindungan data pribadi.

#### **D. METODE KEGIATAN**

Metode kegiatan dalam program Pengabdian Kepada Masyarakat ini disusun secara terstruktur untuk memastikan penyampaian materi dapat diterima dengan baik oleh peserta dan berdampak nyata terhadap peningkatan pemahaman mereka. Pendekatan yang digunakan memadukan metode edukatif, praktis, dan partisipatif, sebagaimana dijelaskan berikut:

1. Metode ceramah digunakan untuk menyampaikan materi dasar mengenai keamanan cyber secara terstruktur. Penyampaian dilakukan melalui presentasi visual yang dilengkapi dengan diskusi dua arah, sehingga siswa dapat memahami konsep-konsep dasar secara menyeluruh dan dapat langsung mengajukan pertanyaan jika ada bagian yang kurang dipahami.
2. Sesi pelatihan bersifat praktik langsung yang mengajarkan siswa langkah-langkah teknis, seperti membuat kata sandi yang kuat, mengatur privasi akun media sosial, dan mengenali email phishing. Melalui metode ini, peserta dapat mengalami secara langsung bagaimana cara mengimplementasikan keamanan digital dalam kehidupan sehari-hari.
3. FGD dilakukan sebagai sesi evaluatif dan reflektif, di mana siswa didorong untuk mendiskusikan pemahaman mereka terhadap materi yang telah disampaikan, berbagi pengalaman, serta mengajukan pertanyaan lebih lanjut untuk memperdalam wawasan.
4. Kegiatan ini menggunakan pendekatan penelitian terapan, yaitu penelitian yang berorientasi pada pemecahan masalah nyata dengan menerapkan teknik dan metode tertentu. Tujuannya adalah menghasilkan solusi terhadap situasi dan fenomena terkait literasi keamanan digital di kalangan pelajar.
5. Variabel utama dalam kegiatan ini adalah siswa-siswi Yayasan Maleo sebagai subjek penerima manfaat. Fokusnya adalah meningkatkan kesadaran dan kemampuan mereka dalam menghadapi risiko ancaman digital serta membekali mereka dengan keterampilan praktis melindungi data pribadi.

### **III. HASIL DAN PEMBAHASAN**

#### **A. PENYAMPAIAN MATERI**

Pengenalan kesadaran keamanan cyber merupakan fondasi utama dari kegiatan Pengabdian Kepada Masyarakat yang memberikan pemahaman mendalam tentang keamanan digital saat ini. Kegiatan ini tidak hanya memberikan pemahaman dasar tentang pentingnya keamanan digital, tetapi juga mengeksplorasi secara komprehensif berbagai jenis ancaman siber yang dihadapi siswa dalam aktivitas digital sehari-hari, seperti yang ditampilkan pada Gambar 1.



Gambar 1. Penyampaian Materi

Kegiatan ini dimulai dengan pengenalan konsep dasar cyber security yang berasal dari dua kata dalam bahasa Inggris, yaitu "cyber" yang berarti dunia maya dan "security" yang berarti keamanan, seperti yang ditampilkan pada gambar 2.



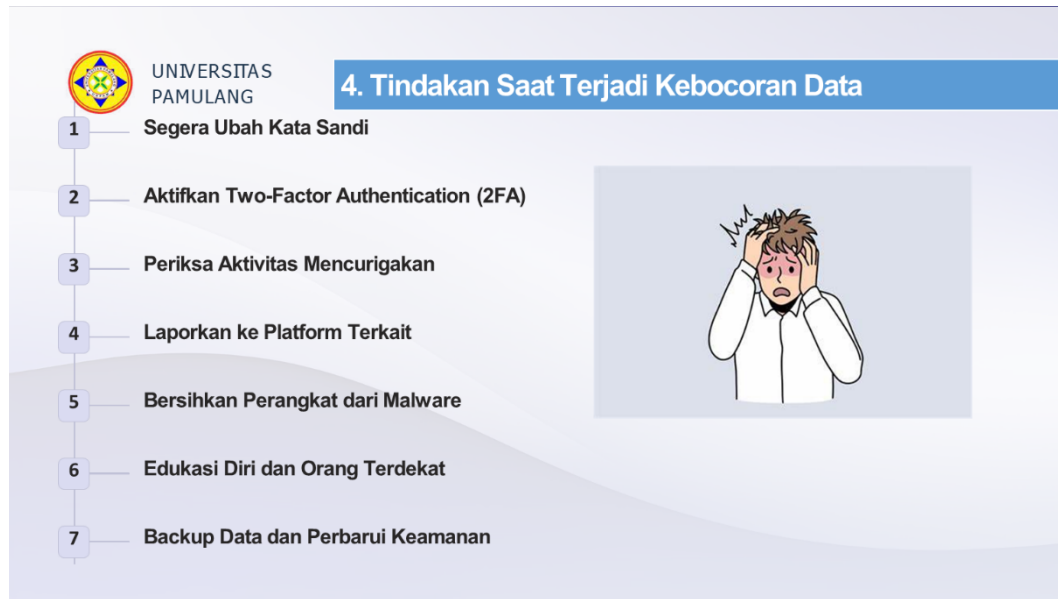
Gambar 2. Pengenalan Cyber Security

Selanjutnya kegiatan dilanjutkan dengan pembahasan mengenai berbagai ancaman cyber yang secara khusus mengintai pelajar seperti phishing dan penipuan online melalui pesan palsu yang mengaku dari sekolah atau platform populer, malware yang masuk melalui unduhan game atau aplikasi bajakan dari situs tidak terpercaya, serta pencurian identitas di mana data pribadi pelajar seperti nama, foto, dan NISN dapat disalahgunakan untuk membuat akun palsu atau aktivitas ilegal lainnya. Penjelasan disertai dengan contoh yang mudah dipahami oleh peserta, sehingga mereka dapat mengidentifikasi dan menghindari ancaman-ancaman tersebut dalam aktivitas digital mereka seperti yang ditunjukkan pada gambar 3.



Gambar 3. Ancaman Cyber Yang Mengintai Pelajar

Kegiatan selanjutnya fokus pada pembahasan tindakan-tindakan praktis yang harus dilakukan ketika terjadi kebocoran data. Tujuh langkah penting yang harus segera dilakukan, dimulai dari mengubah kata sandi, mengaktifkan two-factor authentication (2FA), memeriksa aktivitas mencurigakan, melaporkan ke platform terkait, membersihkan perangkat dari malware, mengedukasi diri dan orang terdekat, hingga melakukan backup data dan memperbarui sistem keamanan seperti yang ditunjukkan pada gambar 4.



Gambar 4. Tindakan Saat Terjadi Kebocoran Data

Pembahasan selanjutnya mengenai aspek etika digital dan keamanan dalam menggunakan sosial media. Pada kegiatan ini dijelaskan lima prinsip penting yang harus diterapkan, yaitu menghormati privasi orang lain dengan tidak membagikan data pribadi tanpa izin, bijak dalam membuat konten dengan menghindari penyebaran hoaks dan ujaran kebencian, mengatur privasi akun dengan mengaktifkan fitur keamanan seperti 2FA, melakukan interaksi yang sopan dan aman dengan menghindari cyberbullying, serta waspada terhadap penipuan dan akun palsu dengan melakukan verifikasi keaslian sebelum berinteraksi seperti yang ditunjukkan pada gambar 5.



Gambar 5. Etika Penggunaan Sosial Media



## B. PRAKTIK KEAMANAN DIGITAL

Kegiatan ini merupakan bentuk penerapan langsung dari materi seminar yang bertujuan melatih siswa dalam menerapkan langkah-langkah teknis untuk melindungi data pribadi di berbagai platform digital. Pelatihan mencakup tiga aspek utama, yaitu penggunaan aplikasi pengelola kata sandi, optimalisasi privasi media sosial melalui audit pengaturan akun di platform populer, serta aktivasi autentikasi multi-faktor menggunakan aplikasi seperti Google Authenticator. Melalui pendekatan ini, siswa dibekali keterampilan praktis untuk meningkatkan keamanan digital secara menyeluruh dalam kehidupan sehari-hari.

## C. SESI TANYA JAWAB

Setelah kegiatan praktik keamanan digital, kegiatan dilanjutkan dengan sesi diskusi dan tanya jawab yang berlangsung aktif dan penuh antusiasme. Peserta memanfaatkan kesempatan ini untuk mengklarifikasi materi, berbagi pengalaman pribadi terkait ancaman siber, serta mengajukan berbagai pertanyaan teknis maupun konseptual, seperti cara mendeteksi email phishing, mengamankan akun media sosial, dan membangun budaya sadar keamanan digital di lingkungan sekolah. Narasumber merespons setiap pertanyaan secara komprehensif disertai contoh praktis dan rekomendasi tools keamanan yang relevan. Untuk meningkatkan partisipasi, panitia menyediakan hadiah menarik bagi peserta yang paling aktif, menciptakan suasana meriah dan edukatif seperti yang ditampilkan pada gambar 2.



Gambar 2. Sesi tanya jawab



#### **IV. KESIMPULAN DAN SARAN**

##### **A. KESIMPULAN**

Berdasarkan hasil kegiatan yang telah dilaksanakan, dapat disimpulkan bahwa program edukasi keamanan siber ini memberikan dampak positif terhadap pemahaman dan perilaku digital siswa. Beberapa poin penting yang dapat disimpulkan antara lain:

1. Kegiatan berhasil meningkatkan pemahaman siswa mengenai berbagai ancaman siber, seperti phishing, malware, dan pencurian identitas.
2. Terdapat perubahan nyata dalam perilaku digital siswa, seperti mulai menggunakan autentikasi dua faktor dan membuat kata sandi yang lebih kuat.
3. Siswa menunjukkan peningkatan kesadaran dalam menjaga informasi pribadi di media sosial.
4. Antusiasme dan partisipasi aktif siswa mencerminkan efektivitas metode penyampaian yang digunakan dalam kegiatan ini.

##### **B. SARAN**

Untuk meningkatkan kesadaran dan pemahaman siswa mengenai pentingnya perlindungan data pribadi di era digital, disarankan untuk melaksanakan kegiatan Sosialisasi dan Edukasi Keamanan Cyber dengan tema "Siswa Cerdas Mengelola Data Pribadi di Dunia Maya". Kegiatan ini bertujuan agar para siswa dapat:

1. Mengenali risiko keamanan di dunia maya, seperti pencurian identitas, penipuan digital, dan peretasan akun.
2. Memahami pentingnya menjaga kerahasiaan data pribadi, termasuk informasi seperti alamat, nomor telepon, NISN, foto, dan data akun media sosial.
3. Menerapkan langkah-langkah perlindungan dasar, seperti membuat kata sandi yang kuat, menghindari tautan mencurigakan, dan menggunakan autentikasi dua faktor.
4. Mengembangkan sikap kritis dalam penggunaan teknologi, terutama saat berbagi informasi di platform digital dan media sosial.

Agar kegiatan ini memberikan dampak jangka panjang dan berkelanjutan, disarankan agar Yayasan Maleo mengintegrasikan materi keamanan siber ke dalam kurikulum sekolah, memberikan pelatihan rutin kepada guru, serta membentuk tim keamanan digital internal. Selain itu, kegiatan pelatihan dapat diperpanjang durasinya

agar materi lebih terserap, dan dan pembinaan budaya literasi digital yang kuat di lingkungan sekolah.

### DAFTAR PUSTAKA

- Aloul, F. A. (2012). The need for effective information security awareness. *Journal of Advances in Information Technology*, 3(4), 176–183.
- Cone, B. D., Irvine, C. E., Thompson, M. F., & Nguyen, T. D. (2007). A video game for cyber security training and awareness. *Computers & Security*, 26(1), 63–72.
- Hadlington, L. (2017). Human factors in cybersecurity: Examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviors. *Heliyon*, 3(7), e00346.
- Kowalski, R. M., Giumetti, G. W., Schroeder, A. N., & Lattanner, M. R. (2014). Bullying in the digital age: A critical review and meta-analysis of cyberbullying research among youth. *Psychological Bulletin*, 140(4), 1073–1137.
- Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications*, 22, 113–122.
- Sikorski, M., & Honig, A. (2012). *Practical malware analysis: The hands-on guide to dissecting malicious software*.
- Stallings, W., & Brown, L. (2018). *Computer security: Principles and practice* (4th ed.). Pearson.
- Suryani, L., Pratama, Y., & Wijayanto, A. (2019). Digital literacy among Indonesian students: A survey and recommendations. *Indonesian Journal of Educational Technology*, 8(2), 156–167.
- Yusuf, M., & Rachmawati, A. (2020). Pentingnya edukasi literasi digital dalam pembelajaran daring bagi siswa sekolah menengah. *Jurnal Pendidikan dan Teknologi Informasi*, 5(1), 45–52.
- Wibowo, A., & Santoso, H. B. (2021). Strategi edukasi keamanan siber untuk siswa sekolah dasar dan menengah di era digital. *Jurnal Pengabdian Masyarakat Informatika*, 3(2), 89–96.