

Meningkatkan Kewaspadaan Terhadap Kejahatan Cyber Di Era Digital Di SMK Negeri 8 Kabupaten Tangerang

Ilham Abdul Hakim¹, Fahri Alvyanto Pratama², Reza Ardian Sitorus³, Azis Firdaus⁴, Siti Fadilah Sari⁵, Sabila Fatimah Azzahra⁶, Dimas Yoga Pratama⁷, Fahrul Hidayat⁸, Suryaningrat⁹

¹Ilmu Komputer, Teknik Informatika, Universitas Pamulang, Tangerang Selatan, Banten, Indonesia
E-mail: : ^{1*}ilhamabdul257@gmail.com , ²fahriincredible@gmail.com , ³rezaardian251099@gmail.com ,
⁴azisfirdaus19@gmail.com , ⁵fadilahv0907@gmail.com , ⁶sabilahsasa@gmail.com , ⁷tnnafalj@gmail.com ,
⁸[fahruht1706@gmail.com](mailto:fahrulht1706@gmail.com) , ⁹d02362@unpam.ac.id

Abstrak - Kegiatan pengabdian kepada masyarakat adalah kegiatan yang mencakup upaya-upaya peningkatan kualitas pengetahuan antara lain dalam hal perluasan wawasan tentang kejahatan cyber. Remaja seringkali kurang memahami dampak dan risiko dari kejahatan siber, baik bagi diri sendiri maupun orang lain, sehingga perlu diberikan pengetahuan dan pemahaman yang benar tentang hal tersebut. Sehingga siswa/i SMK Negeri 8 Kabupaten Tangerang perlu keterampilan dan sikap yang positif dalam menghadapi kejahatan siber, seperti cara mencegah, mengantisipasi, melaporkan, dan menyelesaikan masalah yang timbul akibat kejahatan cyber. Pengabdian masyarakat di SMK Negeri 8 Kabupaten Tangerang ini di harapkan untuk berbagai aspek yang berkaitan dengan keamanan cyber di lingkungan sekolah. seperti peretasan akun, penyebaran konten berbahaya, atau pencurian data pribadi. Selain itu, kita juga akan membahas bagaimana kejahatan cyber dapat memengaruhi belajar dan pengajaran, serta bagaimana mengatasi tantangan tersebut. Selain melindungi siswa dari serangan cyber, penting juga untuk memberdayakan mereka dengan pengetahuan tentang cara berperilaku aman dan etika dalam penggunaan teknologi.

Kata Kunci: Sosialisasi, Kejahatan cyber, Pengabdian Kepada Masyarakat

Abstract - Community service activities are activities that include efforts to improve the quality of knowledge, among others, in terms of broadening horizons about cyber crime. Adolescents often lack understanding of the impact and risks of cybercrime, both for themselves and others, So it is necessary to be given the right knowledge and understanding about it. So that students of SMK Negeri 8 Tangerang Regency need positive skills and attitudes in dealing with cybercrime, such as how to prevent, anticipate, report, and solve problems arising from cyber crime.

Community service at SMK Negeri 8 Tangerang Regency is expected for various aspects related to cybersecurity in the school environment. such as account hacking, spreading malicious content, or stealing personal data. Moreover, We'll also discuss how cybercrime can affect learning and teaching, and how to address those challenges. In addition to protecting students from cyberattacks, it is also important to empower them with knowledge of how to behave safely and ethically in the use of technology.

Keywords: socialization, cybercrime, community service

1 PENDAHULUAN

Sekolah adalah tempat di mana generasi muda mengasah pengetahuan dan keterampilan mereka untuk menghadapi masa depan. Namun, di era digital yang terus berkembang, lingkungan sekolah tidak luput dari ancaman kejahatan cyber yang semakin serius. Keamanan cyber bukan lagi hanya tanggung jawab perusahaan atau pemerintah, sekolah dan institusi pendidikan juga harus menjaga diri dari serangan cyber yang berpotensi merusak. Anak-anak dan remaja yang tumbuh dewasa di era digital memiliki akses lebih besar ke teknologi daripada generasi sebelumnya. Mereka menggunakan perangkat seperti ponsel pintar, tablet, dan komputer untuk belajar, berkomunikasi, dan bermain. Namun, dengan kemudahan akses ini juga datang risiko kejahatan cyber yang bisa mengintai mereka di dunia maya. Oleh karena itu, penting bagi sekolah dan komunitas pendidikan untuk meningkatkan kewaspadaan terhadap kejahatan cyber.

Kejahatan cyber adalah segala aktivitas ilegal yang digunakan oleh pelaku kejahatan dengan menggunakan teknologi sistem informasi jaringan komputer yang secara langsung menyerang teknologi sistem informasi dari korban. Kejahatan cyber dapat dibedakan menjadi dua kategori, yaitu

kejahatan terhadap sistem komputer dan kejahatan yang menggunakan jaringan komputer (Widodo, 2009). Kejahatan dalam bidang komputer ini merupakan sisi gelap dari kemajuan teknologi yang mempunyai dampak sangat luas bagi seluruh sendi kehidupan modern ini (Maskun, 2013).

Berdasarkan data dari BSSN (Badan Sandi dan Siber Negara), sepanjang bulan Januari-agustus 2020, terdapat hampir 190 juta upaya serangan siber di Indonesia, naik empat kali lipat dibanding periode yang samapada tahun lalu hanya tercatat 39 juta (Henarti et al., 2015). Menurut data POLRI, bulan April 2020 setidaknya ada 937 kasus yang dilaporkan. Ada tiga kasus dengan angka tertinggi yaitu kasus Provocative, hate content and hate speech sebanyak 473, Penipuan online 259 kasus, dan Konten pornografi 82 kasus.

Ruang lingkup kejahatan siber menjadi sangat penting guna memberikan batasan, patut disadari bahwa perkembangan internet yang begitu cepat berbanding lurus dengan modus kejahatan yang muncul. Ada beberapa ruang lingkup kejahatan siber, yaitu: pembajakan, penipuan, pencurian, pornografi, pelecehan, pemfitnahan, dan pemalsuan (Bestari, n.d.).

Kejahatan siber secara persebaran mempunyai modus yang berbeda-beda dan seiring berjalannya waktu semakin beragam dan diperbarui modus operasinya, yang paling banyak digunakan adalah rekayasa sosial (social engineering) yakni kejahatan yang memanipulasi psikologi korban, baik disadari atau tidak agar melakukan tindakan tertentu yang menguntungkan pelaku. Media yang digunakan dalam social engineering seperti telepon, SMS, e-mail maupun berbagai media sosial (Rahardjo, 1976).

Upaya untuk mencegah dan menanggulangi peningkatan kejahatan siber ini perlu untuk dilakukan. Pemerintah, masyarakat dan semua stake holder yang ada harus bersama-sama memerangi kejahatan siber ini, karena sifat dari kejahatan siber sendiri yang berbahaya. Dalam kasus kejahatan siber, baik korban maupun pelaku tidak berhadapan langsung dalam satu tempat kejadian perkara (Golose, 2007).

Kegiatan siber meskipun bersifat virtual dapat dikategorikan sebagai tindakan dan perbuatan hukum yang nyata dalam transaksi dan aplikasi. Penggunaan hukum pidana teknologi komputer dalam mengatur masyarakat (lewat peraturan perundang-undangan pidana) pada hakikatnya merupakan bagian dari suatu langkah kebijakan (*policy*).

Dalam materi ini, kami akan menjelajahi berbagai aspek yang berkaitan dengan keamanan cyber di lingkungan sekolah. Kita akan memahami jenis-jenis serangan cyber yang mungkin mengancam sekolah, seperti peretasan akun, penyebaran konten berbahaya, atau pencurian data pribadi. Selain itu, kita juga akan membahas bagaimana kejahatan cyber dapat memengaruhi belajar dan pengajaran, serta bagaimana mengatasi tantangan tersebut. Selain melindungi siswa dari serangan cyber, penting juga untuk memberdayakan mereka dengan pengetahuan tentang cara berperilaku aman dan etika dalam penggunaan teknologi. Ini adalah keterampilan penting yang akan membantu mereka menghadapi tantangan dunia digital dengan bijak. Dalam materi ini, kami akan memberikan panduan praktis tentang bagaimana sekolah dan anggota komunitas pendidikan dapat bersama-sama meningkatkan kewaspadaan terhadap kejahatan cyber. Dengan langkah-langkah yang tepat, kita dapat menciptakan lingkungan sekolah yang aman dan mendukung pertumbuhan positif anak-anak dan remaja di era digital ini. Era digital akan terus berkembang dengan teknologi baru dan serangan cyber yang lebih kompleks. Perkembangan era digital juga merubah kebiasaan masyarakat menjadi serba instan dan cepat sehingga modus dari kejahatan siber semakin beragam. Jika masalah ini tidak diselesaikan, SMKN 8 mungkin akan kesulitan beradaptasi dengan ancaman-ancaman baru yang mungkin muncul kedepannya.

Siswa-siswa SMKN 8 Kabupaten Tangerang memiliki tingkat pengetahuan dan keterampilan teknologi yang beragam. Sebagian dari mereka mungkin telah memiliki pengalaman menggunakan komputer dan perangkat lunak. Terutama siswa yang SMK belajar di jurusan Teknik Komputer Jaringan (TKJ) yang pada dasarnya telah belajar dasar jaringan komputer. Pengalaman dan pengetahuan mengenai kejahatan cyber di kalangan siswa juga beragam, beberapa sudah pernah menjadi korban dan beberapa lagi masih

minim pengetahuan tentang kebiasaan yang dapat meningkatkan resiko menjadi korban kejahatan cyber.

Tujuan PKM ini adalah:

1. Meningkatkan Kewaspadaan Terhadap Kejahatan cyber: Bagaimana tingkat kewaspadaan terhadap kejahatan cyber di kalangan siswa SMKN 8 Kabupaten Tangerang saat ini, dan sejauh mana pemahaman mereka tentang ancaman tersebut?
2. Pengetahuan Tentang Cara Mengidentifikasi Tanda-tanda Serangan: Sejauh mana pengetahuan anggota komunitas SMKN 8 tentang cara mengidentifikasi tanda-tanda serangan cyber dan bagaimana hal tersebut dapat ditingkatkan.

2 METODE PELAKSANAAN

2.1 Tahap Kegiatan

Metode kegiatan yang digunakan kepada peserta merupakan metode pendidikan pedagogi karena peserta sebagian besar ialah sudah mempunyai pengetahuan mengenai topik yang dibahas. Berikut ini ialah tahap kegiatan yang akan dilakukan :

A. Tahapan Awal Kegiatan

- 1) Survei awal, tahapan ini dilakukan survei ke lokasi workshop yang berlokasi di SMK Negeri 8 Kabupaten Tangerang merupakan salah satu Sekolah Menengah Kejuruan favorit di daerah tersebut yang berada di Jl. Sarwani No.10, Tipar Raya, Kec. Jambé, Kabupaten Tangerang, Banten.
- 2) Setelah survei, ditetapkan lokasi pelaksanaan dan sasaran peserta
- 3) Penyusunan bahan ajar dan juga materi yang meliputi slide Power Point dan *hard copy* untuk peserta kegiatan

B. Tahapan Pelaksanaan Kegiatan

Tahapan ini akan diberi pemahaman kepada peserta kegiatan tentang Meningkatkan Kewaspadaan Terhadap Kejahatan cyber Di Era Digital serta memberikan gambaran tentang suasana dan aktivitas di dunia kampus. Penyuluhan dilaksanakan dengan metode sebagai berikut :

1. Sosialisasi

Metode ini dipilih guna memberikan penjelasan tentang materi Kewaspadaan Terhadap Kejahatan cyber Di Era Digital.

2. Diskusi dan Tanya Jawab

Metode ini digunakan agar merangsang daya pikir peserta untuk menceritakan pengalaman dan pengetahuannya di dalam ruang lingkup Cyber Security..awareness.

3. Quiz

Metode ini digunakan sebagai evaluasi pemahaman peserta dan memberikan umpan balik dari materi sosialisasi yang diberikan.

C. Tahapan Pasca Kegiatan

Tahap ini akan disusun laporan dari hasil kegiatan yang telah didapatkan dari peserta untuk mempertanggungjawabkan dari kegiatan dan untuk keperluan publikasi.

2.2 Roundown Acara

Hari/Tanggal : Kamis, 23 November 2023

Lokasi : SMKN 8 Kabupaten Tengerang

Tabel 1. Roundown Acara

Waktu	Kegiatan	Keterangan
07:45-08:00	Persiapan sosialisasi	Panitia
08:00-08:10	Pembukaan dan sambutan	Perwakilan dosen, guru, dan ketua pelaksana
08:10-09:15	Materi “Meningkatkan kewaspadaan terhadap kejahatan siber”	Pemateri
09:15-09:30	Diskusi dan tanya jawab	Moderator
09:30-09:45	Quiz dan pembagian souvenir	Panitia
09:45-10:00	Penutup dan sesi foto bersama	Ketua pelaksana, dan seksi dokumentasi

2.3 Susunan Panitia

Adapun Susunan Kepanitiaan dalam kegiatan PKM ini sebagai berikut:

1. Ketua pelaksana : Ilham Abdul Hakim
2. Pemateri : - Reza Ardian Sitorus
- Azis Firdaus
3. Games dan Quiz : - Siti Fadilah Sari
- Sabila Fatimah Azzahra
4. Dokumentasi : - Dimas Yoga Pratama
- Fahrul Hidayat
5. Moderator : Fahri Alyyanto Pratama

3 ANALISA DAN PEMBAHASAN

Hasil yang di dapat dari pelaksanaan kegiatan PKM ini adalah siswa/siswi SMKN 8 Kabupaten Tangerang menjadi faham tentang apa itu kejahatan cyber dan cara mengatasi nya, sehingga mereka mampu mengatasi apabila terjadi kebocoran data.

Gambar di bawah antusias siswa/siswi saat mengikuti pelaksanaan Kegiatan Pengabdian Kepada Masyarakat.



Gambar 1. Antusias siswa/siswi saat penyampaian materi

Dari Gambar 1 di atas tampak bahwa siswa/siswi sangat antusias mendengarkan materi di kegiatan PKM ini, karena kegiatan ini dapat menambah wawasan siswa/siswi terhadap kejahatan cyber.



Gambar 2. Pembagian Hadiah Quiz

Dalam Gambar 2 di atas pembagian hadiah Quiz dalam menjawab pertanyaan/bertanya yang di berikan, sebagai bentuk mengapresiasi karena telah antusias dalam mendengarkan materi.

Berdasarkan kegiatan PKM yang telah di kalsanakan pada hasil di atas, Siswa-siswa SMKN 8 Kabupaten Tangerang menunjukkan minat dalam mempelajari kejahatan cyber yang sering baru-baru ini dan sering dialami masyarakat. Banyak dari mereka bercerita mengenai pengalam pribadi

mereka menjadi korban kejahatan siber dan berbagi pengalaman dengan teman sekelasnya agar kejadian yang sama tidak terjadi pada orang lain.

Tampak pada gambar 3 di bawah ini Mahasiswa, dan siswa/siswi berfoto Bersama menandakan kegiatan PKM sudah selesai di laksanakan



Gambar 3. Foto Bersama Siswa SMKN 8 Kabupaten Tangerang



Gambar 4. Penyerahan Plakat Kepada Perwakilan Sekolah SMKN 8 Kabupaten Tangerang

4 KESIMPULAN

Berdasarkan hasil Pengabdian Kepada Masyarakat yang telah dilaksanakan, didapatkan hasil bahwa para peserta dapat menyerap pembelajaran terkait meningkatkan kewaspadaan terhadap kejahatan siber peserta antusias menyimak dan berbagi pengalaman mereka menghadapi kejahatan siber dengan teman sekelasnya. Siswa juga aktif dalam mempraktekan pengecekan kesehatan akun email mereka.

Pada umumnya, istilah *cyber crime* merujuk terhadap suatu tindakan kejahatan yang berhubungan dengan dunia maya (*cyberspace*) serta perilaku yang memakai komputer (Mansur & Gultom, 2009).

UCAPAN TERIMAKASIH

Terimakasih kepada

1. Ketuan LPPM Universitas Pamulang
2. Dekan Universitas Pamulang
3. Ketua Program Studi Teknik Informatika Universitas Pamulang
4. Bapak Dosen Pembimbing Teknik Informatika Universitas Pamulang
5. Mahasiswa Teknik Informatika Universitas Pamulang
6. Siswa/Siswi, para guru SMK Negeri 8 Kabupaten Tangerang

REFERENCES

- Alhakim, A. (2021). *Kajian normatif penanganan cyber crime di sektor perbankan di indonesia* (Vol. 4, Nomor 2). <https://doi.org/https://doi.org/10.23887/jatayu.v4i2.38089>
- Fitriani, Y., & Pakpahan, R. (2020). Analisa penyalahgunaan media sosial untuk penyebaran cybercrime di dunia maya atau cyberspace. *Cakrawala-Jurnal Humaniora*, 20. <https://doi.org/10.31294/jc.v19i2>
- Parulian, S., Pratiwi, D. A., & Cahya Yustina, M. (2021). *Ancaman dan solusi serangan siber di indonesia*. <https://doi.org/https://doi.org/10.17509/telnect.v1i2.40866>
- Suharto, M. A., & Apriyani, M. N. (2021). Konsep cyber attack, cyber crime, dan cyber warfare dalam aspek hukum internasional. Dalam *Risalah Hukum* (Vol. 17, Nomor 2). <https://doi.org/https://doi.org/10.30872/risalah.v17i2.705>
- Ubaidillah, D. N. K. A., & Ruth Vanya Octaviany. (2022). Kejahatan cybercrime di era 4.0. Dalam *Universitas Negeri Surabaya* (Vol. 2022). <https://proceeding.unesa.ac.id/index.php/sniis/article/view/133>
- Umbara, A., & Setiawan, D. A. (2022). Analisis kriminologis terhadap peningkatan kejahatan siber di masa pandemi covid-19. *Jurnal Riset Ilmu Hukum*, 81–88. <https://doi.org/10.29313/jrih.v2i2.1324>
- Widya, N., Dosen, S. ", Pamulang, U., Surya Kencana, J., Pamulang, S., & Selatan, T. (2018). Kejahatan cyber dalam perkembangan teknologi informasi berbasis komputer. Dalam *Jurnal Surya Kencana Dua: Dinamika Masalah Hukum dan Keadilan* (Vol. 5). <https://doi.org/http://dx.doi.org/10.32493/SKD.v5i2.v2018.2339>