Pelatihan Basic Cyber Security untuk Siswa MA/Sederajat di Kabupaten Batang

Fauzi Adi Rafrastara[1], Wildanil Ghozi[2], Ramadhan Rakhmat Sani[3]
[1,2]Program Studi Teknik Informatika, Universitas Dian Nuswantoro
[3]Program Studi Sistem Informasi, Universitas Dian Nuswantoro
E-mail: [1]fauziadi@dsn.dinus.ac.id, [2]wildanil.ghozi@dsn.dinus.ac.id,
[3]ramadhan_rs@dsn.dinus.ac.id

Abstrak

Teknologi informasi telah menjadi bagian dari kehidupan masyarakat modern dengan pertumbuhan pengguna yang pesat. Setiap orang menggunakan gadget untuk berkomunikasi dan mengakses berbagai informasi setiap hari. Kejahatan siber merupakan salah satu dampak negatif yang paling berbahaya yang menargetkan para pengguna teknologi informasi dan dapat menargetkan individu menjadi korban. Pemerintah memiliki tanggung jawab untuk melindungi masyarakat terhadap kejahatan siber yang menargetkan individu. Oleh karena itu, pemerintah perlu memahami berbagai skema serangan dan trend perkembangan kejahatan siber. Dengan pengetahuan skema-skema serangan yang mungkin digunakan pada kejahatan siber, maka pemerintah dapat memberikan edukasi yang tepat bagi masyarakat. Balai Pengembangan Sumber Daya Manusia dan Penelitian (BPSDMP) Komunikasi dan Informatika Yogyakarta merupakan salah satu lembaga pemerintah yang bertanggung jawab dalam meningkatkan kemampuan masyarakat dalam pemanfaatan teknologi di wilayah Jawa Tengah dan Yogyakarta termasuk di Kabupaten Batang. Universitas Dian Nuswantoro sebagai institusi pendidikan yang unggul dalam bidang teknologi informasi dan komunikasi, berkolaborasi dengan BPSDMP KOMINFO Yogyakarta untuk memberikan pelatihan basic cyber security untuk siswa SMA/sederajat di Kabupaten Batang. Pelatihan berupa penjelasan materi teori dan praktik implementasi keamanan siber. Pada akhir sesi pelatihan, sebanyak 37 dari 39 siswa peserta pelatihan dinyatakan berhasil.

Kata kunci: pelatihan, keamanan siber, teknologi informasi

Abstract

Information technology has become part of modern society with rapid user growth. Everyone uses gadgets to communicate and access various information every day. Cybercrime is one of the most dangerous negative impacts that targets information technology users and can target individuals as victims. Therefore, the government needs to understand the various attack schemes and development trends of cybercrime. By knowing the attack schemes that might be used in cybercrime, the government can provide appropriate education to the public. Balai Pengembangan Sumber Daya Manusia dan Penelitian Komunikasi dan Informatika (BPSDMP KOMINFO) Yogyakarta *is one of the government institutions responsible for increasing the community's ability to use technology in the Central Java and Yogyakarta regions, including Batang Regency. Universitas Dian Nuswantoro, as an educational institution that excels in the field of information and communication technology, collaborates with BPSDMP KOMINFO Yogyakarta to provide basic cyber security training for high school students in Batang Regency. The training takes the form of explaining theoretical material and practical implementation of cyber security. At the end of the training session, 37 of the 39 students participating in the training were declared successful.*

Keywords: basic training, cyber security, information technology

1. PENDAHULUAN

Teknologi informasi dan komunikasi telah menjadi bagian dari kehidupan masyarakat modern, dengan pertumbuhan pengguna yang pesat. Setiap orang menggunakan gadget untuk berkomunikasi dan mengakses berbagai informasi setiap hari. Hal tersebut berdampak baik bagi perkembangan sosial, ekonomi, dan ilmu pengetahuan [1], [2]. Namun, dampak negatif juga muncul mengiringi hal tersebut. Masalah mental health issue, cyber bullying, cybercrime, dan masalah-masalah lainnya [3]. Masyarakat harus mampu memanfaatkan teknologi informasi dengan sebaik-baiknya, sembari menghindari efek negatif yang ditimbulkan.

Kejahatan siber merupakan salah satu dampak negatif yang paling berbahaya. Kejahatan siber merupakan istilah yang digunakan untuk menggambarkan secara luas, aktivitas kriminal yang dilakukan melalui komputer dan jaringan internet mencakup segala peretasan elektronik hingga serangan mematikan sebuah layanan [4]. Beberapa kategori kejahatan siber antara lain *cyber terorism, cyber warfare, cyber espionage, child pornography, denial of service, cyber bullying,* dan *phishing* [5]. Kejahatan yang dilakukan melalui teknologi dunia maya dapat menargetkan individu seperti serangan *phising* dan *cyber bullying* [2]. *Phising* merupakan salah satu serangan yang paling populer yang menargetkan pengguna secara langsung. Tujuan dari serangan ini adalah untuk memanipulasi user untuk mengirimkan informasi sensitif seperti nomor rekening, data pribadi, dan nomor kartu [6]. *Phishing* dilakukan dengan menjebak seseorang untuk atau memancing seseorang melalui halaman web palsu [7]. Kebanyakan siswa mampu bertanggung jawab dalam menggunakan teknologi, namun sebagian menggunakannya tanpa kepedulian dan tidak bijak menggunakannya untuk melakukan ancaman, intimidasi, menyakiti, mempermalukan, dan menyerang harga diri orang lain itulah yang dinamakan dengan *cyber bullying* [8], [9].

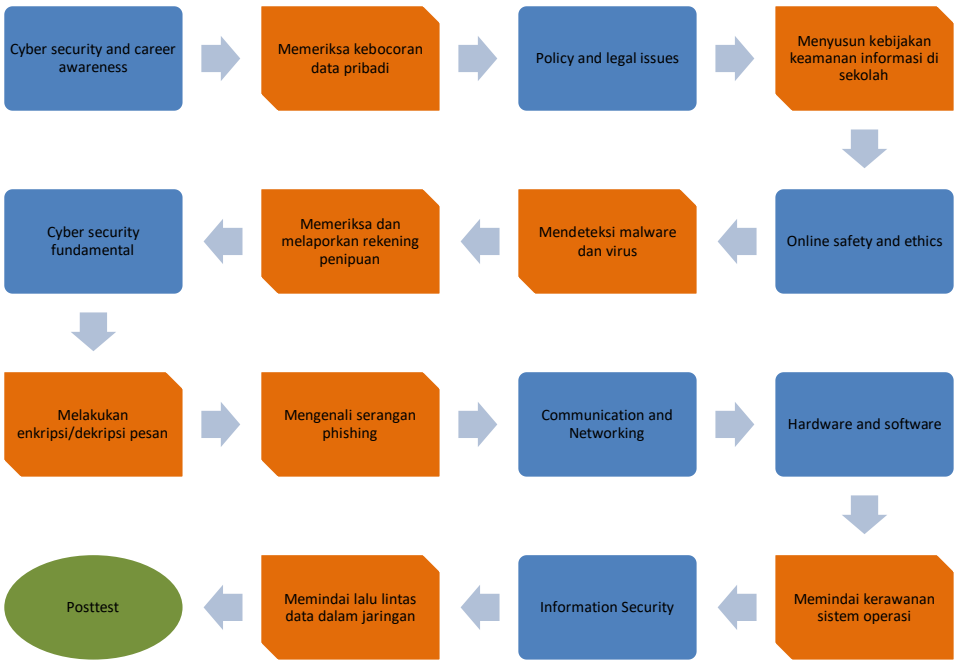
Pemerintah memiliki tanggung jawab untuk melindungi masyarakat terhadap kejahatan siber yang menargetkan individu. Indonesia telah menetapkan beberapa kebijakan untuk menjaga keamanan siber, melalui undang-undang perlindungan data pribadi (UU PDP) dan undang-undang informasi dan transaksi elektronik (UU ITE). Selain kedua undang-undang tersebut, peraturan pemerintah dan undang-undang lain yang juga telah diterbitkan sebagai dasar hukum keamanan siber di Indonesia [10]. Namun penggunaan dari undang-undang tersebut belum maksimal, sehingga masih banyak terjadi kasus kejahatan siber di Indonesia [11].

Serangan siber yang berhasil, seringnya terjadi karena kurangnya edukasi dari korban yang menjadi target serangan. Untuk menanggulangi hal tersebut, maka pemerintah perlu meningkatkan edukasi terhadap masyarakat tentang cara melindungi privasi dan data pribadi di dunia maya [12]. Pemerintah perlu memahami berbagai skema serangan dan trend perkembangan kejahatan siber yang menargetkan individu [13]. Dengan pengetahuan skema-skema serangan yang mungkin digunakan pada kejahatan siber, maka pemerintah dapat memberikan edukasi yang tepat bagi masyarakat.

Kabupaten Batang merupakan salah satu wilayah yang masuk dalam tanggung jawab BPSDMP KOMINFO Yogyakarta untuk diberikan edukasi terkait penggunaan dan pemanfaatan perangkat teknologi informasi, terutama dalam bidang keamanan siber. Masyarakat harus mengetahui bagaimana pemanfaatan teknologi informasi yang baik dan melindungi keamanan data pribadi. Siswa SMA tergolong kelompok umur remaja, dimana salah satu karakternya adalah memiliki semangat yang tinggi. Pada masa-masa tersebut, umumnya mereka juga mulai memiliki kebebasan dalam menjalankan aktivitas sehari-hari. Tak terkecuali juga dalam menggunakan perangkat teknologi seperti smartphone, laptop, dan sebagainya. Keterampilan dalam menggunakan perangkat teknologi informasi tidak hanya pada pemanfaatannya saja, namun juga pada pengamanan pengguna dan pengamanan data yang dikelola oleh setiap orang. Untuk itu, para siswa SMA sebagai pengguna teknologi informasi perlu mendapatkan pelatihan tentang keamanan siber. Pelatihan bertujuan untuk memberikan pemahaman dasar konsep keamanan informasi dan menerapkan keamanan informasi kepada diri sendiri dan lingkungan sekolah. Peserta juga diberikan pelatihan untuk mengenali serangan-serangan siber yang menargetkan dirinya dan perangkat teknologi informasi yang digunakannya.

2. METODE

Pelatihan *basic cyber security* untuk siswa SMA/Sederajat di Kabupaten Batang diadakan dalam dua hari dengan target peserta adalah siswa-siswi SMA dan SMK yang berlokasi di Kabupaten Batang. Pelatihan diberikan dengan metode penyampaian teori-teori tentang keamanan informasi, komunikasi data dalam jaringan komputer, dan jenis-jenis serangan. Metode praktik menganalisis kerentanan dan serangan serta menerapkan instrumen keamanan informasi juga diberikan untuk menguatkan pemahaman peserta. Detail susunan metode pelatihan diilustrasikan pada gambar 1 berikut.



Gambar 1. Metode pelatihan

Materi pembuka adalah tentang *cyber security and career awareness* diberikan untuk memberikan pemahaman kondisi keamanan siber di Indonesia. Berbagai kasus-kasus kejahatan siber yang baru saja terjadi beberapa tahun terakhir digunakan sebagai contoh untuk membangun kesadaran peserta terhadap pentingnya kepedulian terhadap keamanan siber, terutama dalam melindungi diri sendiri. Berbagai contoh kasus yang sering dialami sehari-hari juga didiskusikan. Beberapa contoh yang dialami peserta seperti pesan singkat berisi undian berhadiah, telpon dari orang tidak dikenal, serta penipuan bermodus toko online. Selain itu, materi pembuka ini juga membahas tentang karir di bidang keamanan siber untuk meningkatkan minat peserta dalam belajar dan meniti karir di bidang ini sehingga meningkatkan jumlah praktisi keamanan siber di masa depan.

Praktikum pertama dilakukan berkaitan dengan insiden kejahatan siber yang marak terjadi dan menargetkan para peserta. Untuk meningkatkan pemahaman peserta terhadap privasi data yang mungkin saja telah terekspos ke internet, maka peserta diajarkan untuk memeriksa datanya masing-masing dan memastikan data pribadinya tidak terekspos di internet. Peserta juga diajarkan langkah-langkah yang perlu dilakukan jika data pribadinya sudah terlanjur terekspos di internet.

Pada materi *policy and legal issues*, peserta diperkenalkan dengan produk hukum dan aturan-aturan lain yang telah ditetapkan oleh pemerintah dan lembaga-lembaga penyedia layanan di internet. Peserta diajak untuk menganalisis aturan yang sudah ada, baik kelebihan maupun kelemahannya. Berkaitan dengan materi *online safety and ethics*, peserta diajarkan untuk menggunakan teknologi informasi dengan bijak. Menjaga diri dari tindakan-tindakan yang

melanggar undang-undang pada saat menggunakan teknologi informasi. Peserta juga diajak untuk membuat aturan-aturan yang dapat digunakan untuk meningkatkan keamanan dan privasi data siswa di sekolah sebagai bentuk praktik implementasi aturan keamanan dan etika dalam bersosial media.

Maraknya kasus pencurian data rekening melalui aplikasi malware yang dialami oleh masyarakat harus diatasi dengan pelatihan mendeteksi malware dan virus yang mudah bagi masyarakat umum. Oleh karena itu peserta diajarkan untuk mendeteksi sebuah aplikasi atau file merupakan file yang aman atau tidak. Peserta hanya perlu memasukkan file tersebut pada web aplikasi virustotal untuk kemudian scan otomatis perilaku dari file atau aplikasi tersebut. Peserta juga mempraktikan deteksi rekening penipuan online dengan melalui web cekrekening.id yang telah disediakan oleh kementerian KOMINFO, sehingga dapat mencegah para peserta menjadi korban penipuan bermodus toko online.

Cyber security fundamental mengajarkan kepada peserta untuk memahami konsep keamanan siber secara umum. Teknik-teknik yang dapat digunakan untuk mengamankan data dan lalu lintas data dalam jaringan. Para peserta diajarkan untuk memahami dan membedakan kerawanan sistem dan ancaman yang dapat membahayakan sistem. Peserta juga diajarkan untuk menemukan solusi yang tepat jika ditemukan kerawanan dalam sistem. Praktik melakukan enkripsi dan dekripsi data dilakukan dengan menggunakan algoritma AES dan DES untuk memberikan pengalaman langsung kepada peserta bagaimana cara mengamankan data. Peserta juga diberikan latihan untuk mengenali serangan-serangan phishing dengan praktek secara langsung studi kasus serangan phishing.

Untuk dapat memahami sepenuhnya bagaimana modus-modus kejahatan siber bekerja, maka peserta juga perlu memahami bagaimana komputer dan jaringan internet bekerja. Oleh karena itu, maka materi *communication and networking* perlu diberikan kepada peserta. Peserta juga harus mengetahui apa saja dan bagaimana perangkat jaringan baik hardware maupun software bekerja. Mendeteksi celah-celah keamanan pada perangkat jaringan akan sangat membantu peserta untuk melindungi keamanan perangkat yang digunakannya.

Materi terakhir yang dibahas pada pelatihan ini adalah *information security*, untuk memberikan pemahaman menyeluruh kepada peserta cara mengamankan informasi dan sistem informasi yang digunakan. Praktik menguji keamanan protokol jaringan diberikan kepada peserta supaya dapat membedakan kondisi jaringan yang aman dan yang tidak aman.

Pada akhir sesi pelatihan, posttest diberikan kepada peserta untuk mengukur keberhasilan dari pelatihan yang diberikan kepada peserta.

3. HASIL DAN PEMBAHASAN

Pelatihan diadakan pada tanggal 14 dan 15 Mei 2024 di SMP Negeri 3 Batang. Pelatihan diikuti oleh 39 peserta yang dibagi ke dalam dua kelas yaitu kelas A dan kelas B dengan masing-masing berjumlah 20 dan 19 peserta. Seluruh peserta menghadiri pelatihan dan mengikuti materi dari awal hingga akhir.

Keamanan siber merupakan topik pembahasan yang baru bagi para peserta. Sebelumnya peserta hanya mendapat informasi-informasi umum melalui sosial media, tentang insiden siber yang terjadi. Hal tersebut meningkatkan motivasi para peserta dalam mengikuti materi pelatihan. Setiap topik pembahasan pada sesi teori diberikan penjelasan mendetail materi yang sedang dibahas, kemudian dilanjutkan dengan sesi diskusi. Sesi diskusi diberikan bertujuan untuk membangkitkan suasana pelatihan yang interaktif. Para peserta diajak untuk menceritakan insiden berkaitan dengan topik pembahasan yang pernah dialaminya. Umumnya para peserta baru menyadari bahwa pengalaman-pengalaman tersebut merupakan keadaan yang membahayakan keamanan data pribadi mereka.

Sebagian dari peserta pernah menjadi korban kejahatan siber. Kejadian paling umum adalah sms dan pesan singkat berisi undian berhadiah palsu. Hal ini cukup mudah untuk dihindari oleh para peserta. Sebagian peserta, pernah menderita kerugian hingga ratusan ribu melalui skema toko online palsu. Para peserta tersebut tidak memiliki kemampuan untuk membedakan antara

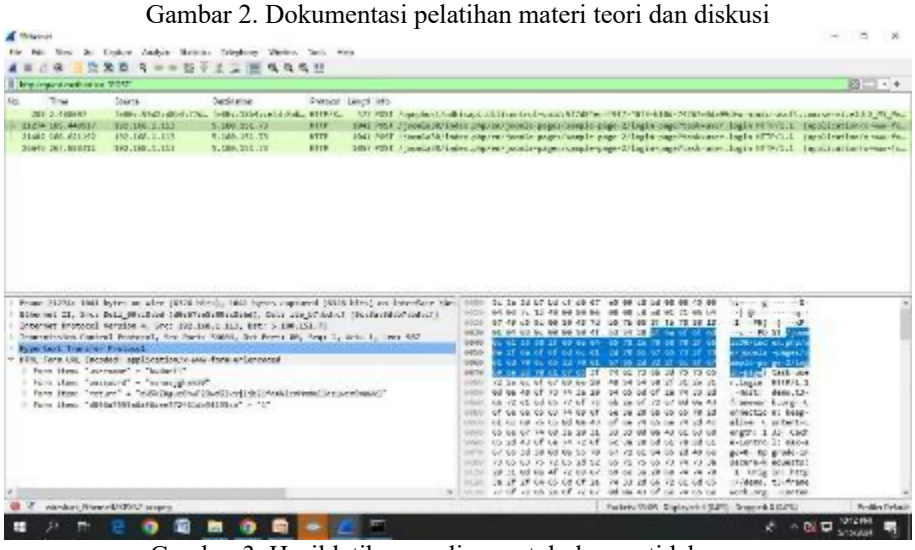
toko online asli dan toko online palsu karena belum pernah dibekali dengan pengetahuan keamanan siber. Kasus lain yang pernah dialami peserta adalah telepon tidak dikenal yang membujuk untuk mengirimkan kode *one time password* (OTP) kepada penelepon. Beberapa kasus lain yang pernah dialami peserta seperti serangan *malware, phishing*, dan *social engineering*.

Berbagai kasus kejahatan siber yang telah dialami peserta dapat dijadikan studi kasus yang nyata tentang bahayanya kejahatan siber. Para peserta yang saling berbagi pengalaman, juga diberikan pemahaman untuk mengenali serangan-serangan siber serupa di masa depan.

Materi-materi praktikum diberikan kepada peserta untuk mempraktikkan secara langsung usaha untuk mengenali serangan-serangan siber yang menargetkan dirinya. Peserta juga diajarkan untuk melakukan pengujian hardware, software, maupun jaringan komputer yang untuk mendeteksi kerawanan pada sistem komputer yang digunakannya. Selain itu, praktikum juga memberikan pengalaman peserta secara langsung untuk menerapkan instrumen keamanan sehingga mencegah keberhasilan dari para pelaku kejahatan siber.

Dokumentasi kegiatan pelatihan ditunjukan pada gambar 2, gambar 3 dan gambar 4. Pada gambar 2 menunjukan kegiatan penyampaian materi teori dan diskusi dengan para peserta. Gambar 3 menunjukan hasil latihan siswa dalam menganalisa protokol jaringan komputer yang tidak aman untuk digunakan. Gambar 4 menunjukan foto para peserta di kelas B bersama dengan narasumber.

Gambar 2. Dokumentasi pelatihan materi teori dan diskusi



Gambar 3. Hasil latihan analisa protokol yang tidak aman

Gambar 4. Foto para peserta di kelas B bersama dengan narasumber

Setelah semua sesi pelatihan berakhir, peserta diberikan posttest untuk mengukur tingkat pemahaman peserta. Selain itu, peserta juga diberikan tugas untuk menyelesaikan studi kasus keamanan siber sebagai pengukuran kemampuan praktik peserta. Penilaian *posttest*, dan tugas peserta menjadi dasar untuk kelulusan dan penerbitan sertifikat kelulusan pelatihan. Hasil dari penilaian peserta ditunjukan pada tabel 1.

Tabel 1. Penilaian kelulusan peserta

Kelas	No Urut	Kehadiran	Posttest	Tugas	Nilai Akhir	Keterangan
A	1	100	80	100	88,00	Lulus
A	2	100	83	90	86,30	Lulus
A	3	100	80	95	86,25	Lulus
A	4	100	87	95	90,45	Lulus
A	5	100	87	85	86,95	Lulus
A	6	100	83	95	88,05	Lulus
A	7	100	85	95	89,25	Lulus
A	8	100	83	85	84,55	Lulus
A	9	100	86	95	89,85	Lulus
A	10	100	89	100	93,40	Lulus
A	11	100	86	100	91,60	Lulus
A	12	100	89	100	93,40	Lulus
A	13	100	79	95	85,65	Lulus
A	14	100	89	80	86,40	Lulus
A	15	100	88	100	92,80	Lulus
A	16	100	85	100	91,00	Lulus
A	17	100	87	70	81,70	Lulus
A	18	100	79	90	83,90	Lulus
A	19	100	87	90	88,70	Lulus
A	20	100	87	80	85,20	Lulus
B	1	100	100	92	95,00	Lulus
B	2	100	85	93	90,75	Lulus
B	3	100	95	90	92,25	Lulus
B	4	100	100	90	94,00	Lulus
B	5	100	100	93	96,00	Lulus
B	6	100	80	33	53,00	Lulus
B	7	100	70	0	29,50	Tidak Lulus
B	8	100	80	85	84,00	Lulus

B	9	100	80	33	53,00	Tidak Lulus
B	10	100	100	62	77,00	Lulus
B	11	100	100	88	93,00	Lulus
B	12	100	95	60	74,25	Lulus
B	13	100	95	87	90,25	Lulus
B	14	100	100	58	75,00	Lulus
B	15	100	100	87	92,00	Lulus
B	16	100	95	88	91,25	Lulus
B	17	100	100	33	60,00	Lulus
B	18	100	100	90	94,00	Lulus
B	19	100	90	85	87,50	Lulus

Untuk memperoleh sertifikat kelulusan, para peserta harus memperoleh nilai akhir minimal skor 60. Nilai tersebut diperoleh dari kehadiran dengan bobot 5%, penilaian *posttest* dengan bobot 35%, dan tugas dengan bobot 60%. Berdasarkan penilaian pada tabel 1, sebanyak 37 dari 39 peserta dinyatakan lulus pelatihan sehingga dapat dinyatakan bahwa persentase kelulusan peserta sebesar 94,87%.

4. KESIMPULAN DAN SARAN

Pelatihan basic cyber security untuk siswa SMA/sederajat di Kabupaten Batang telah dilaksanakan sesuai dengan metode yang telah disusun. Kegiatan pelatihan dilaksanakan sesuai jadwal dan dihadiri oleh seluruh peserta yang telah terdaftar. Setelah pelatihan dilaksanakan dan penilaian dilakukan terhadap peserta, dapat disimpulkan bahwa pemahaman peserta terhadap keamanan siber sudah baik. Sebanyak 37 peserta sudah mampu melindungi data pribadi, mengenali serangan siber, dan menerapkan instrumen keamanan siber. Hal tersebut dibuktikan dengan penilaian posttest dan tugas yang diberikan kepada peserta.

Kegiatan pelatihan ini dibutuhkan bagi masyarakat umum, terutama siswa SMA/sederajat yang dikategorikan sebagai pengguna baru teknologi informasi. Namun pelatihan ini hanya mampu diberikan kepada peserta dengan jumlah terbatas. Kami memberikan saran supaya kegiatan pelatihan ini dapat ditingkatkan lagi untuk jumlah peserta yang lebih banyak. Sehingga semakin banyak siswa yang teredukasi untuk mampu melindungi keamanan data pribadinya.

DAFTAR PUSTAKA

[1] H. Djanggih and N. Qamar, "Penerapan Teori-Teori Kriminologi dalam Penanggulangan Kejahatan Siber (Cyber Crime)," *pandecta*, vol. 13, no. 1, pp. 10–23, Aug. 2018, doi: 10.15294/pandecta.v13i1.14020.

[2] R. Butarbutar, "Kejahatan Siber Terhadap Individu: Jenis, Analisis, Dan Perkembangannya," *Technology and Economics Law Journal*, vol. 2, no. 2, pp. 299–317, Aug. 2023.

[3] Y. Karali, S. Panda, and C. Panda, "Cyber Crime: An Analytical Study of Cyber Crime Cases at the Most Vulnerable States and Cities in India.," *International Journal of Engineering and Management Research (IJEMR)*, vol. 5, no. 2, pp. 43–48, 2015.

[4] S. Das and T. Nayak, "IMPACT OF CYBER CRIME: ISSUES AND CHALLENGES," *International Journal of Engineering Sciences*, vol. 6, no. 2, Oct. 2013.

[5] W. A. Al-Khater, S. Al-Maadeed, A. A. Ahmed, A. S. Sadiq, and M. K. Khan, "Comprehensive Review of Cybercrime Detection Techniques," *IEEE Access*, vol. 8, pp. 137293–137311, 2020, doi: 10.1109/ACCESS.2020.3011259.

[6] Z. Alkhalil, C. Hewage, L. Nawaf, and I. Khan, "Phishing Attacks: A Recent Comprehensive Study and a New Anatomy," *Front. Comput. Sci.*, vol. 3, p. 563060, Mar. 2021, doi: 10.3389/fcomp.2021.563060.

[7] N. S. Azzahra, A. M. Tambunan, N. N. Aulia, A. Binarsih, and T. H. Saepudin, "TINJAUAN LITERATUR TENTANG ANCAMAN CYBERCRIME DAN IMPLEMENTASI KEAMANAN SIBER DI INDUSTRI PERBANKAN".
[8] R. A. Sabella, J. W. Patchin, and S. Hinduja, "Cyberbullying myths and realities," *Computers in Human Behavior*, vol. 29, no. 6, pp. 2703–2711, 2013, doi: https://doi.org/10.1016/j.chb.2013.06.040.
[9] P. Arsi, I. Prayoga, and M. H. Asyari, "Optimasi Strategi Pencegahan Cyberbullying bagi Usia Remaja di Kab. Banyumas Berbasis IT," *JA*, vol. 6, no. 2, p. 377, May 2023, doi: 10.33633/ja.v6i2.1011.
[10] M. H. Rumlus and H. Hartadi, "Kebijakan Penanggulangan Pencurian Data Pribadi dalam Media Elektronik," *j. ham*, vol. 11, no. 2, p. 285, Aug. 2020, doi: 10.30641/ham.2020.11.285-299.
[11] Achmad Mukhlis, Baiq Laila Alfila, and Aliya Zhafira Wastuyana, "Ancaman dan Langkah Pengamanan Sistem Informasi Menggunakan Metode Systematic Literature Review," *JUISIK*, vol. 3, no. 2, pp. 143–152, Jun. 2023, doi: 10.55606/juisik.v3i2.496.
[12] R. D. Hapsari and K. G. Pambayun, "ANCAMAN CYBERCRIME DI INDONESIA: Sebuah Tinjauan Pustaka Sistematis," *JK*, vol. 5, no. 1, pp. 1–17, Oct. 2023, doi: 10.33701/jk.v5i1.3208.
[13] B. Arora, "Exploring and analyzing Internet crimes and their behaviours," *Perspectives in Science*, vol. 8, pp. 540–542, Sep. 2016, doi: 10.1016/j.pisc.2016.06.014.