# Penyuluhan dan Pelatihan Dasar Keamanan Siber pada Siswa SMK Muhammadiyah 1 Semarang

**Ramadhan Rakhmat Sani[1], Wildanil Ghozi[2], Fauzi Adi Rafrastara[3], Abdussalam[4], Elkaf Rahmawan Pramudya[5], Wellia Shinta Sari[6]**

[1]ramadhan_rs@dsn.dinus.ac.id, [2]wildanil.ghozi@dsn.dinus.ac.id, [3]fauziadi@dsn.dinus.ac.id,
[4]abdussalam@dsn.dinus.ac.id, [5]elkaf.rahmawan@dsn.dinus.ac.id, [6]wellia.shinta@dsn.dinus.ac.id
[1,6]Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro, Semarang 50131
[2,3,4,5]Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro, Semarang 50131

**Artikel Info**

***Kata kunci:***

Penyuluhan
Pelatihan
Keamanan siber
Kata sandi
Data pribadi

ABSTRAK (10 PT)

Di era digital saat ini, sesorang semakin bergantung pada teknologi dan internet dalam kegiatan sehari-hari. Namun, pengetahuan mereka tentang keamanan informasi dan ancaman siber masih sangat minim. Banyak yang belum memahami pentingnya melindungi data pribadi, cara berkomunikasi secara aman di jaringan, dan jenis-jenis serangan siber yang mengancam privasi serta keamanan mereka. Siswa atau pelajar 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 pribadi yang dikelola oleh setiap orang. Terutama juga Siswa SMK Muhammadiyah 1 Semarang yang mana dalam aktifitas keseharian masih kurangnya kesadaran mereka tentang keamanan informasi, serta keterbatasan pemahaman tentang serangan siber kurangnya pemahaman tentang kata sandi yang kuat. Pada akhir sesi kegiatan, dari 29 peserta terdapat 21 siswa yang menyelesaikan pelatihan dengan melaporkan hasil yang didapat yaitu terdapat 19 siswa memiliki sandi yang kuat dan 2 yang masih lemah. Sedangkan dari sisi kebocoran data terdapat 4 siswa yang teridikasi ada kebocoran data dan 17 siswa datanya aman.

*Author Korespondensi :*

Ramadhan Rakhmat Sani,
Program Studi Sistem Informasi
Fakultas Ilmu Komputer
Universitas Dian Nuswantoro, Semarang 50131
Email: ramadhan_rs@dsn.dinus.ac.id

## 1. PENDAHULUAN

Perkembangan teknologi di era digital telah membawa dampak signifikan dalam berbagai aspek kehidupan, termasuk pendidikan, komunikasi, sosial dan ekonomi [1], [2]. Teknologi telah mempermudah akses informasi dan meningkatkan efisiensi dalam berbagai bidang. Siswa di sekolah pun kini semakin bergantung pada perangkat digital dan internet, baik untuk proses pembelajaran maupun untuk berkomunikasi dan bersosialisasi [3]. Namun, di balik semua manfaat yang ditawarkan, kemajuan teknologi juga membawa tantangan baru, terutama terkait keamanan siber. Salah satu dampak negatif dari pesatnya perkembangan teknologi adalah meningkatnya kejahatan siber dan juga mental *health issue*, *cyber bullying*, *cybercrime*, dan masalah-masalah lainnya [4], [5]. Kejahatan ini meliputi berbagai bentuk serangan, seperti pencurian data pribadi, peretasan akun, penyebaran *malware*, hingga penipuan daring (*phishing*). Kejahatan siber sangat berbahaya karena dapat merugikan individu maupun institusi, serta menimbulkan ancaman serius terhadap

privasi dan keamanan informasi [6]. Siswa, sebagai pengguna teknologi yang aktif, sering menjadi target yang rentan akibat kurangnya pemahaman mereka tentang risiko dan cara melindungi diri dari ancaman tersebut.

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 [7]. Namun penggunaan dari undang-undang tersebut belum maksimal, sehingga masih banyak terjadi kasus kejahatan siber di Indonesia [8]. Meski ancaman kejahatan siber semakin nyata, perhatian dan tanggung jawab sekolah serta institusi pendidikan terhadap masalah ini sering kali masih kurang. Banyak sekolah belum memberikan edukasi yang cukup kepada siswa tentang pentingnya menjaga keamanan siber, baik dalam penggunaan perangkat digital maupun aktivitas online sehari-hari [9]. Kurangnya program yang mengajarkan literasi digital [10] dan keamanan informasi membuat siswa rentan terhadap serangan siber [11], terutama karena mereka banyak menghabiskan waktu di dunia maya untuk belajar dan berinteraksi. Kondisi ini menimbulkan kebutuhan mendesak untuk meningkatkan kesadaran dan kemampuan siswa dalam melindungi diri dari ancaman siber.

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 [12], [13]. Kejahatan siber merupakan salah satu dampak negatif yang paling berbahaya [14]. 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 [15].

Tujuan utama dari pelaksanaan pengabdian ini adalah membekali siswa dengan keterampilan praktis yang dapat mereka terapkan dalam kehidupan sehari-hari agar terhindar dari serangan siber, sekaligus mendorong institusi pendidikan untuk lebih memperhatikan aspek keamanan digital bagi siswa. Pelatihan dasar keamanan siber ini dapat meningkatkan kesadaran siswa mengenai risiko dan bahaya kejahatan siber. Melalui kegiatan ini, siswa akan diberikan pengetahuan dasar tentang keamanan informasi, jenis-jenis ancaman siber, serta langkah-langkah pencegahan yang dapat diambil untuk melindungi data pribadi mereka. Siswa mempelajari bagaimana cara mendeteksi adanya serangan Man-in-the-Middle, di mana pelaku kejahatan siber berusaha menyadap komunikasi antara dua pihak. Misalnya, dengan menganalisis lalu lintas jaringan sehingga dapat melihat apakah ada pihak ketiga yang tidak sah menyisipkan diri di antara komunikasi. Selain itu juga dapat mengidentifikasi mengenai serangan *snofin*g, di mana pelaku kejahatan berusaha mengumpulkan data sensitif yang dikirimkan melalui jaringan, seperti kata sandi

Adapun mereka menjadi target potensial dari berbagai jenis serangan siber seperti phishing, malware, atau pencurian data pribadi. Disertai juga mengenai banyaknya siswa yang tidak menyadari pentingnya menjaga informasi pribadi mereka, terutama ketika berinteraksi di dunia digital. 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. Beberapa kategori kejahatan siber antara lain cyber terorism, *cyber warfare, cyber espionage, child pornography, denial of service, cyber bullying,* dan *phishing* [16]. Kejahatan yang dilakukan melalui teknologi dunia maya dapat menargetkan individu seperti serangan *phising* dan *cyber bullying. 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. *Phishing* dilakukan dengan menjebak seseorang untuk atau memancing seseorang melalui halaman web palsu. 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* [12], [13]

## 2. METODE

Metode pelaksanaan yang digunakan dalam kegiatan pengabdian ini meliputi permasalahan mitra dan alur kegiatan

### 2.1 Permasalahan Mitra

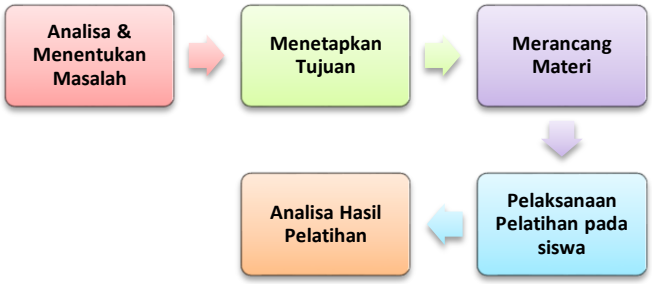
Beberapa permasalahan yang dihadapi mitra beserta solusinya dituangkan dalam tabel 1 sebagai berikut :

Tabel 1. Tabel Permasalahan dan Solusi

| Masalah | Solusi |
|---|---|
| 1. Banyaknya siswa yang tidak menyadari pentingnya menjaga informasi pribadi mereka, terutama ketika berinteraksi di dunia digita | 1. Memberikan Pemahaman Tentang Keamanan Informasi Menggunakan CIA Triad yang terdiri dari tiga prinsip: Confidentiality (Kerahasiaan), Integrity (Integritas), Availability (Ketersediaan) |
| 2. Kejahatan yang dilakukan melalui teknologi dunia maya dapat menargetkan individu seperti siswa yang masih awam | 2. Mengedukasikan jenis-jenis Serangan Siber seperti Phishing, Malware, dan DDoS Attacks |

2.2 Alur Kegiatan

Program Kemitraan Masyarakat dilakukan di SMK Muhammadiyah 1 Semarang. Berikut pada gambar 1 merupakan alur kegiatan yang dilakukan yaitu tahap Analisa dan menentukan masalah, menetapkan tujuan, merancang materi, pelaksanaan pelatihan pada siswa, dan Analisa hasil pelatihan.

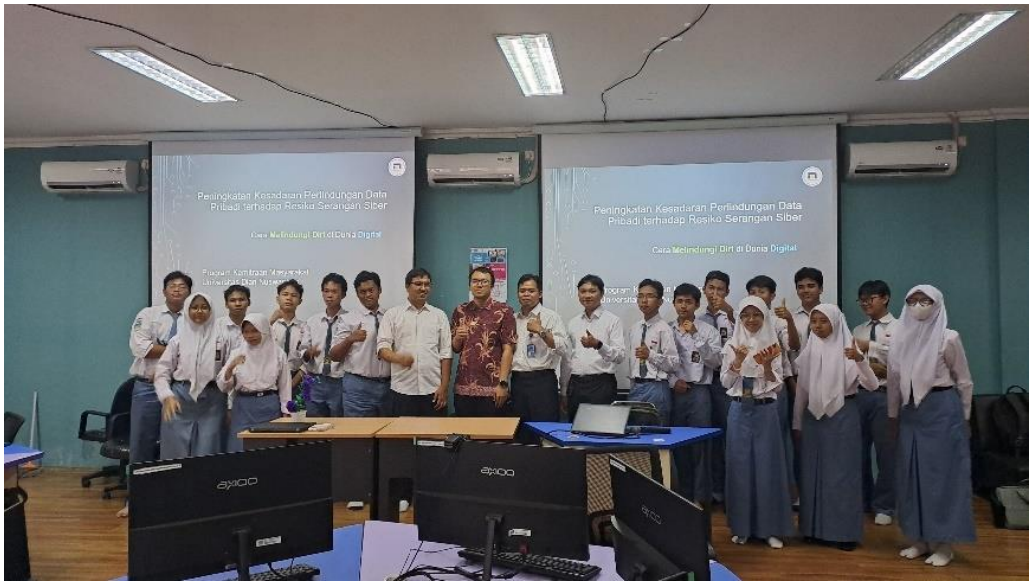



Gambar 1. Alur Kegiatan

1. Analisa dan Menentukan Masalah.
   Dalam penentuan masalah ini tim pengabdi melakukan diskusi bersama dengan salah satu guru SMK Muhammadiyah 1 Semarang. Didapatkan hasil dengan asumsi bahwa siswa kurang memiliki kesadaran tentang keamanan informasi dan minimnya pengetahuan tentang keamanan komunikasi data serta memiliki keterbatasan pemahaman tentang serangan siber kurangnya pemahaman tentang kata sandi yang kuat.
2. Menetapkan tujuan.
   Tujuan dari pelaksanan ini adalah dengan membekali siswa dengan penyuluhan dengan materi yang dapat mereka terapkan dalam kehidupan sehari-hari agar terhindar dari serangan siber, sekaligus mendorong institusi pendidikan untuk lebih memperhatikan aspek keamanan digital bagi siswa.
3. Merancang materi.
   Materi dirancang oleh Dosen dari Prodi Sistem Informasi dan Teknik Informatika yang melibatkan mahasiswa Udinus semester 7. Dimana materi tersebut mengenai *cyber security* and *career awareness* yang memberikan pemahaman kondisi keamanan siber di Indonesia, *materi policy* and *legal issues* dengan mengenalkan produk hukum dan aturan-aturan lain yang telah ditetapkan oleh pemerintah dan lembaga-lembaga penyedia layanan di internet dan materi praktikum
4. Pelaksanaan Pelatihan pada siswa.
   Pelaksanaan pelatihan akan dilakukan di SMK Muhammadiyah 1 Semarang setelah usulan ini disetujui dengan waktu sesuai kesepakatan antara pihak sekolah dan tim pengabdi.
5. Analisa hasil pelatihan.
   Analisa dari hasil pelatihan dilihat dari percobaan yang diberikan kepada siswa saat pelatihan selesai.

## 3. PEMBAHASAN HASIL

Program kemitraan masyarakat ini dilaksanakan pada tanggal 25 februari 2025 di ruang Labaroratorium Animasi yang biasa digunakan untuk kegiatan praktek. Berikut pada gambar 2 merupakan dokumentasi kegiatan tersebut.




Gambar 2. Dokumentasi bersama siswa SMK 1 Muhammadyah Semarang

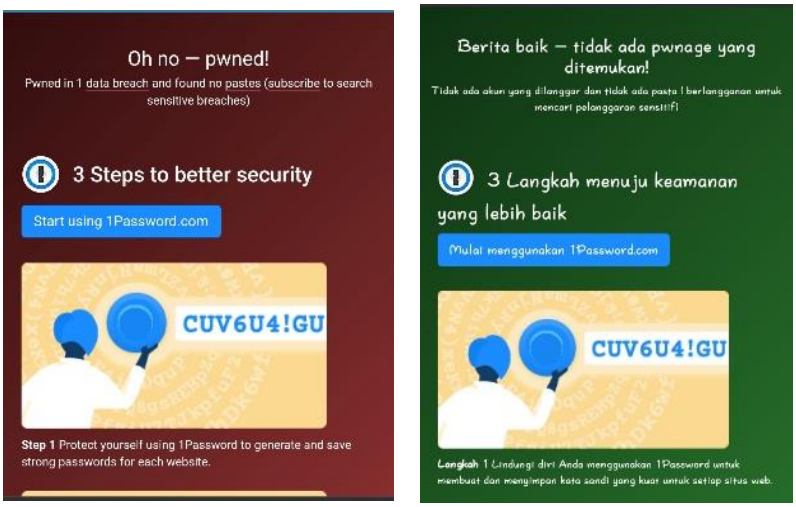
Pada kegiatan Pelatihan ini siswa diminta untuk mengakses https://www.security.org/how-secure-is-my-password/ kemudian mulai menginputkan kata sandi yang biasa digunakan untuk mengakses akun media social ataupun akun lainnya. Dari hasil tersebut akan menghasilkan jumlah waktu bagaimana sistem computer dapat menebak kata sandi yang diinputkan. Berikut gradasi warna yang dihasilkan dari inputan kata sandi berdasarkan kriteria yang terdiri dari adanya besar dan kecil huruf, angka dan juga symbol yang digabungkan. Berikut hasil warna ditunjukkan pada gambar 3.

| # of Characters | Lowercase Letters Only | At Least 1 Uppercase Letter | At Least 1 Uppercase Letter + Number | At Least 1 Uppercase Letter + Number + Symbol |
|---|---|---|---|---|
| 1 | Instantly | Instantly | - | - |
| 2 | Instantly | Instantly | Instantly | - |
| 3 | Instantly | Instantly | Instantly | Instantly |
| 4 | Instantly | Instantly | Instantly | Instantly |
| 5 | Instantly | Instantly | Instantly | Instantly |
| 6 | Instantly | Instantly | Instantly | Instantly |
| 7 | Instantly | Instantly | 1 Minute | 6 Minutes |
| 8 | Instantly | 22 Minutes | 1 Hour | 8 Hours |
| 9 | 2 Minutes | 19 Hours | 3 Days | 3 Weeks |
| 10 | 1 Hour | 1 Month | 7 Months | 5 Years |
| 11 | 1 Day | 5 Years | 41 Years | 400 Years |
| 12 | 3 Weeks | 300 Years | 2,000 Years | 34,000 Years |

Gambar 3. Gradasi warna terhadap keamanan kata sandi

Setelah mengetahui keamanan kata sandi dari masing-masing siswa, hal yang dilakukan berikutnya adalah mulai mencoba untuk mengetahui mengenai kebocoran data yang berasal baik dari akun social media, *e-commerse* ataupun akun lainnya berdasarkan dari email yang digunakan.

☼ ISSN: 3047-8510




(a) (b)

Gambar 4. (a) contoh jika ada kebocoran data, (b) tidak ada kebocoran data

Pada gambar 4 (a) dan (b) diatas merupakan hasil yang didapatkan ketika siswa menginputkan *e-mail* mereka pada halaman web https://haveibeenpwned.com/. Hasil keseluruhan dari percobaan yang dilakukan oleh siswa hadir terdiri dari 29 peserta, terdapat 21 siswa yang menyelesaikan pelatihan dengan melaporkan hasil yang didapat yaitu terdapat 19 siswa memiliki sandi yang kuat dan 2 yang masih lemah. Sedangkan dari sisi kebocoran data terdapat 4 siswa yang terindikasi ada kebocoran data dan 17 siswa datanya aman. Selebihnya dapat dilihat pada tabel 2 berikut :

Tabel 2. hasil Percobaan Siswa

| Siswa | Waktu untuk memecahkan kata sandi | Jumlah Kebocoran data |
|---|---|---|
| Siswa1 | 42 menit | 1 |
| Siswa2 | 41 tahun | - |
| Siswa3 | 84 miliar | 3 |
| Siswa4 | 41 tahun | - |
| Siswa5 | 41 tahun | - |
| Siswa6 | 400 tahun | - |
| Siswa7 | 43 miliar | - |
| Siswa8 | 500 kuintiliun | 1 |
| Siswa9 | 41 tahun | - |
| Siswa10 | 5000 tahun | - |
| Siswa11 | 6 bulan | - |
| Siswa12 | 13 septiliun quinquagintiliun | - |
| Siswa13 | 129 tahun | - |
| Siswa14 | 6 bulan | - |
| Siswa15 | 100 triliun tahun | 1 |
| Siswa16 | 32 juta tahun | - |
| Siswa17 | 100 tahun | - |
| Siswa18 | 100 ribu tahun | - |
| Siswa19 | 1 tahun | - |
| Siswa20 | 1 tahun | - |
| Siswa21 | 100 ribu tahun | - |

Dari data dalam tabel 2 tersebut mencerminkan bahwa siswa sebagian besar secara tidak langsung sudah mampu menerapkan prinsip-prinsip keamanan informasi menggunakan CIA Triad. Sedangkan dalam kasus adanya kebocoran data bisa jadi diakibatkan karena kesalahan dalam pengaturan privasi atau pengiriman email yang salah atupun kecerobohan dalam penanganan data sensitif, seperti menyimpan file penting di lokasi yang tidak aman.

## 4. KESIMPULAN

Berdasarkan hasil yang Analisa pelatihan terhadap siswa SMK Muhammadiyah 1 Semarang dapat disimpulkan bahwa mayoritas dari siswa sudah mampu menerapkan kata sandi yang aman walaupun masih ada beberapa siswa saja yang kurang aman. Sedangkan dari sisi kebocaron data ada beberapa akun dari siswa

yang rentan terhadap penyalahgunaan data yang dikarenakan mungkin saja karena adanya celah keamanan yang kurang aman dari aplikasi yang digunakan.

## UCAPAN TERIMA KASIH

Dalam kesempatan ini penulis mengucapkan terima kasih yang sebesar-besarnya kepada Lembaga Penelitian dan Pengabdian Masyarakat Universitas Dian Nuswantoro yang telah memberikan pendanaan dalam program kemitraan masyarakat ini.

## REFERENCES

[1] H. Djanggih and N. Qamar, "Penerapan Teori-Teori Kriminologi dalam Penanggulangan Kejahatan Siber (Cyber Crime)," *Pandecta Res. Law J.*, 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," *Technol. Econ. Law J.*, vol. 2, no. 2, pp. 299–317, Aug. 2023.

[3] S. Das and T. Nayak, "IMPACT OF CYBER CRIME: ISSUES AND CHALLENGES," *Int. J. Eng. Sci.*, vol. 6, no. 2, Oct. 2013.

[4] 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.

[5] 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.," *Int. J. Eng. Manag. Res. IJEMR*, vol. 5, no. 2, pp. 43–48, 2015.

[6] R. D. Hapsari and K. G. Pambayun, "ANCAMAN CYBERCRIME DI INDONESIA: Sebuah Tinjauan Pustaka Sistematis," *J. Konstituen*, vol. 5, no. 1, pp. 1–17, Oct. 2023, doi: 10.33701/jk.v5i1.3208.

[7] 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.

[8] Achmad Mukhlis, Baiq Laila Alfila, and Aliya Zhafira Wastuyana, "Ancaman dan Langkah Pengamanan Sistem Informasi Menggunakan Metode Systematic Literature Review," *J. Ilm. Sist. Inf. Dan Ilmu Komput.*, vol. 3, no. 2, pp. 143–152, Jun. 2023, doi: 10.55606/juisik.v3i2.496.

[9] N. Konety, N. Nidatya, and A. Akim, "SOSIALISASI KEJAHATAN SIBER PADA SISWA-SISWI SDN MEKARSARI JATINANGOR," *Sawala J. Pengabdi. Masy. Pembang. Sos. Desa Dan Masy.*, vol. 1, no. 2, p. 67, Jul. 2020, doi: 10.24198/sawala.v1i2.27679.

[10] E. Sapitri *et al.*, "Pentingnya Peningkatan Literasi Keamanan Digital Bagi Siswa SMP Negeri 4 Kota Tasikmalaya Untuk Melindungi Data Pribadi," *J. Pengabdi. Masy. Bangsa*, vol. 2, no. 10, pp. 4724–4733, Dec. 2024, doi: 10.59837/jpmba.v2i10.1779.

[11] M. Alawida, A. E. Omolara, O. I. Abiodun, and M. Al-Rajab, "A deeper look into cybersecurity issues in the wake of Covid-19: A survey," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 10, Part A, pp. 8176–8206, Nov. 2022, doi: 10.1016/j.jksuci.2022.08.003.

[12] R. A. Sabella, J. W. Patchin, and S. Hinduja, "Cyberbullying myths and realities," *Comput. Hum. Behav.*, vol. 29, no. 6, pp. 2703–2711, 2013, doi: https://doi.org/10.1016/j.chb.2013.06.040.

[13] P. Arsi, I. Prayoga, and M. H. Asyari, "Optimasi Strategi Pencegahan Cyberbullying bagi Usia Remaja di Kab. Banyumas Berbasis IT," *ABDIMASKU J. Pengabdi. Masy.*, vol. 6, no. 2, p. 377, May 2023, doi: 10.33633/ja.v6i2.1011.

[14] K. Hantoro and A. Ramdhani, "Sosialisasi Keamanan Siber untuk Anak-anak di Panti Asuhan Aisiyah Bekasi," 2020.

[15] R. Oktafiani, S. E. Trisnawati, S. Maymunah, and S. Paridah, "Mini Research Teknologi Keuangan Syariah Identitas Digital Vs Kejahatan Siber (Studi Intensitas Kasus dan Pola Kejahatan Siber Melalui Platform Digital)," *J. Sharia Econ. Law*, vol. 2, no. 1, pp. 23–34, Aug. 2024, doi: 10.37680/jshel.v2i1.5755.

[16] 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.