JSI (Jurnal Sistem Informasi) Universitas Dirgantara Marsekal Suryadarma
p-ISSN: 2355-9675
e-ISSN: 2541-3228

Penerapan Metode *Multiple Criteria Decision Analysis* pada Analisis Keamanan Siber Siswa-siswi SMK Al-Mujahirin

Yulisa Gardenia[1,*], Fitria Risyda[2], Muryan Awaludin[3]
[1,2,]Department of Informatics Management, Universitas Dirgantara Marsekal Suryadarma, Indonesia
[3]Department of Information Systems, Universitas Dirgantara Marsekal Suryadarma, Indonesia
yulisagardenia@gmail.com, frisdya@gmail.com, muryanawaludin@gmail.com

Article Info

Article history:

Received November 15, 2024
Accepted Desember 16, 2024
Published January 2, 2025

Kata Kunci*:*

Keamanan siber
Kejahatan siber
Multi Criteria Decison Analysis

ABSTRAK (10 PT)

Penelitian ini bertujuan adalah untuk menganalisis faktor-faktor apa saja yang mempengaruhi tingkat kesadaran akan keamanan siber yang dimiliki siswa-siswi SMK Al-Mujahirin. Metode analisis sekaligus metode perhitungan yang digunakan dalam penelitian ini adalah analisis multi kriteria atau *Multi Criteria Decision Analysis* (MCDA). Pengumpulan data menggunakan metode kuesioner yang dilakukan secara online menggunakan aplikasi Gform. Analisis tingkat kesadaran keamanan siber siswa-siswi diukur berdasarkan dimensi knowledge (pengetahuan), attitude (sikap), dan behaviour (perilaku). Area yang digunakan dalam konsep pengukuran adalah regulation, internet, password, data security, dan cyberattack. Karakteristik responden adalah representasi dari keberadaan responden yang terlibat, yaitu siswa-siswi SMK Al-Mujahirin. Berdasarkan kuesioner yang sudah disebar, diketahui bahwa reponden dari kelas TKJ (Teknik Komputer Jaringan) sebanyak 64 orang dengan presentase 53,3%, kelas Multimedia sebanyak 36 dengan presentase 30%, dan kelas DKV (Desain Komunikasi Visual) sebanyak 20 dengan presentase 16,6%. Kesadaran keamanan informasi siswa-siswi SMK Al-Mujahirin Depok sudah berada pada level "sedang" dan hampir baik dengan nilai keseluruhan 69,3%. Oleh karena itu, hanya perlu mempertahankan yang sudah baik dan meningkatkan yang masih berada pada level sedang. Untuk memastikan bahwa proses ke arah itu dapat dilakukan, diperlukan pengawasan yang berkelanjutan. Selain itu, semua pihak harus bekerja sama untuk meningkatkan kesadaran terhadap keamanan data. Dari tiga dimensi, hanya dimensi tingkah laku yang menghasilkan hasil yang "buruk". Demikian pula, dari lima area pengukuran, hanya tiga area yang menghasilkan hasil yang "buruk". Sebagai contoh, "selalu taat pada aturan", "berhati-hati menggunakan perangkat seluler", dan "menyadari konsekuensi setiap tindakan" adalah bagian-bagian yang termasuk dalam kategori ini.

Check for updates

Corresponding Author:

Yulisa Gardenia,
Department of Informatics Management,
Universitas Dirgantara Marsekal Suryadarma,
Email: *yulisagardenia@gmail.com

1. PENDAHULUAN

Revolusi Industri 4.0 dan Society 5.0 yang sedang terjadi, telah memberikan kontribusi signifikan terhadap peningkatan jumlah pengguna Internet. Kemajuan teknologi yang diperkenalkan pada era ini

telah mendorong perkembangan teknologi di seluruh aspek masyarakat, termasuk pendidikan. Pengajaran dan pembelajaran online telah memperoleh manfaat besar dari kemajuan teknologi Internet ini. Namun, tidak semua orang menyadari dampak negatif yang terkait dengan peningkatan penggunaan Internet (Gardenia & Gani, 2024).

Salah satu dampak negatif yang terjadi karena adanya peningkatan jumlah penguna internet adalah peningkatan kejahatan siber (*cybercrime*). Hasil survei penetrasi internet Indonesia 2024 yang dirilis APJII menunjukkan peningkatan 1,4% dibandingkan periode sebelumnya. Sejak 2018, penetrasi internet Indonesia mencapai 64,8%, kemudian naik 73,7% pada 2020, 77,01% pada 2022, dan 78,19% pada 2023 (APJII, 2024).

Seiring berkembangnya dunia digital, istilah cybercrime menjadi lebih umum akhir-akhir ini. Cybercrime atau kejahatan di dunia maya sendiri merupakan salah satu akibat negatif dari penggunaan media internet sebagai platform yang saat ini banyak digunakan oleh individu-individu di Masyarakat (Widya Ramailis, 2020). Cybercrime ialah kejahatan yang dilakukan melalui media digital dan contoh dari tindakan cybercrime tersebut adalah pembobolan beberapa data penting pada korban, hacker medsos, pengambilan dengan lembut saldo rekening korban, dan lain sebagainya (Saputra, 2022). Kejahatan ini tidak hanya menyerang individu, tetapi juga perusahaan dan pemerintahan, menyebabkan ancaman keamanan informasi dan kerugian finansial besar. Serangan ransomware, phishing, dan penyebaran malware adalah contoh jenis cybercrime yang berusaha menggunakan kerentanan manusia atau sistem keamanan untuk mencuri kata sandi, data, atau uang secara langsung. (Agency, n.d.).

Teknologi Global IBM menekankan masalah pelanggaran sebagai salah satu masalah terpenting yang harus ditangani melalui langkah-langkah keamanan dan protokol praktik terbaik yang direkomendasikan (Awaludin, 2019). Sebenarnya, telah ada penekanan yang meningkat baru-baru ini pada peran perilaku pribadi dalam pengurangan risiko siber. Meskipun demikian, pemahaman tentang bagaimana orang-orang berbeda dalam kesadaran, pemahaman, dan praktik keamanan siber mereka saat menghadapi berbagai ancaman siber masih agak terbatas. Selain itu, sejauh yang kami ketahui, belum ada studi yang belum membandingkan dan menilai ketiga elemen ini di seluruh negara (Zwilling et al., 2022).

Kurangnya kesadaran akan bahaya penggunaan internet dan interaksi yang dilakukan dengan media sosial yang dilakukan secara online, menyebabkan hilangnya bahkan penggunaan data pribadi yang disalahgunakan oleh individu yang tidak berwenang. Semua usia yang merupakan penguna internet dapat terkena dampak dari kejahatan dunia maya, karena kurangnya pemahaman mengenai keamanan siber. Para siswa sekolah menengah kejuruan juga dapat terkena imbas akibat kurangnya pemahaman mengenai keamanan siber dan kejahatan siber (Firdaus, Muksin, & Awaludin, 2022). Berdasarkan penelitian yang dilakukan oleh Irwan Cholid Husain mengenai kesadaran keamanan informasi yang dimiliki oleh siswa SMA XYZ kelas XII, disimpulkan bahwa tingkat kesadaran keamanan informasi yang dimiliki oleh siswa adalah baik. Lima indikator yang digunakan dalam mengukur tingkat kesadaran baik karena memiliki rata-rata nilai diatas 80%, namun dari lima indikator terdapat dua indikator yang diketahui memiliki tingkat kesadaran keamanan informasi yang buruk (Prasetya, I. A., & Safriadi, 2015).

Penelitian dikalangan siswa-siswi sekolah mengenai keamanan data juga pernah dilakukan oleh Abrar Farizi, dkk, hasil dari penelitian yang telah dilakukan adalah perlunya terus meningkatkan literasi digital pada kalangan siswa, walaupun Sebagian besar siswa-siswi sudah menunjukkan hasil yang baik dalam bermedia sosial tetapi penciptaan lingkungan digital yang aman dan bertanggung jawab bagi siswa akan terus didukung dengan dukungan terkoordinasi sekolah guru dan orang tua (Mahendra, Hatta, & Aristyagama, 2024).

Peneliti sebelumnya sudah pernah melakukan penelitian mengenai pengukuran kesadaran cybersecurity menggunakan metode AHP dan metode SEM dengan objek yang digunakan adalah mahasiswa Teknik penerbangan Universitas Dirgantara Marsekal Suryadarma pada tahun 2023. Hasil dari penelitian adalah seluruh mahasiswa mempunyai kesadaran akan cybersecurity dan cybercrime.

Penelitian ini dilakukan berdasarkan penelitian terdahulu yang sudah dilakukan oleh peneliti. Perbedaannya ada pada objek penelitian yaitu siswa-siswi sekolah menengah kejuruan Al-Mujahirin Depok, level penilaian dan metode perhitungan yang digunakan. SEM Amos menjadi metode perhitungan pada penelitian sebelumnya, sedangkan metode AHP yang digunakan untuk menentukan dimensi dan menggambarkan hierarki dari tingkat kesadaran akan keamanan siber. Skala likert dengan level Sangat setuju berbobot 5, setuju berbobot 4, cukup setuju bobotnya 3, tidak setuju 2 dan sangat

tidak setuju 1 merupakan level penilaian yang digunakan untuk perhitungan.

Tujuan dari penelitian ini adalah untuk menganalisis faktor-faktor apa saja yang mempengaruhi tingkat kesadaran akan keamanan siber yang dimiliki siswa-siswi SMK Al-Mujahirin.

2. METODE

2.1. Studi Literatur

Pada tahap ini studi literature Pada tahap ini, penelitian literatur dilakukan dari berbagai sumber, termasuk jurnal nasional, jurnal internasional, e-book, prosiding, dan website. Hasilnya akan berupa teori atau konsep tentang model atau teknik pengukuran keamanan informasi dan keamanan privasi.

Tabel 1 Penelitian Terdahulu

Sumber	Metode Penelitian	Pembahasan
(Haikal Arief, Arifa Fitri, & Malays Sari, 2024)	Analisis statistik deskriptif	Metode yang digunakan untuk mendeskripsikan karakteristik responden, menganalisis distribusi frekuensi dan presentase jawaban responden, serta mengidentifikasi pola dan tren dalam data.
(Gardenia & Gani, 2024)	Metode AHP dan SEM Amos	Metode AHP digunakan untuk menentukan hierarki dimensi dan focus area, SEM Amos digunakan untuk menghitung hasil kuesioner.
(Mahendra et al., 2024)	Analisis statistik deskriptif	Penelitian ini menggunakan skala Guttmann untuk menghitung hasil kuesioner dan analisis penelitian menggunakan statistik deskriptif.
(Kusumaningrum, Wijayanto, & Raharja, 2022)	Multi Criteria Decision Analysis dan Analytical Hierarcy Process	Pada penelitian ini peneliti menggunakan metode AHP, dimana metode ini menjadi salah satu metode dari multi criteria decision.

Metode yang digunakan dalam penelitian dipilih berdasarkan tujuan dari penelitian dan hasil akhir yang diharapkan oleh peneliti. Beberapa metode yang digunakan oleh peneliti terdahulu untuk melakukan penelitian adalah analisis statistik deskriptif dan multi criteria decision analysis, keduanya memiliki kelebihan dan kekurangannya masing-masing. Analisis statistik deskriptif memiliki kelebihan mudah dipahami dan diterapkan oleh peneliti, kekurangannya tidak bisa memberikan informasi tentang hubungan antara variable. Metode multi criteria decision analysis memiliki banyak kelebihan salah satunya memiliki banyak alternatif metode yang bisa digunakan dan kekurangannya adalah jika kriteria yang diukur banyak, maka tingkat analysis akan semakin lama.

2.2. Pengumpulan Data

Penelitian ini menggunakan pendekatan kualitatif dengan metode survei online (Haikal Arief et al., 2024). Survei online digunakan dalam pengumpulan data yang hasilnya akan dihitung menggunakan metode multi criteria decision analysis. Kuesioner yang dilakukan secara online menggunakan aplikasi Gform. Analisis tingkat kesadaran keamanan siber siswa-siswi diukur berdasarkan dimensi knowledge (pengetahuan), attitude (sikap), dan behaviour (perilaku). Area yang digunakan dalam konsep pengukuran adalah regulation, internet, password, data security, dan cyberattack.

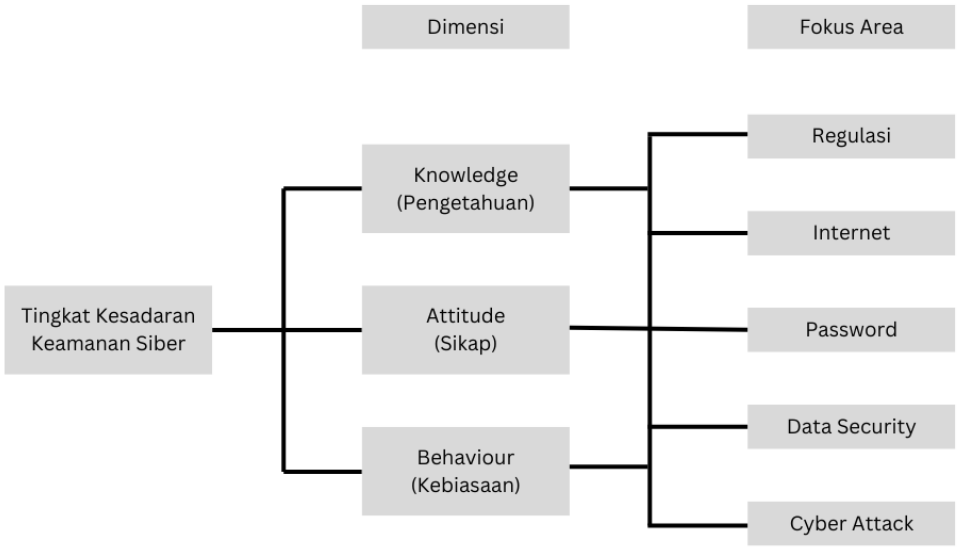
2.3. Metode Multi Criteria Decision Analysis

Salah satu elemen proses manajemen risiko yang termasuk dalam SNI ISO 31000 adalah penilaian risiko. Elemen ini terdiri dari tiga rangkaian aktivitas: identifikasi risiko, analisis risiko, dan penilaian risiko. Ketiga aktivitas tersebut dilakukan sebagai dasar untuk menilai seberapa penting suatu risiko bagi suatu organisasi/lembaga dan mengambil tindakan risiko. Teknik penilaian risiko dapat dilakukan dengan menggunakan berbagai alat, termasuk analisis keputusan multi-kriteria atau Multiple Criteria Decision Analysis (MCDA) (Antonius, 2019). Menurut Mahdi, Teknik penilaian ini sangat sesuai untuk semua aktivitas penilaian risiko, terutama dalam mengevaluasi dampak dan tingkat risiko pada proses analisis risiko. Proses analisis keputusan multikriteria dapat dilakukan melalui lima tahap, yaitu menetapkan tujuan, menetapkan kriteria, melakukan pembobotan kriteria, menyusun penilaian, dan menyusun rekomendasi keputusan. Metode Analisis Keputusan Berbasis Beberapa Kriteria (MCDA) umumnya digunakan untuk membuat keputusan mengenai berbagai alternatif yang memiliki banyak kriteria. Metode Analisis Keputusan Berdasarkan Kriteria Ganda digunakan untuk menilai nilai keseluruhan alternatif berdasarkan kriteria tertentu. Pendekatan MCDA dibagi menjadi tiga kategori (Kusumaningrum et al., 2022).

Pengukuran menggunakan metode multi criteria decision analysis ditunjukkan dengan persamaan sebagai berikut:

$$V(a) = \Sigma_{i=1}^{n} v_i(a) w_i \ldots . (1)$$

Keterangan :
- V(a) adalah nilai seluruh alternative nilai seluruh alternative a,
- vi (a) adalah nilai skor yang mewakili performansi alternative a,
- wi adalah bobot yang diberikan untuk menggambarkan tingkat kepentingan kriteria i.



Sumber: (Gardenia dan Alcianno, 2023)

Gambar 1 Kerangka Penelitian Keamanan Siber

Untuk menguji knowledge (pengetahuan), attitude (sikap) dan behaviour (perilaku) responden berkaitan dengan enam area kesadaran keamanan siber disusunlah pentanyaan sebanyak 15 (lima belas) buah, atau masing-masing area memiliki 3 (tiga) pertanyaan. Setiap pertanyaan diberikan jawaban dengan 3 skala yaitu, benar, salah, dan tidak tahu. Pertanyaan ini digunakan untuk menghitung nilai vi(a) (Kusumaningrum et al., 2022). Tabel 1 (Gardenia & Gani, 2024) merupakan contoh dari pertanyaan focus area kesadaran tentang keamanan siber.

Tabel 2 Pertanyaan dari Dimensi Tingkat Kesadaran Keamanan Siber

No	Knowledge	Attitude	Behaviour
1.	Pengetahuan akan Regulasi	Selalu berhati-hati dalam memposting sesuatu	Tidak pernah menyebarkan berita bohong
2.	Mengetahui keamanan data	Menggunakan antivirus di laptop dan gawai	Selalu waspada jika ada yang mengirimkan data di sosial media
3.	Mengetahui tentang kata sandi yang kuat	Menggunakan kata sandi yang aman di setiap aplikasi yang digunakan	Tidak pernah membagi kata sandi dengan orang lain
4.	Mengetahui akan bahaya internet	Menggunakan banyak aplikasi di laptop dan di gawai	Mengunggah aplikasi yang aman
5.	Mengetahui tentang kejahatan siber	Menyimpan data pribadi secara aman	Tidak pernah meretas sosial media atau email orang lain

Sumber: (Gardenia dan Alcianno, 2023)

Perhitungan perkalian dengan bobot w_i dilakukan setelah mendapatkan nilai v_i(a). Metode analitycal hierarchy process (AHP) digunakan untuk menentukan bobot w_i, dimana metode AHP menjadi salah satu metode dari Multiple Criteria Decision Analysis (MCDA). Skala yang digunakan mengikuti penelitian Krugger dan Kerney dan dapat dilihat pada tabel 2 (Kruger & Kearney, 2006).

Tabel 3 Bobot Tiap Dimensi

Dimensi	Bobot
Pengetahuan	30
Sikap	20
Kebiasaan	50

Sebelum menetapkan tingkat kesadaran keamanan informasi sebagai hasil akhir, proses penghitungan total skor untuk setiap dimensi per area yang telah disebutkan sebelumnya dapat dilihat pada tabel berikut ini.

Tabel 4 Perhitungan Total Nilai

Dimensi	**Area**					**Total Nilai**
	A1	**A2**	**A3**	**A4**	**A5**	
Pengetahuan	A11	A21	A31	A41	A51	$\Sigma_{i=1}^{n} A1i/5$
Sikap	A12	A22	A32	A42	A52	$\Sigma_{i=1}^{n} A2i/5$
Kebiasaan	A13	A23	A33	A43	A53	$\Sigma_{i=1}^{n} A3i/5$
Total Nilai	$\Sigma_{i=1}^{n} A1i/3$	$\Sigma_{i=1}^{n} A2i/3$	$\Sigma_{i=1}^{n} A3i/3$	$\Sigma_{i=1}^{n} A4i/3$	$\Sigma_{i=1}^{n} A5i/3$	

Tabel 4 merupakan presentase mengenai level tingkat kesadaran keamanan siber yang telah

ditetapkan yaitu baik, sedang dan buruk.

Tabel 5 Tingkat Kesadaran Keamanan Siber (Kusumaningrum et al., 2022)

Hasil Pengukuran (dalam persen)	Level
80 – 100	Baik
60 – 79	Sedang
0 – 59	Buruk

3. HASIL DAN PEMBAHASAN

Karakteristik responden adalah representasi dari keberadaan responden yang terlibat, yaitu siswa-siswi SMK Al-Mujahirin. Berdasarkan kuesioner yang sudah disebar, diketahui bahwa reponden dari kelas TKJ (Teknik Komputer Jaringan) sebanyak 64 orang dengan presentase 53,3%, kelas Multimedia sebanyak 36 dengan presentase 30%, dan kelas DKV (Desain Komunikasi Visual) sebanyak 20 dengan presentase 16,6%.

Tabel 6 Hasil Perhitungan Responden berdasarkan Jurusan

Jurusan	Jumlah	Presentase %
TKJ	64	53,3 %
MM	36	30 %
DKV	20	16,6 %
Total	120	100 %

Hasil perhitungan responden jurusan Teknik Komputer Jaringan sebesar 53,3% menunjukkan bahwa sebagian besar responden berasal dari jurusan TKJ. Perhitungan pembobotan yang dilakukan untuk fokus area yang sudah ditentukan menggunakan AHP dapat dilihat pada tabel 6.

Tabel 7 Hasil Pembobotan

Dimensi	w_i
Regulasi	0,2
Internet	0,4
Password	0,5
Data Security	0,1
Cyber Attack	0,2

Dari tabel 6 diketahui bahwa focus area password (kata sandi) memiliki bobot nilai yang paling maksimum. Hal ini menunjukkan bahwa siswa-siswi SMK Al-Mujahirin mengetahui cara menjaga keamanan data pribadi dan mereka mengetahui cara pembuatan password yang kuat seperti apa. Setelah mengetahui hasil pembobotan, selanjutnya pada tabel 7 adalah hasil perhitungan tingkat kesadaran keamanan siber untuk tiap dimensi dan focus area.

Tabel 8 Hasil Perhitungan Tingkat Kesadaran Keamanan Siber

Dimensi	Area					Total Nilai
	A1	A2	A3	A4	A5	
Pengetahuan	80	73	90	76	69	77,6
Sikap	65	85	85	75	76	77,2
Kebiasaan	20	75	75	55	40	53
Total Nilai	55	77,7	83,3	68,7	61,7	69,3

Hasil perhitungan tingkat kesadaran keamanan siber untuk semua dimensi dari semua fokus area yang ada yaitu 69,3%. Berdasarkan tabel 4 yang merupakan level kesadaran keamanan informasi menunjukkan bahwa hasil tersebut masuk dalam level sedang (mendekati baik). Pada level ini siswa-siswi sekolah menengah kejuruan harus meningkatkan kesadaran akan keamanan data. Hasil pengukuran pada pengetahuan sebesar 77,6% dan sikap 77,2% menunjukkan bahwa dimensi pengetahuan dan sikap memiliki level baik, tetapi dimensi kebiasaan sebesar 69,3% yang artinya siswa-siswi harus mengubah kebiasaan dan bebenah diri agar dapat memiliki kebiasan yang baik dalam menggunakan internet.

4. KESIMPULAN

Berdasarkan hasil perhitungan pada tabel 7, kesadaran keamanan informasi siswa-siswi SMK Al-Mujahirin Depok sudah berada pada level "sedang" dan hampir baik dengan nilai keseluruhan 69,3%. Oleh karena itu, hanya perlu mempertahankan yang sudah baik dan meningkatkan yang masih berada pada level sedang. Untuk memastikan bahwa proses ke arah itu dapat dilakukan, diperlukan pengawasan yang berkelanjutan. Selain itu, semua pihak harus bekerja sama untuk meningkatkan kesadaran terhadap keamanan data. Dari tiga dimensi, hanya dimensi tingkah laku yang menghasilkan hasil yang "buruk". Demikian pula, dari lima fokus area pengukuran, hanya tiga area yang menghasilkan hasil yang "buruk". Sebagai contoh, "Selalu taat pada aturan perusahaan", "Berhati-hati menggunakan perangkat seluler", dan "Menyadari konsekuensi setiap tindakan" adalah bagian-bagian yang termasuk dalam kategori ini.

DAFTAR PUSTAKA

Agency, N. C. (n.d.). Cybercrime.

Antonius, A. (2019). *Multi-criteria Decision Analysis*. Bandung: CyberWhale.

APJII. (2024). Survey Penetasi Interrnet Indonesia.

Awaludin, M. (2019). Penerapan Algoritma K-Means Clustering Pada K-Harmonic Means Untuk Schedule Preventive Maintenance Service. *Jurnal Sistem Informasi Universitas Suryadarma*, *6*(1), 1–17. https://doi.org/10.35968/jsi.v6i1.271

Firdaus, V. F., Muksin, A., & Awaludin, M. (2022). *Analisis Faktor-Faktor Yang Mempengaruhi Audit Report Lag Dan Dampaknya Terhadap Abnormal Return Pada Perusahaan Sektor Energi Yang Terdaftar Di Bursa Efek Indonesia Periode 2020-2022*. 1–14.

Gardenia, Y., & Gani, A. G. (2024). Cybersecurity Awareness Model with Methods: Analytical Hierarchy Process and Structural Equation Model. *ICST Transactions on Scalable Information Systems*, *11*, 1–7. https://doi.org/10.4108/eetsis.6931

Haikal Arief, M., Arifa Fitri, K., & Malays Sari, E. (2024). Analisis Kesadaran Cyber Crime Di Kalangan Masyarakat Menengah Kebawah. *Tekinfo*, *2*(2), 24–39.

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security*, *25*(4), 289–296. https://doi.org/https://doi.org/10.1016/j.cose.2006.02.008

Kusumaningrum, A., Wijayanto, H., & Raharja, B. D. (2022). Pengukuran Tingkat Kesadaran Keamanan Siber di Kalangan Mahasiswa saat Study From Home dengan Multiple Criteria

Decision Analysis (MCDA). *Jurnal Ilmiah SINUS*, *20*(1), 69. https://doi.org/10.30646/sinus.v20i1.586

Mahendra, A. F., Hatta, P., & Aristyagama, Y. H. (2024). Analisis Tingkat Kesadaran Keamanan Cyber di Media Sosial Instagram: Studi Kasus pada Siswa SMK Negeri 1 Banyudono. *Bina Insani Ict Journal*, *11*(1), 86. https://doi.org/10.51211/biict.v11i1.2963

Prasetya, I. A., & Safriadi, N. (2015). Jurnal Sistem dan Teknologi Informasi. *Penerapan Visual Novel Dari Cerita Rakyat Asal Usul Kota Pontianak*, *1*(2), 1–5.

Saputra, S. (2022). *Analisis Pembuktian Hukum Perkara Tindak Pidana Penggelapan Melalui Elektronik Sistem (Studi Perkara Nomor 118/Pid. B/2021/PN Cbn)*. 1–24.

Widya Ramailis, N. (2020). Cyber Crime Dan Potensi Munculnya Viktimisasi Perempuan Di Era Teknologi Industri 4.0. *Sisi Lain Realita*, *5*(01), 1–20. https://doi.org/10.25299/sisilainrealita.2020.vol5(01).6381

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*, *62*(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269