Measuring Information Security Awareness at Muhammadiyah University of Palembang Using HAIS-Q

M. Rizky Mahendra[1)*)], Catur Eri Gunawan[2)], Freddy Kurnia Wijaya[3)]

[1)2)3)]Sistem Informasi, Sains dan Teknologi, Universitas Islam Negeri Raden Fatah Palembang
***)Correspondence author:** M. Rizky Mahendra, rizky.mahendr44@gmail.com, Palembang, Indonesia
DOI : https://doi.org/10.37012/jtik.v12i1.3379

Abstract

The rapid development of information technology has transformed various aspects of human life, including the way people work, interact, and learn. This progress has driven increased efficiency in daily activities, especially in higher education. The increasing dependence of the academic community on digital systems in academic and administrative activities has also increased information security risks in higher education. Muhammadiyah University of Palembang, which is undergoing a digital transformation, faces challenges in building information security awareness among its users. This study aims to measure the level of information security awareness of the academic community using quantitative methods through the Human Aspects of Information Security Questionnaire (HAIS-Q), which covers the dimensions of Knowledge, Attitude, and Behavior in 7 focus areas. The measurement stages refer to the Kruger & Kearney model with the determination of the importance weight of each focus area using the Analytic Hierarchy Process (AHP) method. The questionnaire data were analyzed descriptively. The results showed that the level of information security awareness was in the moderate category with a total score of 74.15%. The Knowledge dimension obtained a score of 70.39%, Attitude 75.63%, and Behavior 75.82%. The lowest scores were found in the sub-focus area of internet and social media usage behavior. This finding underscores the need for strategic interventions in the form of ongoing training, outreach, and technical policy development to strengthen information security awareness within universities, particularly in areas with low levels of awareness.

Keywords: *Information Security, Information Security Awareness, Use of Digital Systems in Higher Education, HAIS-Q, AHP.*

Abstrak

Perkembangan teknologi informasi yang berlangsung pesat telah mengubah berbagai aspek kehidupan manusia, termasuk cara bekerja, berinteraksi, hingga proses pembelajaran. Kemajuan ini mendorong peningkatan efisiensi dalam aktivitas sehari-hari, terutama di lingkungan pendidikan tinggi. Meningkatnya ketergantungan sivitas akademika pada sistem digital dalam aktivitas akademik dan administratif turut memperbesar risiko keamanan informasi di perguruan tinggi. Universitas Muhammadiyah Palembang yang sedang bertransformasi digital menghadapi tantangan dalam membangun kesadaran keamanan informasi di kalangan penggunanya. Penelitian ini bertujuan mengukur tingkat kesadaran keamanan informasi sivitas akademika menggunakan metode kuantitatif melalui kuesioner Human Aspects of Information Security Questionnaire (HAIS-Q), yang mencakup dimensi Pengetahuan, Sikap, dan Perilaku pada 7 fokus area. Tahapan pengukuran mengacu pada model Kruger & Kearney dengan penentuan bobot kepentingan tiap fokus area menggunakan metode Analytic Hierarchy Process (AHP). Data hasil kuesioner dianalisis secara deskriptif. Hasil penelitian menunjukkan tingkat kesadaran keamanan informasi berada pada kategori sedang dengan skor total 74,15%. Dimensi Pengetahuan memperoleh skor 70,39%, Sikap 75,63%, dan Perilaku 75,82%. Skor terendah ditemukan pada sub-fokus area perilaku penggunaan internet dan media sosial. Temuan ini menegaskan perlunya intervensi strategis berupa pelatihan, sosialisasi, dan penyusunan kebijakan teknis yang

berkelanjutan untuk memperkuat kesadaran keamanan informasi di lingkungan universitas, terutama pada area dengan tingkat kesadaran rendah.

Kata Kunci : Keamanan Informasi, Kesadaran Keamanan Informasi, Penggunaan Sistem Digital di Perguruan Tinggi, HAIS-Q, AHP.

PENDAHULUAN

Perkembangan teknologi informasi yang berlangsung pesat telah mengubah berbagai aspek kehidupan manusia, termasuk cara bekerja, berinteraksi, hingga proses pembelajaran. Kemajuan ini mendorong peningkatan efisiensi dalam aktivitas sehari-hari, terutama di lingkungan pendidikan tinggi. Di perguruan tinggi, pemanfaatan teknologi informasi telah menjadi bagian integral dari kegiatan akademik dan administratif. Sivitas akademika kini sangat bergantung pada berbagai sistem digital seperti SIMAK, E-learning, DIGILIB, Repository, serta media eksternal seperti media sosial dan email. Transformasi digital ini memberikan kemudahan dalam pengelolaan data, komunikasi, dan akses sumber belajar, sehingga meningkatkan efektivitas proses pendidikan (Ariyadi et al., 2023).

Namun, meningkatnya ketergantungan terhadap teknologi juga diikuti oleh eskalasi ancaman terhadap keamanan informasi. Kasus kebocoran data mahasiswa Universitas Diponegoro (UNDIP) pada 5 Januari 2021 menjadi contoh nyata, di mana lebih dari 125 ribu data mahasiswa bocor dan tersebar di internet, mencakup informasi pribadi seperti nama, tanggal lahir, alamat, serta data keluarga (Siaran Pers ELSAM, 2021). Kejadian ini menunjukkan bahwa perguruan tinggi memiliki kerentanan serius terhadap pelanggaran keamanan informasi dan memerlukan upaya sistematis untuk mencegah insiden serupa. Laporan Indonesia Threat Landscape Report oleh SOCRadar (2023) juga mencatat bahwa dari 130 insiden ransomware global pada 2023–2024, sebanyak 24 kasus terjadi di Indonesia. Sektor pendidikan turut terdampak dengan kontribusi 3,17% dari total serangan. Meskipun angka ini lebih rendah dibandingkan sektor industri lain, risiko terhadap institusi pendidikan tetap signifikan karena besarnya volume data sensitif yang dikelola, seperti data pribadi mahasiswa dan informasi akademik.

Faktor manusia menjadi penyebab utama berbagai insiden keamanan informasi. Laporan Verizon Data Breach Investigations Report (Hylender et al., 2024) menunjukkan

bahwa 68% kasus pelanggaran keamanan melibatkan elemen manusia. Sebagian besar terjadi akibat rendahnya kesadaran dan perilaku tidak aman pengguna, seperti menjadi korban phishing atau serangan social engineering. Teknik social engineering memanfaatkan kelemahan manusia sebagai titik terlemah dalam sistem, di mana penyerang memanipulasi korban agar secara tidak sadar memberikan akses atau informasi sensitif (Peltier, 2006; Tyas Darmaningrat et al., 2022; Syafitri et al., 2022). Rendahnya pengetahuan dan kesadaran pengguna terhadap keamanan informasi menjadikan faktor manusia sebagai ancaman dominan dalam insiden kebocoran data (Nugroho et al., 2024). Oleh karena itu, peningkatan kesadaran keamanan informasi menjadi langkah krusial untuk meminimalkan risiko pelanggaran (Rohan, Pal, et al., 2023). Perguruan tinggi perlu memahami sejauh mana tingkat kesadaran keamanan informasi di lingkungan internalnya untuk menentukan strategi peningkatan yang tepat.

Berdasarkan hal tersebut, penelitian ini bertujuan mengukur tingkat kesadaran keamanan informasi sivitas akademika di Universitas Muhammadiyah Palembang, yang mencakup mahasiswa, dosen, dan tenaga kependidikan. Pengukuran ini difokuskan pada penggunaan sistem digital yang dikelola universitas dalam mendukung aktivitas akademik dan administratif. Hasil penelitian diharapkan dapat menjadi dasar dalam perumusan kebijakan serta strategi peningkatan kesadaran keamanan informasi yang lebih efektif dan berkelanjutan, sesuai dengan kebutuhan dan karakteristik Universitas Muhammadiyah Palembang.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kuantitatif dengan metode survei untuk mengukur kesadaran keamanan informasi sivitas akademika Universitas Muhammadiyah Palembang dalam penggunaan sistem digital akademik dan administratif. Pengukuran dilakukan berdasarkan model Kruger & Kearney (2006) yang menilai dimensi Pengetahuan, Sikap, dan Perilaku, serta dioperasionalisasikan melalui instrumen HAIS-Q yang mencakup 7 fokus area: Manajemen Kata Sandi, Penggunaan Email, Penggunaan Internet, Penggunaan Media Sosial, Perangkat Mobile, Penanganan Data & Informasi, dan Pelaporan Insiden.

Populasi dalam penelitian ini adalah seluruh sivitas akademika Universitas Muhammadiyah Palembang yang aktif menggunakan sistem digital di lingkungan universitas. Data populasi diperoleh dari Biro PUSDATIN dan Biro SDM pada Mei 2025, dengan total sebanyak 11.970 orang. Penelitian ini menggunakan metode sampling acak sederhana dengan perhitungan jumlah sampel berdasarkan rumus Slovin. Metode ini dipilih karena jumlah populasi penelitian sangat besar, sehingga tidak memungkinkan untuk menjadikan seluruh anggota populasi sebagai responden. Untuk menentukan jumlah sampel minimum, perhitungan dilakukan menggunakan rumus Slovin dengan rumus n = N ÷ (1 + Ne^2) dengan n sebagai ukuran sampel, N sebagai jumlah populasi, 1 sebagai konstanta, dan e sebagai tingkat kesalahan (margin of error) (C. Wahyudi, 2023).

Mengingat adanya kendala dalam mendapatkan responden terutama karena jumlah item kuesioner yang cukup banyak dan memerlukan waktu pengisian yang lama, peneliti menetapkan margin of error sebesar 10% (0,1). Dari hasil perhitungan jumlah minimum responden yang dibutuhkan adalah 100 orang (dibulatkan ke atas). Untuk mengantisipasi adanya data yang tidak sesuai atau tidak lengkap, peneliti menaikkan minimum sampelnya sebesar 5% sehingga total jumlah responden yang ditetapkan menjadi 105 orang.

Sebelum pengukuran, dilakukan pembobotan kepentingan menggunakan metode Analytic Hierarchy Process (AHP) melalui formulir matriks pairwise comparison oleh pihak manajemen. Data dikumpulkan dengan menyebarkan kuesioner berbasis HAIS-Q kepada sampel yang dipilih menggunakan teknik sampling acak sederhana, dengan kriteria responden merupakan pengguna aktif sistem digital dan bersedia berpartisipasi. Data yang terkumpul dianalisis menggunakan statistik deskriptif untuk menggambarkan distribusi, persentase, pola, dan kecenderungan kesadaran pada setiap dimensi. Hasil analisis ditampilkan dalam bentuk tabel, grafik, dan peta kesadaran sesuai tahapan model Kruger & Kearney.

HASIL DAN PEMBAHASAN

Hasil Pengumpulan Data

Kuesioner penelitian disusun menggunakan platform Google Forms, kemudian disebarkan kepada sivitas akademika Universitas Muhammadiyah Palembang secara langsung (tatap muka) selama periode pengumpulan data, yaitu dari tanggal 28 Mei hingga 3 Juli 2025. Dari proses penyebaran tersebut, terkumpul total sebanyak 118 responden, yang terdiri dari 38 responden pada penyebaran skala kecil dan 80 responden dari penyebaran skala besar. Tahap penyebaran skala kecil dilakukan terlebih dahulu untuk keperluan pengujian validitas dan reliabilitas instrumen penelitian dan masih digunakan dalam pengumpulan data utama. Sedangkan kuesioner dari penyebaran skala besar digunakan dalam pengumpulan data utama untuk analisis penelitian.

Data Screening

Sebelum dilakukan pengolahan data, terlebih dahulu dilakukan proses screening terhadap hasil kuesioner untuk memastikan kelengkapan dan kesesuaian data dengan kriteria penelitian. Salah satu kriteria tambahan yang ditetapkan adalah lama responden berada di kampus. Responden yang berada di kampus kurang dari 1,5 tahun tidak dimasukkan dalam analisis, dengan pertimbangan bahwa pengalaman mereka dalam menggunakan sistem digital kampus masih terbatas. Sebaliknya, responden yang telah berada di kampus minimal 1,5 tahun dianggap memiliki pemahaman yang lebih memadai. Penetapan kriteria ini bertujuan untuk meminimalkan bias dari responden yang masih berada pada tahap adaptasi terhadap sistem digital kampus.

Pada tahap penyebaran skala kecil, kuesioner terlebih dahulu disebarkan untuk menguji validitas dan reliabilitas instrumen penelitian. Mengacu pada Perneger et al. (2015), ukuran sampel minimal 30 responden direkomendasikan dalam penyebaran awal untuk memperoleh kekuatan statistik yang memadai dalam mendeteksi potensi permasalahan. Dari total 38 kuesioner yang terkumpul, hanya 34 responden yang digunakan dalam analisis karena 4 responden tidak memenuhi kriteria yang telah ditetapkan. Jumlah tersebut telah

memenuhi rekomendasi ukuran sampel minimal sebagaimana disarankan oleh Perneger et al. (2015).

Selanjutnya, pada tahap penyebaran kuesioner skala besar terkumpul sebanyak 80 responden. Setelah dilakukan pengecekan, terdapat 3 responden yang tidak memenuhi kriteria, sehingga hanya 77 responden yang diambil. Dengan demikian, total data yang digunakan berasal dari gabungan kuesioner skala kecil (34 responden) dan skala besar (77 responden), sehingga jumlah keseluruhan adalah 111 responden. Selain itu, dilakukan pula transformasi pada nilai skala Likert di 20 pernyataan yang menggunakan reverse scoring, agar interpretasi data tetap konsisten.

Penentuan Bobot Fokus Area

Setelah diperoleh hasil pengukuran dari masing-masing dimensi, langkah selanjutnya adalah menghitung bobot kepentingan untuk Fokus Area yang belum diketahui. Adapun bobot kepentingan untuk masing-masing Dimensi telah ditetapkan berdasarkan penelitian Kruger dan Kearney (2006), sebagaimana ditampilkan pada Tabel 1.

Tabel 1. Bobot Kepentingan Dimensi (Sumber: Kruger & Kearney, 2006)

Dimensi	Bobot
Pengetahuan	30%
Sikap	20%
Perilaku	50%

Perhitungan bobot untuk setiap Fokus Area dilakukan dengan menggunakan formulir pairwise comparison yang dirancang berdasarkan metode AHP. Proses pengisian formulir dilakukan oleh manajemen yang memiliki kewenangan langsung dalam pengelolaan sistem digital di lingkungan universitas, yaitu BIRO PUSDATIN. Dalam penelitian ini, pengisian formulir dilakukan oleh Kepala Biro PUSDATIN sebagai pemangku kepentingan tertinggi sekaligus pihak yang memiliki pemahaman paling komprehensif terkait operasional, kebijakan, serta pengelolaan keamanan sistem digital Universitas Muhammadiyah Palembang.

Berdasarkan hasil perhitungan yang dilakukan menggunakan AHP Priority Calculator, diperoleh nilai Consistency Ratio (CR) sebesar 5,7%, yang berada di bawah ambang batas maksimum 10%. Hal ini menunjukkan bahwa hasil perhitungan tersebut konsisten dan dapat diterima. Nilai bobot kepentingan dari masing-masing fokus area ditampilkan pada Tabel 2.

Tabel 2. Hasil Perhitungan Bobot Kepentingan Fokus Area

No.	Fokus Area	Bobot Kepentingan
1.	Manajemen *Password*	17,8%
2.	Penggunaan *Email*	17,2%
3.	Penggunaan Internet	21,5%
4.	Penggunaan Media Sosial	3,2%
5.	Perangkat *Mobile*	2,6%
6.	Penanganan Data & Informasi	21,7%
7.	Pelaporan Insiden	15,9%

Pengukuran Tingkat Kesadaran Keamanan Informasi Keseluruhan

Setelah diperoleh nilai tingkat kesadaran dan bobot kepentingan untuk seluruh fokus area dan dimensi, maka dapat dihitung nilai tingkat kesadaran secara keseluruhan dengan menggunakan model skoring dari Kruger & Kearney (2006). Adapun tahapan perhitungannya adalah sebagai berikut:

1. Menghitung nilai rata-rata setiap sub-fokus area dan fokus area pada ketiga dimensi: Pengetahuan, Sikap, dan Perilaku, sebagaimana telah dijelaskan pada subbab sebelumnya.
2. Menghitung tingkat kesadaran per fokus area, dengan cara mengalikan nilai rata-rata fokus area pada masing-masing dimensi dengan bobot dari tiap dimensi, kemudian menghitung nilai rata-ratanya.
3. Menghitung tingkat kesadaran per dimensi, dengan cara mengalikan nilai fokus area dengan bobot masing-masing fokus area dalam dimensi tersebut, lalu menghitung nilai rata-ratanya.
4. Menghitung tingkat kesadaran total, yaitu dengan mengalikan nilai rata-rata kesadaran setiap dimensi dengan bobot dari masing-masing dimensi, kemudian menghitung nilai totalnya.

Hasil perhitungan tingkat kesadaran secara keseluruhan ditampilkan pada Tabel 3.

Tabel 1. Nilai Tingkat Kesadaran secara Keseluruhan

Fokus Area	Dimensi			Nilai Kesadaran/Fokus Area
	Pengetahuan (Bobot 30%)	**Sikap** (Bobot 20%)	**Perilaku** (Bobot 50%)	
Manajemen *Password* (Bobot 17,8%)	69,43%	79,40%	78,38%	75,90%
Penggunaan *Email* (Bobot 17,2%)	73,57%	73,93%	77,60%	75,66%
Penggunaan Internet (Bobot 21,5%)	58,62%	75,56%	69,73%	67,56%
Penggunaan Media Sosial (Bobot 3,2%)	62,16%	75,74%	67,87%	67,73%
Perangkat *Mobile* (Bobot 2,6%)	77,54%	74,29%	75,44%	75,84%
Penanganan Data & Informasi (Bobot 21,7%)	74,89%	75,20%	80,78%	77,90%
Pelaporan Insiden (Bobot 15,9%)	78,74%	74,59%	74,65%	75,87%
Nilai Kesadaran/Dimensi	70,39%	75,63%	75,82%	
Nilai Tingkat Kesadaran Total	74,15%			

Berdasarkan Tabel 3, Pada Fokus Area Penggunaan Internet Di Dimensi Pengetahuan Berada Pada Kategori Buruk (58,62%) Dan Pada Fokus Area Penanganan Data & Informasi Berada Pada Kategori Baik (80,78%), Dan Sisa Fokus Area-Nya Berada Pada Kategori Sedang. Jika Dilihat Berdasarkan Nilai Kesadaran/Dimensi Dan Nilai Kesadaran/Fokus Area, Nilai Keduanya Berada Dalam Kategori Tingkat Kesadaran Sedang. Secara Keseluruhan, Nilai Tingkat Kesadaran Sivitas Akademika Universitas Muhammadiyah Palembang Terhadap Keamanan Informasi Berada Pada Kategori Sedang, Dengan Skor Akhir Sebesar 74,15%.

KESIMPULAN DAN REKOMENDASI

Berdasarkan hasil pengukuran tingkat kesadaran secara keseluruhan, tingkat kesadaran sivitas akademika Universitas Muhammadiyah Palembang terhadap keamanan informasi berada pada kategori sedang, dengan nilai sebesar 74,16%. Secara rinci, tingkat kesadaran pada dimensi Sikap sebesar 75,77%, dimensi Perilaku sebesar 75,73%, dan dimensi Pengetahuan sebesar 70,49%, seluruhnya berada dalam kategori sedang. Jika dilihat berdasarkan fokus area, masih terdapat fokus area yang masuk dalam kategori buruk, yaitu fokus area Penggunaan Internet. Sebagian besar fokus area lainnya berada pada kategori sedang, dan hanya satu fokus area yang masuk kategori baik.

Berdasarkan hasil penelitian ini, disarankan agar Universitas Muhammadiyah Palembang menindaklanjuti temuan terkait rendahnya tingkat kesadaran keamanan informasi pada beberapa fokus area, khususnya yang berada dalam kategori buruk. Evaluasi lebih lanjut perlu dilakukan oleh unit terkait, seperti Biro Pusdatin, untuk mengidentifikasi akar penyebab rendahnya kesadaran pada area tersebut. Selain itu, hasil penelitian ini dapat menjadi dasar dalam menyusun program peningkatan kesadaran keamanan informasi.

REFERENSI

Alvito, G. B. N., Setiadi, F., & Irsan, M. (2025). Pengukuran tingkat kesadaran keamanan informasi pada mahasiswa Fakultas Informatika menggunakan Human Aspect of Information Security Questionnaire. *LOGIC: Jurnal Ilmu Komputer*. https://journals.telkomuniversity.ac.id/logic/article/view/9590

Anugrah, S., Himawan, M. Z., Qalby, N. R., et al. (2025). Pengaruh etika profesi terhadap keamanan informasi dalam konteks kebocoran data BSI (Bank Syariah Indonesia): Studi literatur sistematis. *Jurnal Teknologi Informasi*. https://ojs.unikom.ac.id/index.php/JTK3TI/article/view/17033

Ariyadi, T., Widodo, T. L., Apriyanti, N., & Kirana, F. S. (2023). Analisis kerentanan keamanan sistem informasi akademik Universitas Bina Darma menggunakan OWASP. *Techno.Com, 22*(2), 418–429. https://doi.org/10.33633/tc.v22i2.7562

Darmansah, T., Pasaribu, G. A., Juliani, D., et al. (2025). Optimalisasi sistem informasi administrasi digital untuk meningkatkan efisiensi layanan dan keamanan informasi organisasi. *Jurnal Penelitian Ilmu-Ilmu Sosial*. https://www.ojs.daarulhuda.or.id/index.php/Socius/article/view/1489

Hylender, D., Langlois, P., Pinto, A., & Widup, S. (2024). *2024 data breach investigations report*. Verizon. https://www.verizon.com/business/resources/Tad3/reports/2024-dbir-data-breach-investigations-report.pdf

Karunia, W. A., Zahra, A. F., et al. (2025). Evaluasi ancaman baru dalam keamanan informasi: Systematic literature review tentang kerentanan cyber security pasca-pandemi. *Cyber Security Journal*. https://journal.uin-suka.ac.id/saintek/cybersecurity/article/view/4889

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

Nadanta, A. H., Farisi, H., & Brata, D. W. (2025). Analisis evaluasi indeks KAMI (Keamanan Informasi) 5.0 dalam pengelolaan keamanan informasi di SMK Telkom Purwokerto. *J-PTIIK*. https://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/15233

Nugraha, F., & Hendrik, B. (2025). Perbandingan framework COBIT 2019 dan TOGAF dalam manajemen keamanan informasi. *Journal of Education Research*. https://jer.or.id/index.php/jer/article/view/2156

Nugroho, M. A., Asih, S. W., & Karunia, A. N. (2024). Peran kesadaran manusia dalam keamanan informasi dan social engineering. *Bureaucracy Journal, 4*(1), 199–216. https://bureaucracy.gapenas-publisher.org/index.php/home/article/view/401

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The human aspects of information security questionnaire (HAIS-Q): Two further validation studies. *Computers & Security, 66*, 40–51. https://doi.org/10.1016/j.cose.2017.01.004

Rohan, R., Pal, D., Hautamäki, J., Funilkul, S., Chutimaskul, W., & Thapliyal, H. (2023). A systematic literature review of cybersecurity scales assessing information security awareness. *Heliyon, 9*(3). https://doi.org/10.1016/j.heliyon.2023.e14234

Siaran Pers ELSAM. (2021, Januari 6). Data mahasiswa UNDIP bocor: RUU pelindungan data pribadi penting segera disahkan. Diakses Januari 7, 2025, dari https://www.elsam.or.id/siaran-pers/data-mahasiswa-undip-bocor-ruu-pelindungan-data-pribadi-penting-segera-disahkan

SOCRadar. (2023). *Healthcare threat landscape report* (Vol. 1, pp. 1–14). https://media.cert.europa.eu/static/MEMO/2021/TLP-WHITE-CERT-EU-Threat_Landscape_Report-Volume1.pdf

Syafitri, W., Shukur, Z., Mokhtar, U. A., Sulaiman, R., & Ibrahim, M. A. (2022). Social engineering attacks prevention: A systematic literature review. *IEEE Access, 10*, 39325–39343. https://doi.org/10.1109/ACCESS.2022.3162594

Tyas Darmaningrat, E. W., Noor Ali, A. H., Herdiyanti, A., Subriadi, A. P., Muqtadiroh, F. A., Astuti, H. M., & Susanto, T. D. (2022). Sosialisasi bahaya dan upaya pencegahan social engineering untuk meningkatkan kesadaran masyarakat tentang keamanan informasi. *Sewagati, 6*(2). https://doi.org/10.12962/j26139960.v6i2.92

Wahyudi, C. (2023). Peningkatan minat siswa dalam meneliti sejarah lokal melalui program kunjungan museum perjuangan rakyat Jambi. *Allimna: Jurnal Pendidikan Profesi Guru, 2*(2), 111–126. https://doi.org/10.30762/allimna.v2i02