Journal of Informatics, Electrical and Electronics Engineering
ISSN 2807-9507 (Media Online)
Vol 5, No 2, December 2025
Hal 208-216
https://djournals.com/jieee

Analisis Kesadaran Keamanan Informasi Penggunaan Layanan M-Banking Menggunakan Human Aspects of Information Security Questionnaire

Ngurah Gede Prema Satya Ananda[1,*], Gede Arna Jude Saskara[1], Bagus Gede Krishna Yudistira[2]

[1] Fakultas Teknik dan Kejuruan, Program Studi Sistem Informasi, Universitas Pendidikan Ganesha, Singaraja, Indonesia
[2] Fakultas Teknik dan Kejuruan, Program Studi Pendidikan Teknik Informatika, Universitas Pendidikan Ganesha, Singaraja, Indonesia
Email: [1,*]prema.satya@undiksha.ac.id, [2]jude.saskara@undiksha.ac.id, [3]krishna.yudistira@undiksha.ac.id
Email Penulis Korespondensi: prema.satya@undiksha.ac.id

Abstrak−Penelitian ini mengkaji masalah kesenjangan antara pemahaman dan praktik keamanan informasi pada pegawai Dinas Perdagangan, Perindustrian, dan Koperasi Usaha Kecil dan Menengah Kabupaten Buleleng dalam menggunakan layanan M-Banking yang rentan terhadap phishing. Tujuannya adalah untuk mengukur tingkat kesadaran keamanan informasi secara keseluruhan dan mengidentifikasi area terlemah sebagai dasar rekomendasi mitigasi yang lebih terfokus. Penelitian ini menggunakan pendekatan kuantitatif dengan metode survei terhadap 119 pegawai. Instrumen penelitian dikembangkan berdasarkan kerangka Human Aspects of Information Security Questionnaire (HAIS-Q) untuk mengukur dimensi Pengetahuan, Sikap, dan Perilaku. Data yang terkumpul dianalisis menggunakan metode Multiple Weighted Score Analysis (MWSA) untuk menentukan skor dan peringkat kerentanan. Tingkat kesadaran keamanan informasi pegawai secara umum berada pada kategori "Baik" dengan skor 3,69. Meskipun demikian, temuan ini mengungkap adanya knowledge-attitude-behavior gap yang signifikan, dimana skor Pengetahuan dan Sikap yang tergolong "Baik" tidak diimbangi dengan skor dimensi Perilaku yang terkategori "Sedang". Untuk menjembatani kesenjangan ini, rekomendasi difokuskan pada pembuatan Standar Operasional Prosedur (SOP) yang dirancang sebagai alat untuk membentuk kebiasaan yang aman. Agar efektif, implementasi SOP ini didukung oleh kegiatan sosialisasi yang berorientasi pada perubahan perilaku, dan bukan sekadar penyampaian informasi. Sosialisasi ini perlu disertai pelatihan dan simulasi langsung, khususnya simulasi serangan phishing.

Kata Kunci: HAIS-Q; Kesadaran Keamanan; M-Banking; MWSA

Abstract−This study examines the gap between information security understanding and practice among employees of the Department of Trade, Industry, Cooperatives, Small and Medium Enterprises of Buleleng Regency when using M-Banking services vulnerable to phishing. Its objective is to measure the overall level of information security awareness and identify the weakest areas to serve as a basis for more focused mitigation recommendations. This research employs a quantitative approach using a survey method involving 119 employees. The research instrument was developed based on the Human Aspects of Information Security Questionnaire (HAIS-Q) framework to measure the dimensions of Knowledge, Attitude, and Behavior. The collected data were analyzed using the Multiple Weighted Score Analysis (MWSA) method to determine vulnerability scores and rankings. The overall level of employees' information security awareness falls into the "Good" category with a composite score of 3.69. However, the findings reveal a significant knowledge-attitude-behavior gap, where the "Good" scores for Knowledge and Attitude dimensions are not matched by the Behavior dimension score, which is categorized as "Moderate." To bridge this gap, recommendations focus on developing Standard Operating Procedures (SOPs) designed as tools to foster secure habits. For effectiveness, SOP implementation must be supported by socialization activities oriented towards behavioral change, rather than mere information dissemination. This socialization should include practical training and direct simulations, particularly phishing attack simulations.

Keywords: HAIS-Q; Security Awareness; M-Banking; MWSA

1. PENDAHULUAN

Seiring dengan pergeseran masif aktivitas masyarakat ke platform digital, internet kini berfungsi sebagai infrastruktur utama. Jaringan internet ini tidak hanya memfasilitasi konektivitas, tetapi juga menyediakan ekosistem layanan yang beragam untuk mendukung interaksi virtual, salah satunya melalui platform media sosial [1]. Berdasarkan data hasil survey dari Asosiasi Penyelenggara Jasa Internet Indonesia atau disebut dengan APJII yang dibagikan oleh Finaka et al. [2], pengguna internet di Indonesia mengalami peningkatan mencapai 210.026.769 jiwa pada periode 2021-2022, dengan 64% masyarakat kini menggunakan aplikasi finansial melalui *smartphone*. Namun, kemudahan ini diikuti dengan lonjakan insiden siber hingga lima kali lipat berdasarkan laporan dari Badan Siber dan Sandi Negara Tahun 2020 [3]. Serangan ini tidak lagi terbatas pada ancaman teknis semata, melainkan semakin mengeksploitasi faktor manusia melalui rekayasa sosial (*Social engineering*), dengan *phishing* menjadi salah satu sektor serangan yang paling dominan, khususnya menargetkan sektor publik dan keuangan. Data ini mengindikasikan tingginya penggunaan mobile banking di Indonesia, yang diperkirakan terus meningkat setiap tahun. Menurut Ramadhan & Purwandari [4] yang mengatakan bahwa aktivitas masyarakat, seperti bersosial media, bertransaksi, dan menyimpan data di internet, turut meningkatkan utilisasi layanan perbankan digital. Sehingga faktor sumber daya manusia menjadi penyebab dominan terjadinya pelanggaran keamanan informasi. Oleh karena itu, diperlukan pengukuran tingkat kesadaran keamanan informasi untuk mengetahui sejauh mana tingkat kesadaran tersebut dimiliki oleh individu terkait [5]. Sebagaimana juga dilakukan pada mahasiswa akuntansi untuk menilai kesiapan mereka dalam menghadapi risiko keamanan informasi [6]

Kerentanan pada aspek manusia ini diperkuat oleh temuan awal yang diidentifikasi di lingkungan Dinas Perdagangan, Perindustrian, dan Koperasi Usaha Kecil dan Menengah Kabupaten Buleleng, di mana beberapa pegawai telah menjadi sasaran upaya *phishing*. Meskipun tidak ada kerugian finansial, insiden-insiden berikut mengungkap celah

kesadaran pada perilaku keamanan yang signifikan. Beberapa insiden pegawai yang diketahui adalah beberapa pegawai menerima dan mengakses tautan *phishing*, meskipun tidak sampai mengisi data pribadi, tindakan mengakses tautan itu sendiri menunjukkan rendahnya pengetahuan dan sikap terhadap bahaya *phishing* karena sudah membuka risiko infeksi *malware*. Insiden lain menunjukkan seorang pegawai yang menjawab panggilan telepon *phishing* namun tidak mengaktifkan fitur perlindungan preventif seperti *auto-blocker*, serta pegawai lain yang tetap mengklik dan mengakses tautan palsu dari WhatsApp karena tidak mengaktifkan fitur peramban yang aman. Kejadian tersebut secara konsisten menunjukkan adanya kesenjangan antara pengetahuan dan praktik keamanan, atau *Knowledge-Attitude-Behavior Gap*. Sejumlah penelitian terkait, seperti yang dilakukan oleh [4], [7], serta [8], secara konsisten menemukan adanya fenomena *Knowledge-Attitude-Behavior Gap*, di mana skor pengetahuan dan sikap pengguna yang tinggi tidak diimbangi oleh skor perilaku yang rendah. Analisis lebih lanjut menunjukkan bahwa perbedaan mendasar penelitian ini terletak pada kedalaman analisisnya. Penelitian-penelitian sebelumnya cenderung berhenti pada kesimpulan umum bahwa perilaku adalah dimensi terlemah, tanpa secara sistematis mengidentifikasi dan memetakan indikator-indikator spesifik mana di dalam dimensi perilaku tersebut yang menjadi titik paling lemah ketitik yang paling kuat. Selain itu, analisis ini juga memetakan mengenai perbandingan berdasarkan karakteristik responden yang bertujuan untuk menggali temuan lebih lanjut dengan membandingkan skor kesadaran keamanan informasi terhadap data karakteristik responden yang telah dikumpulkan.

Alasan utama penelitian ini diadakan adalah untuk mengisi kekosongan tersebut dengan berfokus pada konteks organisasi pemerintahan daerah yang masih jarang dieksplorasi dengan melakukan pendekatan dari metode *Kruger and Kearney*. Menurut penelitian yang dibagikan oleh Maulidi [9], metode *Kruger and Kearney* merupakan pendekatan dari psikologi sosial dan digunakan untuk membuat alat pengukuran tertentu. Pendekatan ini berfokus pada tiga hal yaitu sikap, perilaku, dan pemahaman yang dianggap dapat memengaruhi bagaimana seseorang berpikir atau bertindak terhadap sesuatu. Kruger dan Kearney kemudian mengembangkan metode ini menjadi tiga dimensi pengukuran, yang dikenal dengan istilah *KAB* (*Knowledge, Attitude, Behavior*) atau pengetahuan, sikap, dan perilaku. Dimensi ini digunakan untuk menilai aspek-aspek penting yang dapat berpengaruh terhadap suatu objek atau isu yang diteliti. Untuk itu, penelitian ini menggunakan instrumen *Human Aspects of Information Security Questionnaire* (*HAIS-Q*) yang didasarkan pada kerangka kerja *KAB* dan telah tervalidasi untuk mengukur tiga dimensi kesadaran (Pengetahuan, Sikap, dan Perilaku) beserta indikatornya (*Password Management, Email Use, Internet Use, Mobile Device* dan *Incident Reporting*) [10]. Kebaruan dan perbedaan utama penelitian ini terletak pada metode analisisnya, yaitu menggunakan pendekatan deskriptif kuantitatif dengan metode *Multiple Weighted Score Analysis* (*MWSA*), yang diadaptasi dari penelitian [11]. Pendekatan *MWSA* memungkinkan penelitian ini tidak hanya mengonfirmasi adanya kesenjangan, tetapi juga secara spesifik mengidentifikasi, memetakan, dan menyusun peringkat kerentanan pada setiap dimensi dan indikator secara objektif, sejalan dengan pendekatan MCDA yang digunakan dalam pengukuran kesadaran keamanan informasi [12].

Berdasarkan hal tersebut, pertanyaan tujuan penelitian ini adalah: (1) Bagaimana tingkat kesadaran keamanan informasi pegawai Dinas Perdagangan, Perindustrian, dan Koperasi UKM Kabupaten Buleleng berdasarkan pengukuran menggunakan metode *Human Aspects of Information Security Questionnaire* (*HAIS-Q*)? dan (2) Dimensi dan indikator mana yang memiliki tingkat kesadaran paling rendah dan dapat dijadikan dasar utama dalam menentukan prioritas rekomendasi mitigasi terhadap kerentanan keamanan informasi?. Penelitian ini diharapkan dapat memberikan rekomendasi yang lebih terfokus dan berbasis bukti, bukan sekadar saran umum, untuk menjembatani kesenjangan antara pemahaman dan praktik keamanan di lingkungan pemerintahan.

2. METODOLOGI PENELITIAN

2.1 Kerangka Dasar Penelitian

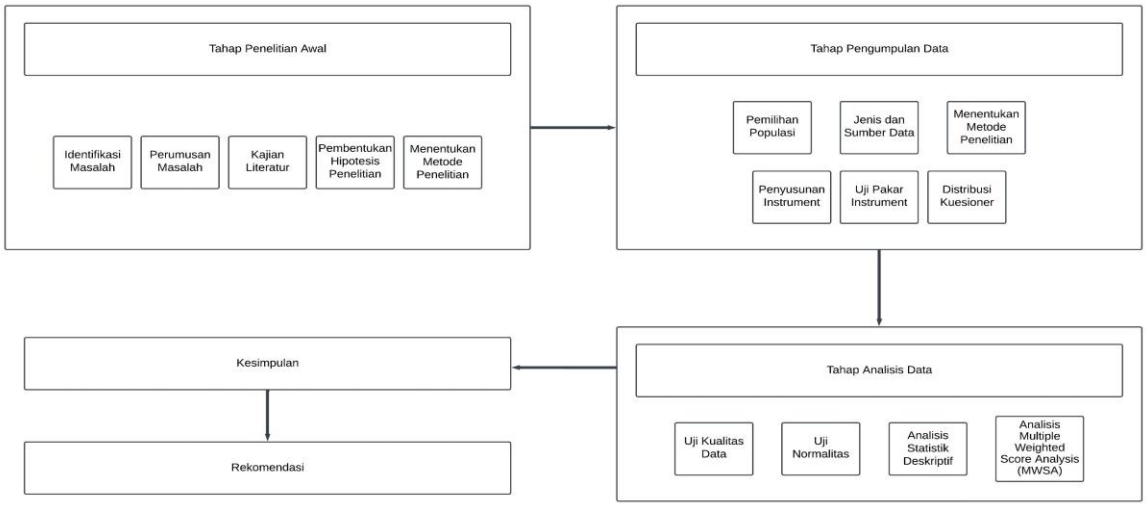
Penelitian ini menggunakan pendekatan deskriptif kuantitatif dengan metode survei untuk mengukur tingkat kesadaran keamanan informasi dalam penggunaan layanan M-Banking. Lokasi penelitian adalah Dinas Perdagangan, Perindustrian, dan Koperasi Usaha Kecil dan Menengah Kabupaten Buleleng. Populasi dalam penelitian ini adalah seluruh pegawai aktif yang berjumlah 119 orang pada tahun 2025. Sebelum survei utama, dilakukan uji validitas instrumen terhadap 30 pegawai Dinas Perdagangan, Perindustrian, dan Koperasi Usaha Kecil dan Menengah Kabupaten Buleleng yang dipilih secara acak (*Random sampling*). Data primer dikumpulkan menggunakan kuesioner yang dikembangkan berdasarkan kerangka *Human Aspects of Information Security Questionnaire* (*HAIS-Q*). Instrumen ini mengukur tiga dimensi utama kesadaran keamanan informasi, yaitu Pengetahuan (*Knowledge*), Sikap (*Attitude*), dan Perilaku (*Behavior*). Setiap dimensi diukur melalui lima indikator yang relevan dengan penggunaan layanan M-Banking. Setiap butir pernyataan dalam kuesioner menggunakan *Skala Likert* dengan rentang 1 (Sangat tidak setuju) hingga 5 (Sangat setuju) [13]. Proses pengumpulan data dilakukan secara luring dengan membagikan lembar kuesioner cetak kepada seluruh responden. Data sekunder berupa jumlah pegawai keseluruhan dan gambaran umum permasalahan diperoleh melalui wawancara dengan Kepala Bidang Kepegawaian.

Alur pemikiran yang mendasari penelitian ini dimulai dari fenomena meluasnya penggunaan layanan *M-Banking* yang diiringi dengan meningkatnya ancaman siber yang menargetkan faktor manusia, seperti *phishing*. Temuan awal di Dinas Perdagangan, Perindustrian, dan Koperasi Usaha Kecil dan Menengah Kabupaten Buleleng mengindikasikan adanya kerentanan pada pegawai terhadap serangan rekayasa sosial, meskipun tidak menimbulkan kerugian finansial. Hal

ini memunculkan dugaan adanya kesenjangan antara apa yang diketahui dan apa yang dilakukan oleh para pegawai dalam praktik keamanan sehari-hari. Fenomena ini dapat dijelaskan melalui kerangka teori *Knowledge-Attitude-Behavior* (*KAB*) yang menyatakan bahwa tingkat pengetahuan yang tinggi dan sikap yang positif tidak selalu berbanding lurus dengan penerapan perilaku yang aman. Untuk membuktikan dan mengukur kesenjangan ini secara empiris, penelitian ini menggunakan instrumen *Human Aspects of Information Security Questionnaire* (*HAIS-Q*) yang valid untuk mengukur ketiga dimensi *KAB*. Untuk memberikan rekomendasi yang lebih tajam dan terprioritaskan, penelitian ini akan menganalisis lebih dalam guna mengidentifikasi dimensi dan indikator mana yang menjadi titik terlemah. Hasil dari analisis ini akan menjadi dasar penyusunan rekomendasi mitigasi yang lebih strategis dan efektif, sesuai dengan kebutuhan spesifik di lokasi penelitian.

2.2 Tahapan Penelitian

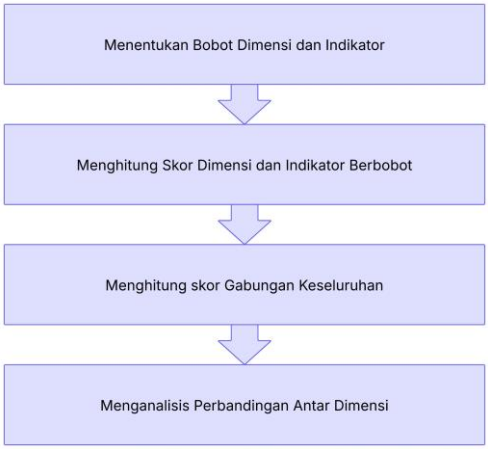
Penelitian ini dilaksanakan melalui beberapa tahapan. Tahap Penelitian Awal mencakup identifikasi masalah terkait ancaman *phishing* pada *M-Banking*, perumusan tujuan, kajian literatur sebagai landasan teori, dan penyusunan kerangka konseptual. Tahap Pengumpulan Data melibatkan pemilihan populasi yang relevan, yaitu pegawai Dinas Perdagangan, Perindustrian dan Koperasi Usaha Kecil dan Menengah Kabupaten Buleleng, serta uji reliabilitas untuk memastikan konsistensi instrumen dan pengumpulan data menggunakan kuesioner. Tahap Analisis Data meliputi uji kualitas data, uji normalitas, analisis statistik deskriptif untuk memahami pola data dan melakukan analisis *Multiple Weighted Score Analysis* (*MWSA*). Terakhir, pada Tahap Kesimpulan dan Rekomendasi, peneliti menyusun kesimpulan dari temuan utama dan memberikan saran untuk meningkatkan kesadaran terhadap ancaman phishing pada perbankan digital. Berikut adalah alur tahapan penelitian yang akan dipaparkan secara rinci pada Gambar 1.



Gambar 1. Alur Penelitian

2.3 Teknik Analisis Multiple Weighted Score Analysis (MWSA)

Data yang terkumpul dianalisis menggunakan statistik deskriptif kuantitatif dengan metode *Multiple Weighted Score Analysis* (*MWSA*). Metode ini digunakan untuk menghitung skor rata-rata, memberikan bobot pada setiap dimensi dan indikator, serta menyusun peringkat kerentanan berdasarkan skor berbobot tersebut. Alur Analisis *Multiple Weighted Score Analysis* (*MWSA*) dapat dilihat pada Gambar 2.



Gambar 2. Alur Analisis Multiple Weighted Score Analysis (MWSA)

Adapun alur analisis MWSA secara rinci, [1] [2] [3] [4] adalah sebagai berikut:

a. Menentukan bobot dimensi dan indikator
Tahap analisis diawali dengan penentuan bobot (*Weighting*) untuk setiap dimensi dan indikator guna mengukur kontribusi relatifnya. Bobot ini dihitung secara empiris dari data respons kuesioner. Prosesnya melibatkan penghitungan nilai rata-rata (*Mean*) dari skor *Skala Likert* untuk setiap komponen. Bobot kemudian diperoleh dengan menormalisasi nilai rata-rata setiap komponen terhadap jumlah total nilai rata-rata. Dengan demikian, komponen dengan skor rata-rata lebih tinggi secara proporsional akan memberikan kontribusi yang lebih signifikan terhadap hasil analisis akhir. Secara matematis, bobot dimensi dihitung dengan rumus:

$$w_i = \frac{\bar{x_i}}{\sum_{j=1}^{n} \bar{x}_j} \quad (1)$$

Dalam rumus tersebut, w_i merepresentasikan bobot ternormalisasi untuk dimensi ke-i. Nilai ini dihitung dengan membagi ($\bar{x_i}$), yang merupakan nilai rata-rata dari dimensi ke-i, dengan jumlah total dari nilai rata-rata seluruh dimensi (n) yang dianalisis.

b. Menghitung skor dimensi berbobot
Setelah bobot ditentukan, skor berbobot (*Weighted score*) dihitung untuk setiap komponen. Proses ini dilakukan dengan mengalikan nilai rata-rata (*Mean*) dari setiap dimensi dan indikator dengan bobotnya masing-masing. Hasilnya adalah skor yang telah disesuaikan dengan tingkat kepentingan relatif setiap komponen, sehingga memberikan gambaran performa yang lebih akurat dan proporsional dibandingkan skor rata-rata mentah. Secara matematis, bobot dimensi dihitung dengan rumus:

$$s_{ik} = \bar{x}_{ik} \times w_{ik} \quad (2)$$

Dalam rumus di atas, s_{ik} adalah skor berbobot final untuk indikator ke-k pada dimensi ke-i. Nilai ini diperoleh dengan mengalikan $\bar{x}_{ik}$, yang merupakan nilai rata-rata indikator tersebut dari hasil kuesioner, dengan w_{ik} yaitu bobot proporsional yang telah dihitung untuk indikator yang sama.
Setelah skor berbobot indikator dihitung, langkah selanjutnya adalah menjumlahkan seluruh skor berbobot indikator dalam satu dimensi. Nilai ini kemudian dikalikan dengan bobot dimensi yang telah ditentukan. Rumus perhitungan skor berbobot dimensi dapat dituliskan sebagai berikut.

$$s_i = (\sum_{k=1}^{m} s_{ik}) \times w_i \quad (3)$$

Dalam rumus ini, s_i merepresentasikan skor berbobot akhir untuk dimensi ke-i. Nilai ini dihitung dengan menjumlahkan seluruh s_{ik}, yang merupakan skor berbobot dari setiap indikator ke-k di dalam dimensi tersebut, di mana proses penjumlahan dilakukan untuk semua indikator hingga m, yaitu jumlah total indikator dalam dimensi ke-i. Hasil penjumlahan tersebut kemudian dikalikan dengan w_i, yang merupakan bobot proporsional untuk dimensi ke-i itu sendiri.

c. Menghitung skor gabungan keseluruhan
Tahap ketiga dalam analisis *Multiple Weighted Score Analysis* (*MWSA*) adalah menghitung skor gabungan keseluruhan yang merepresentasikan tingkat pencapaian responden pada seluruh dimensi dan indikator penelitian. Skor gabungan ini diperoleh dengan menjumlahkan seluruh skor berbobot dimensi yang telah dihitung pada tahap sebelumnya, sehingga menghasilkan nilai agregat yang mencerminkan kinerja keseluruhan dari variabel penelitian. Adapun rumus yang digunakan untuk menghitung skor gabungan ini adalah sebagai berikut.

$$S\ total = \sum_{i=1}^{n} \sum_{k=1}^{m_i} (\bar{x}_i k \times w_{ik} \times w_i) \quad (4)$$

Dalam rumus ini, skor total dihitung melalui penjumlahan ganda. Penjumlahan pertama dilakukan untuk semua n, yaitu jumlah dimensi keseluruhan, dan penjumlahan kedua dilakukan untuk semua m_i, yang merupakan jumlah indikator pada dimensi ke-i. Perhitungan intinya melibatkan perkalian tiga variabel: $\bar{x}_i k$, yaitu nilai rata-rata indikator ke-k pada dimensi ke-i; w_{ik}, yang merupakan bobot proporsional untuk indikator dan w_i, yaitu bobot untuk dimensi ke-i itu sendiri. Hasil akhir dari rumus ini adalah skor komposit yang selanjutnya diklasifikasikan ke dalam kategori tertentu (misalnya "Baik", "Sedang", atau "Buruk") berdasarkan interval skor yang telah ditetapkan.

d. Menganalisis perbandingan antar dimensi
Analisis perbandingan antar dimensi dan indikator dalam metode *Multiple Weighted Score Analysis* (*MWSA*) bertujuan untuk mengidentifikasi prioritas relatif dari masing-masing dimensi maupun indikator berdasarkan skor berbobot yang telah dihitung sebelumnya. Sehingga penelitian ini tidak hanya memberikan gambaran umum mengenai tingkat pengetahuan, sikap, dan perilaku pegawai terhadap keamanan informasi penggunaan layanan *M-Banking*, tetapi juga mampu menunjukkan indikator mana yang memiliki kontribusi paling besar terhadap keseluruhan konstruk penelitian.

ISSN 2807-9507 (Media Online)
Vol 5, No 2, December 2025
Hal 208-216
https://djournals.com/jieee

3. HASIL DAN PEMBAHASAN

3.1 Hasil Penelitian

Penelitian ini berhasil menjangkau keseluruhan populasi target, dengan total 119 pegawai aktif di Dinas Perdagangan, Perindustrian, dan Koperasi Usaha Kecil dan Menengah Kabupaten Buleleng yang mengembalikan kuesioner secara lengkap. Karakteristik demografis responden yang relevan, seperti jenis kelamin, rentang usia, dan masa kerja, diringkas pada Tabel 1. Data ini penting untuk memahami konteks responden dan memastikan keterwakilan populasi dalam sampel.

Tabel 1. Data Karakteristik Responden

Deskriptif	Keterangan	Frekuensi	Persentasi (%)
Rentang Usia	Di bawah 25 tahun	2	2%
	25 – 30 tahun	38	32%
	31 – 35 tahun	38	32%
	36 – 40 tahun	5	4%
	41 – 45 tahun	22	18%
	46 – 50 tahun	9	8%
	Di atas 50 tahun	5	4%
	Jumlah	119	100%
Gender	Pria	66	55%
	Wanita	53	45%
	Jumlah	119	100%
Kisaran Gaji	Di bawah Rp2.000.000	5	4%
	Rp2.000.000 – Rp3.999.999	93	78%
	Rp4.000.000 – Rp5.999.999	19	16%
	Rp6.000.000 – Rp7.999.999	2	2%
	Rp8.000.000 – Rp9.999.999	0	0%
	Rp10.000.000 ke atas	0	0%
	Jumlah	119	100%
Bank yang Digunakan	Bank Central Asia - BCA	12	9%
	Bank Rakyat Indonesia - BRI	4	3%
	Bank Mandiri	8	6%
	Bank Negara Indonesia - BNI	12	9%
	Bank Syariah Indonesia - BSI	0	0%
	Bank Pembangunan Daerah Bali - BPD Bali	93	72%
	Lainnya	0	0%
	Jumlah	129	100%

Berdasarkan Tabel 1, dapat dilihat bahwa profil responden didominasi oleh pegawai pada rentang usia produktif, yaitu 25-35 tahun (Mencapai 64%), dengan mayoritas (78%) memiliki kisaran gaji antara Rp 2 juta hingga Rp 4 juta per bulan. Terkait penggunaan layanan *M-Banking*, Bank Pembangunan Daerah Bali (BPD Bali) menjadi pilihan utama bagi sebagian besar pegawai, yaitu sebanyak 72%.

3.1.1 Tingkat Kesadaran Keamanan Informasi Secara Keseluruhan

Analisis data yang dilakukan untuk mendapatkan gambaran umum tingkat kesadaran keamanan informasi pegawai. Menggunakan *Multiple Weighted Score Analysis* (*MWSA*), skor gabungan dari ketiga dimensi (Pengetahuan, Sikap, dan Perilaku) dihitung untuk menentukan skor kesadaran keseluruhan. Hasil analisis menunjukkan skor rata-rata tertimbang keseluruhan sebesar 3,69 dari skala maksimal 5. Berdasarkan interval kategori yang telah ditetapkan sebelumnya (1,00 – 2,33 = Buruk; 2,34 – 3,67 = Sedang; 3,68 – 5,00 = Baik), skor ini menempatkan tingkat kesadaran keamanan informasi pegawai secara umum pada kategori “Baik”. Meskipun hasil ini tampak positif, perlu dicatat bahwa skor 3,69 hanya sedikit melampaui ambang batas bawah kategori "Baik" (3,68). Hal ini mengisyaratkan bahwa meskipun sudah tergolong baik, tingkat kesadaran ini belum sepenuhnya solid dan masih memiliki ruang yang signifikan untuk perbaikan.

3.1.2 Tingkat Kesadaran Berdasarkan Dimensi

Ketika skor agregat diuraikan ke dalam tiga dimensi utamanya, muncul sebuah pola yang sangat signifikan dan menjadi inti dari temuan penelitian ini. Terdapat perbedaan yang mencolok antara tingkat Pengetahuan dan Sikap dengan tingkat Perilaku. Rangkuman hasil per dimensi disajikan pada Tabel 2.

Tabel 2. Kategori Dimensi Pengetahuan, Sikap dan Perilaku menggunakan HAIS-Q

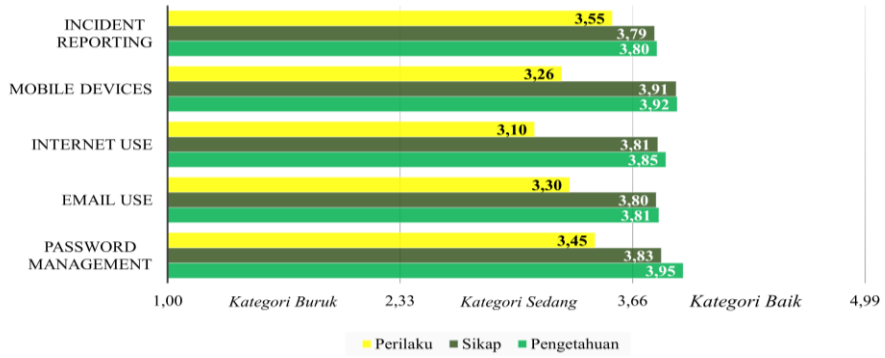
Dimensi	Mean	Kategori
Pengetahuan	3,86	Baik
Sikap	3,82	Baik

Dimensi	Mean	Kategori
Perilaku	3,33	Sedang

Pada dimensi Pengetahuan meraih skor tertinggi (3,86), diikuti sangat dekat oleh dimensi Sikap (3,82), di mana keduanya masuk dalam kategori "Baik". Namun, terjadi penurunan drastis pada dimensi Perilaku, yang hanya mencatatkan skor rata-rata 3,33 dan jatuh ke dalam kategori "Sedang". Temuan ini secara jelas memvisualisasikan adanya kesenjangan antara apa yang dipahami dan diyakini oleh pegawai dengan apa yang secara konsisten mereka praktikkan. Dimensi Perilaku teridentifikasi sebagai area kerentanan utama dalam kesadaran keamanan informasi di lingkungan Dinas Perdagangan, Perindustrian, dan Koperasi Usaha Kecil dan Menengah Kabupaten Buleleng.

3.1.3 Identifikasi Indikator Pada Setiap Dimensi

Untuk mengukur setiap dimensi utama (Pengetahuan, Sikap, dan Perilaku) pada penelitian ini, dapat dilakukan pengidentifikasian lima indikator kunci yang diadopsi dari kerangka *Human Aspects of Information Security Questionnaire* (*HAIS-Q*) yaitu indikator Pengelolaan Kata Sandi (Password Management), Penggunaan Email (*Email Use*), Penggunaan Internet (*Internet Use*), Perangkat Bergerak (*Mobile Devices*) dan Pelaporan Insiden (*Incident Reporting*). Indikator-indikator ini diterapkan secara konsisten pada ketiga dimensi untuk memastikan bahwa setiap aspek (*Kognitif, afektif, dan konatif*) dapat diukur secara komprehensif dan seimbang. Secara visual, struktur dan hasil data dari dimensi serta indikator yang digunakan dalam penelitian ini dapat dilihat pada Gambar 3 berikut.



Gambar 3. Diagram Histogram Skor Indikator Pada Setiap Dimensi

Berdasarkan perbandingan antar indikator pada masing-masing dimensi sebagaimana divisualisasikan pada Gambar 3, terlihat adanya variasi capaian skor yang menunjukkan pola kesenjangan yang konsisten. Indikator Password Management menunjukkan capaian yang baik pada dimensi Pengetahuan (3,95) dan Sikap (3,83), namun menurun pada dimensi Perilaku (3,45), yang mengindikasikan bahwa pemahaman dan sikap positif belum sepenuhnya diwujudkan dalam praktik. Kesenjangan yang lebih jelas terlihat pada indikator Internet Use dan Email Use, di mana skor Pengetahuan dan Sikap berada pada kategori “Baik” (masing-masing di atas 3,80), tetapi skor Perilaku menurun signifikan, khususnya pada Internet Use yang hanya mencapai 3,10. Sementara itu, indikator Mobile Devices menunjukkan capaian yang relatif lebih seimbang pada dimensi Pengetahuan (3,92) dan Sikap (3,91), meskipun Perilaku masih berada pada kategori “Sedang” (3,26). Pada indikator Incident Reporting, skor Pengetahuan (3,80) dan Sikap (3,79) tergolong “Baik”, namun skor Perilaku sebesar 3,55 menunjukkan bahwa praktik pelaporan insiden keamanan belum optimal. Secara keseluruhan, perbandingan ini menegaskan bahwa kesenjangan paling besar terdapat pada dimensi Perilaku, khususnya pada indikator Internet Use, Email Use, Mobile Devices, Password Management, dan *Incident Reporting*.

3.2 Pembahasan

3.2.1 Tinjauan Hasil pada Setiap Dimensi Utama

Hasil penelitian menunjukkan bahwa pegawai memiliki fondasi kesadaran keamanan informasi yang kuat pada imensi Pengetahuan dan Sikap. Dimensi Pengetahuan meraih skor tinggi sebesar 3,86 (Kategori “Baik”), yang mengindikasikan bahwa pegawai telah memahami konsep-konsep esensial keamanan informasi, seperti ancaman phishing dan pentingnya kata sandi yang kuat. Temuan ini sejalan dengan penelitian yang dilakukan oleh [4] dan [17] yang juga mengidentifikasi tingkat pengetahuan yang tinggi di kalangan pengguna layanan digital. Selanjutnya, pemahaman yang kuat ini terbukti berkorelasi positif dengan pembentukan sikap. Dimensi Sikap juga mencapai skor 3,82 (kategori “Baik”), menunjukkan bahwa pegawai juga peduli dan setuju akan pentingnya praktik keamanan. Sikap positif ini menjadi modal penting yang secara internal memotivasi pegawai untuk bertindak aman, sebuah temuan yang juga didukung oleh studi [17].

Namun, hal yang signifikan ditemukan pada dimensi Perilaku, yang hanya mencatatkan skor rata-rata 3,33 (kategori “Sedang”). Skor yang lebih rendah ini mengungkap adanya ketidakselarasan antara apa yang diketahui dan diyakini dengan apa yang dipraktikkan secara konsisten. Dengan kata lain, dimensi perilaku menjadi area kelemahan utama yang memerlukan perhatian lebih lanjut, Temuan ini sejalan dengan hasil penelitian [18] yang menunjukkan bahwa meskipun tingkat kesadaran keamanan informasi pengguna perangkat Android berada pada kategori baik, dimensi perilaku tetap menjadi aspek paling lemah dalam praktik keamanan sehari-hari.”

3.2.2 Identifikassi Kekuatan dan Kelemahan pada Setiap Indikator

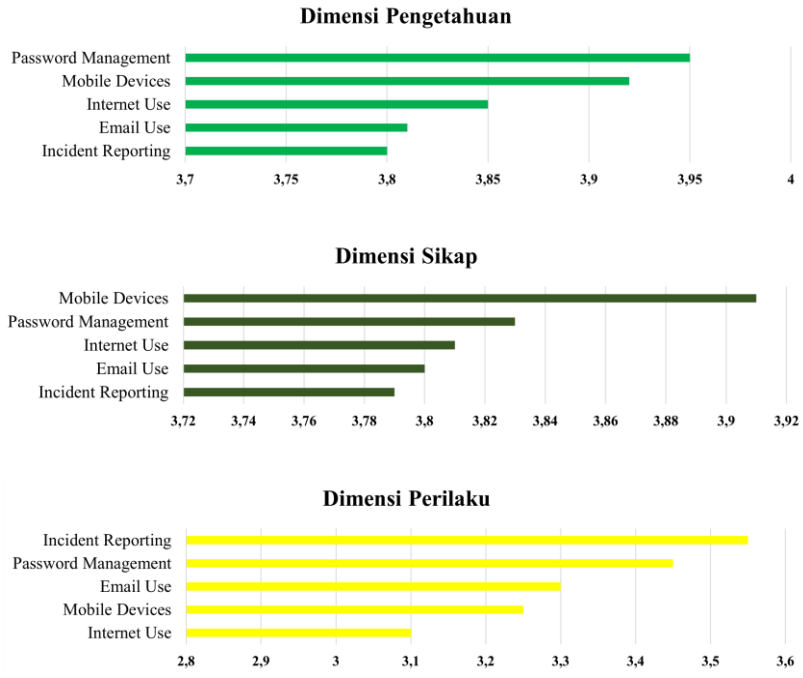
Analisis mendalam pada indikator menunjukkan pola yang konsisten dalam kekuatan pada domain pengetahuan dan sikap yang tidak diimbangi oleh praktik perilaku pegawai. Pada indikator Pengelolaan Kata Sandi, pegawai memiliki pengetahuan (skor 3,95) dan sikap (skor 3,83) yang "Baik", namun perilaku mengganti kata sandi secara berkala masih tergolong "Sedang" (skor 3,45), sejalan dengan temuan [19]. Pola serupa juga terlihat pada Penggunaan Email dan Penggunaan Internet, di mana pengetahuan dan sikap pegawai sudah baik, namun terdapat kelemahan signifikan pada dimensi perilaku. Indikator Penggunaan Internet bahkan menjadi area paling kritis dengan skor perilaku terendah (3,10). Untuk indikator Perangkat Seluler, pengetahuan pegawai memiliki skor 3,92 dan sikap (skor 3,91) pegawai sangat tinggi. Meskipun demikian, skor perilaku yang hanya mencapai 3,26 ("Sedang") menunjukkan bahwa praktik keamanan seperti pembaruan sistem belum menjadi prioritas, sejalan dengan analisis oleh [7]. Sementara itu, indikator Pelaporan Insiden menunjukkan temuan yang relatif lebih baik pada domain perilaku. Meskipun masih dalam kategori "Sedang" (skor 3,55), skor ini merupakan yang tertinggi di antara indikator perilaku lainnya. Hal ini menunjukkan adanya kecenderungan yang sedikit lebih positif dalam melaporkan insiden, meskipun pada umumnya pelaporan insiden sering kali menjadi aspek terlemah, seperti dalam studi [20].

3.2.3 Gambaran Mengenai Kesenjangan antara Pengetahuan dan Sikap dengan Perilaku Pegawai

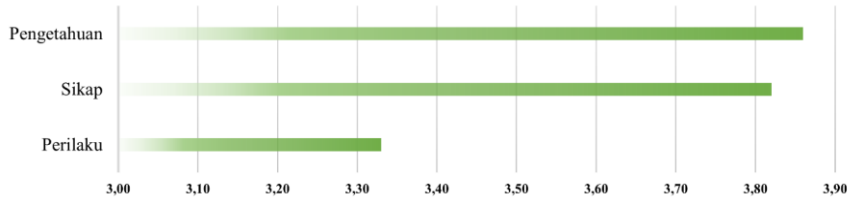
Temuan paling krusial dari penelitian ini adalah adanya kesenjangan yang signifikan antara apa yang diketahui dan diyakini dengan praktik nyata pegawai, yang dikenal sebagai *Knowledge-Attitude-Behavior Gap*. Hal ini menunjukkan bahwa pengetahuan dan sikap yang tinggi tidak secara otomatis menjamin terwujudnya perilaku yang konsisten. Secara kuantitatif, kesenjangan ini terbukti dari skor dimensi Pengetahuan (3,86) dan Sikap (3,82) yang keduanya terkategori “Baik”, namun tidak terealisasi pada dimensi Perilaku yang hanya mencapai skor 3,33 (“Sedang”). Selisih yang signifikan ini mengindikasikan bahwa proses transfer dari pemahaman dan keyakinan ke tindakan nyata tidak berjalan secara optimal. Kesenjangan ini semakin jelas pada bagian indikator. Dimana, pada indikator Penggunaan Internet, pegawai memiliki pengetahuan (skor 3,85) dan sikap (skor 3,81) yang sangat baik. Namun, dalam praktiknya, perilaku aman saat menggunakan internet justru menjadi yang terendah (skor 3,10). Pola serupa juga ditemukan pada indikator Penggunaan Email dan Perangkat Seluler, di mana pemahaman dan sikap positif tidak sepenuhnya diimplementasikan dalam perilaku sehari-hari.

3.2.4 Gambaran Keseluruhan Tingkat Kesadaran Keamanan Informasi

Secara keseluruhan, tingkat kesadaran keamanan informasi pegawai berada pada kategori “Baik”, dengan skor gabungan tertimbang sebesar 3,69 dari skala 5. Meskipun hasil ini positif, skor tersebut hanya sedikit melampaui ambang batas minimal (3,68), yang menunjukkan bahwa tingkat kesadaran ini belum sepenuhnya optimal. Skor keseluruhan yang “Baik” ini secara signifikan dipengaruhi oleh tingginya capaian pada dimensi Pengetahuan (3,86) dan Sikap (3,85). Kedua dimensi ini secara efektif mengangkat skor rata-rata dari dimensi Perilaku yang lebih rendah (3,35). Jadi, dapat disimpulkan bahwa skor keseluruhan yang baik dapat menyembunyikan kelemahan pada dimensi Perilaku. Berikut adalah rincian mengenai pemeringkatan skor pada setiap dimensi beserta indikatornya dimulai dari nilai yang terkuat hingga nilai yang terlemah dan dapat dilihat pada Tabel 4.



Gambar 4. Diagram Clustered Bar Skor Pemeringkatan Indikator Setiap Dimensi



Gambar 5. Diagram Clustered Bar Skor Pemeringkatan Dimensi

Visualisasi pada Gambar 5 menegaskan inti temuan penelitian ini, yaitu adanya perbedaan yang signifikan antar dimensi kesadaran keamanan informasi. Dimensi Pengetahuan menempati peringkat tertinggi dengan skor 3,86, diikuti oleh dimensi Sikap dengan skor 3,82, yang keduanya berada pada kategori "Baik" dan menunjukkan fondasi kognitif serta afektif yang kuat pada pegawai. Namun, capaian tersebut tidak diimbangi oleh dimensi Perilaku yang hanya memperoleh skor 3,33 dan terkategori "Sedang". Selisih skor sebesar 0,53 poin antara dimensi Pengetahuan dan Perilaku menjadi bukti kuantitatif adanya fenomena Knowledge–Attitude–Behavior Gap, yang mengindikasikan bahwa kesadaran keamanan yang baik belum sepenuhnya terinternalisasi menjadi tindakan nyata yang konsisten

4. KESIMPULAN

Berdasarkan hasil analisis dan pembahasan, tingkat kesadaran keamanan informasi penggunaan layanan M-Banking pada pegawai Dinas Perdagangan, Perindustrian, dan Koperasi UKM Kabupaten Buleleng secara umum berada pada kategori "Baik", dengan skor keseluruhan sebesar 3,69 dari skala 1–5, yang terutama didorong oleh tingginya skor pada dimensi Pengetahuan (3,86) dan Sikap (3,82). Namun demikian, temuan ini juga mengungkap adanya ketidakseimbangan yang signifikan, karena dimensi Perilaku hanya memperoleh skor 3,33 dan terkategori "Sedang", yang menunjukkan bahwa pengetahuan dan sikap positif pegawai belum sepenuhnya terwujud menjadi tindakan keamanan yang konsisten. Analisis lebih lanjut mengidentifikasi dimensi Perilaku sebagai area kerentanan utama, khususnya pada indikator Penggunaan Internet (3,10), Perangkat Seluler (3,26), Penggunaan Email (3,30), Pengelolaan Kata Sandi (3,45), dan Pelaporan Insiden (3,55), sehingga kelima indikator tersebut perlu diprioritaskan dalam penyusunan rekomendasi perbaikan. Oleh karena itu, penelitian ini merekomendasikan penyusunan dan penerapan Standar Operasional Prosedur (SOP) yang berfokus pada panduan tindakan praktis dan didukung oleh sosialisasi serta pelatihan yang berorientasi pada perubahan perilaku, serta menyarankan agar penelitian selanjutnya memperluas cakupan objek dan menggunakan pendekatan kualitatif untuk menggali lebih dalam faktor-faktor yang memengaruhi kesenjangan antara pengetahuan dan perilaku keamanan informasi.

REFERENCES

[1] A. D. Harahap, D. Juardi, and A. S. Y. Irawan, "Rancang Bangun Sistem Bangun Sistem Pendeteksi link Phising Mengunakan Algoritma Random Forest Berbasis Web," *Jurnal Informatika dan Teknik Elektro Terapan*, vol. 12, no. 3, Aug. 2024, doi: 10.23960/jitet.v12i3.4858.

[2] A. W. Finaka, Y. Nurhanisah, and C. Devina, "Pengguna Internet di Indonesia Makin Tinggi." Accessed: Nov. 13, 2023. Available: https://indonesiabaik.id/infografis/pengguna-internet-di-indonesia-makin-tinggi

[3] Badan Siber dan Sandi Negara, "Laporan Tahunan Monitoring Keamanan Siber 2020," Jakarta, 2020. Accessed: May 19, 2024. Available: https://www.bssn.go.id/monitoring-keamanan-siber/

[4] T. Ramadhan and B. Purwandari, "Analisis Tingkat Kesadaran Keamanan Informasi: Studi Kasus Pengguna Aplikasi Perbankan Digital Di Indonesia Guna Mencegah Social Engineering," *Jurnal Syntax Idea*, vol. 5, no. 1, pp. 86–98, Jan. 2023, doi: 10.36418/syntax-idea.v3i6.1227.

[5] H. D. Kartika and R. F. Aji, "Pengukuran tingkat kesadaran keamanan informasi: Studi kasus PT MNC Sky Vision Tbk.," pp. 1–51, 2018, Accessed: Mar. 01, 2025. Available: https://lontar.ui.ac.id/detail?id=20479175

[6] P. K. J. S. Agri, "Evaluasi Tingkat Kesadaran Keamanan Informasi Mahasiswa Akuntansi Universitas Sanata Dharma," *Skripsi Fakultas Ekonomi, Universitas Sanata Dharma Yogyakarta*, pp. 95–98, 2019, Accessed: Mar. 01, 2025. Available: https://repository.usd.ac.id/35156/1/152114017

[7] M. Ramadhani and P. K. Sari, "Examining the Knowledge, Attitude, and Behavior of IT Division Staff on Information Security Issues: A Case Study in a Telecommunication Company," *IRJEMS International Research Journal of Economics and Management Studies*, vol. 3, no. 6, pp. 354–361, Jun. 2024, doi: 10.56472/25835238/IRJEMS-V3I6P139.

[8] D. Nurjanah and S. Destya, "Pengukuran Tingkat Kesadaran Keamanan Informasi Mahasiswa pada Pembelajaran Online," *Jurnal Sistem dan Teknologi Informasi (JustIN)*, vol. 10, no. 1, p. 81, Jan. 2022, doi: 10.26418/justin.v10i1.44362.

[9] A. Z. F. Maulidi, "Analisis Kesadaran Keamanan SIber Pada Siswa SMP Di Nganjuk," Yogyakarta, Aug. 2024. Accessed: Oct. 31, 2024. Available: https://dspace.uii.ac.id/handle/123456789/52140

[10] K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac, and T. Zwaans, "The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies," *Jurnal Computers & Security*, vol. 66, pp. 40–51, May 2017, doi: doi.org/10.1016/j.cose.2017.01.004.

[11] S. R. Mohd. Hashim, N. Abdullah, and A. Aziz, "Ranking Method Using Multiple Weighted Score Analysis," Kinabalu, Sep. 2017. Available: https://www.researchgate.net/publication/265733128

[12] Dafid and Dorie, "Metode MCDA Untuk Pengukuran Tingkat Kesadaran Keamanan Informasi Pada Mahasiswa," *Jurnal Teknik Informatika dan Sistem Informasi*, vol. 7, no. 1, pp. 11–0, Apr. 2020, doi: https://doi.org/10.35957/jatisi.v7i1.296.

[13] A. Joshi, S. Kale, and S. Chandel, "Likert Scale: Explored and Explained," *Br J Appl Sci Technol*, vol. 7, no. 4, pp. 396–403, Feb. 2015, doi: 10.9734/BJAST/2015/14975.
[14] Abduloh and Gunawansyah, "Sistem Pendukung Keputusan Penerima Dana Bantuan Rumah Tidak Layak Huni Menggunakan Metode Multi Attribute Utility Theory (MAUT)," *G-Tech: Jurnal Teknologi Terapan*, vol. 6, no. 2, pp. 211–220, Sep. 2022, doi: 10.33379/gtech.v6i2.1679.
[15] M. Faruq Arifin and D. Arifianto, "Penerapan Metode Multi Attribute Utility Theory (Maut) Untuk Pemilihan Sekolah Menengah Atas Di Kecamatan Balung Berbasih Web," Jember, 2021. Available: http://repository.unmuhjember.ac.id/id/eprint/9513
[16] C. Tofallis, "Objective weights for scoring: the automatic democratic method," *Multiple Criteria Decision Making*, vol. 17, pp. 69–84, Dec. 2022, doi: 10.22367/mcdm.2022.17.04.
[17] I. R. Maulana and Candiwan, "Pengukuran Tingkat Kesadaran Keamanan Pegawai Divisi Ict Perusahaan Minyak X Di Indonesia," Oct. 2023. Accessed: Dec. 13, 2024. Available: https://openlibrarypublications.telkomuniversity.ac.id/index.php/management/article/view/21059
[18] M. Ula, R. T. Adek, and Bustami, "Mengukur Tingkat Kesadaran Keamanan Informasi Pengguna Handphone Android Mahasiswa Universitas Malikussaleh Dengan Metode Analytical Hierarchy Process (AHP)," Aceh, 2022. Accessed: Jan. 03, 2026. Available: https://snft2022.ft.unimal.ac.id/TI/016-TI.pdf
[19] M. Anastasiah and H. Pandia, "Analisis Perilaku Pengguna Mobile Banking Terhadap Keamanan Informasi Menggunakan Metode Human Aspects of Information Security Questionnaire (HAIS-Q)," *Journal Of Social Science Research*, vol. 4, no. 2, pp. 1–12, Apr. 2024, doi: https://doi.org/10.31004/innovative.v4i2.9684.
[20] S. Sembiring and H. Pandia, "Analisa Perilaku Keamanan Informasi Pengguna Mobile Banking," *TeIKa Jurnal Teknologi Informasi dan Komunikasi*, vol. 14, no. 1, pp. 52–63, Apr. 2024, doi: 10.36342/teika.v14i1.3382.