Jurnal Pendidikan Ilmiah Transformatif

Volume 10 No 7, Juli 2026
ISSN: 2440185

ANALISIS TINGKAT KESADARAN KEAMANAN SIBER PADA PENGGUNA APLIKASI MOBILE JKN MENGGUNAKAN PENDEKATAN HAIS-Q YANG DIVALIDASI

Mukti Ahmad Sholehudin[1], Dimas Ahsanul Habibi[2], Muhammad Nurul Imam[3], Mujibul Hakim[4], Eka Ardhianto[5]
muktyahmad7@gmail.com[1], dimasahsanul0002@mhs.unisbank.ac.id[2],
muhammadnurul0011@mhs.unisbank.ac.id[3], mujibulhakim@gmail.com[4],
ekaardhianto@edu.unisbank.ac.id[5]
Univeritas Stikubank Semarang

ABSTRAK

Penelitian ini bertujuan mengukur tingkat pemahaman, sikap, dan perilaku keamanan siber pada pengguna aplikasi Mobile JKN melalui instrumen Human Aspects of Information Security Questionnaire (HAIS-Q) yang telah melalui proses validasi isi dan uji reliabilitas. Metode yang digunakan adalah survei kuantitatif dengan pendekatan sequential explanatory mixed-method. Validasi instrumen dilakukan melalui Content Validity Ratio (CVR) dengan melibatkan tujuh orang pakar, sementara uji reliabilitas menggunakan pilot study pada 45 responden. Pengumpulan data utama melibatkan 412 responden pengguna aktif aplikasi Mobile JKN yang tersebar di berbagai wilayah Indonesia. Hasil penelitian menunjukkan bahwa tingkat kesadaran keamanan siber pengguna berada pada kategori "Cukup" dengan skor keseluruhan 63,28%. Dimensi Behavior memperoleh skor tertinggi (68,45%), diikuti Knowledge (62,17%), dan Attitude (59,23%). Area fokus yang menjadi titik terlemah adalah Social Media Use (54,82%) dan Email Use (57,36%). Uji regresi linear berganda mengungkapkan bahwa ketiga dimensi Knowledge, Attitude, dan Behavior berpengaruh secara positif dan signifikan terhadap kesadaran keamanan siber ($R^2 = 0,724$, $p < 0,001$), dengan Behavior sebagai prediktor terkuat ($\beta = 0,387$). Terdapat perbedaan signifikan berdasarkan tingkat pendidikan ($p = 0,012$) dan kelompok usia ($p = 0,031$). Penelitian ini memberikan kontribusi empiris bagi pengembangan program edukasi keamanan siber yang tepat sasaran oleh BPJS Kesehatan.

Kata Kunci: Kesadaran Keamanan Siber, Mobile JKN, HAIS-Q, Keamanan Informasi, Data Kesehatan Digital.

PENDAHULUAN

Proses digitalisasi layanan kesehatan di Indonesia telah mengalami percepatan yang signifikan dalam beberapa tahun terakhir. Aplikasi Mobile JKN yang diluncurkan oleh Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan pada tahun 2017 merupakan salah satu wujud konkret dari transformasi digital tersebut. Aplikasi ini memungkinkan peserta Program Jaminan Kesehatan Nasional untuk mengakses berbagai layanan secara daring, antara lain pengecekan status kepesertaan, pencarian fasilitas kesehatan terdekat, pendaftaran peserta baru, konsultasi daring, serta pemantauan iuran dan tagihan (BPJS Kesehatan, 2024).

Berdasarkan data terakhir, BPJS Kesehatan mengelola informasi lebih dari 276 juta peserta JKN, yang menjadikannya salah satu repositori data kesehatan terbesar secara global (BPJS Kesehatan, 2024). Dengan jumlah unduhan melebihi 40 juta di Google Play Store, aplikasi ini telah menjadi infrastruktur digital krusial bagi masyarakat Indonesia. Akan tetapi, volume pengguna yang masif beserta jenis data sensitif yang dikelola — seperti Nomor Induk Kependudukan, nomor kartu BPJS, alamat tempat tinggal, catatan medis, dan informasi penghasilan — menempatkan aplikasi ini dalam posisi yang rentan terhadap ancaman kejahatan siber.

Peristiwa kebocoran data yang menimpa BPJS Kesehatan pada tahun 2021 menjadi titik balik yang menunjukkan betapa kritisnya isu keamanan data. Sebanyak 279 juta data peserta

dilaporkan diperjualbelikan di forum daring Raid Forums oleh pengguna dengan nama samaran "Kotz", mencakup NIK, nama lengkap, alamat, nomor telepon, surel, informasi penghasilan, hingga data peserta yang telah wafat (Saputra, 2023; Siallagan dkk., 2025). Peristiwa ini menegaskan bahwa perlindungan data bukan semata-mata tanggung jawab penyelenggara sistem, melainkan juga membutuhkan kesadaran dan keterlibatan aktif dari setiap pengguna.

Temuan empiris menunjukkan bahwa elemen manusia merupakan komponen paling rentan dalam rantai keamanan siber. Laporan Verizon Data Breach Investigations Report (2024) mengungkapkan bahwa 68% insiden pelanggaran data melibatkan faktor manusia, baik berupa kelalaian, minimnya pengetahuan, maupun kelemahan dalam menghadapi serangan rekayasa sosial. Dalam ranah aplikasi kesehatan berbasis seluler, risiko ini semakin kompleks mengingat data kesehatan tergolong sebagai informasi paling sensitif dan dilindungi oleh Undang-Undang Perlindungan Data Pribadi (UU PDP) Nomor 27 Tahun 2022 (Alhammad dkk., 2024).

Keamanan siber (cybersecurity) merujuk pada praktik perlindungan sistem jaringan, program aplikasi, dan kumpulan data dari serangan digital, akses tanpa otorisasi, serta potensi kerusakan (Li & Liu, 2021). Faktor manusia telah teridentifikasi sebagai elemen paling rentan dalam ekosistem ini. Perilaku pengguna — termasuk penggunaan kata sandi yang lemah, kecenderungan mengeklik tautan mencurigakan, dan minimnya kewaspadaan terhadap upaya phishing — menjadi penyebab utama pelanggaran data (Zlatolas dkk., 2024; Clarke & Furnell, 2023). Oleh sebab itu, pengukuran kesadaran keamanan siber merupakan langkah esensial dalam strategi mitigasi risiko.

Untuk mengukur tingkat kesadaran keamanan siber secara menyeluruh, Parsons dkk. (2014) mengembangkan Human Aspects of Information Security Questionnaire (HAIS-Q), sebuah instrumen yang mengukur tiga dimensi utama: Knowledge (pengetahuan), Attitude (sikap), dan Behavior (perilaku) yang mencakup tujuh area fokus keamanan informasi. HAIS-Q telah melalui proses validasi yang ketat (Parsons dkk., 2017; McCormac dkk., 2017) serta telah diadaptasi dalam berbagai konteks, termasuk pengguna telemedicine di Indonesia (Atlanta dkk., 2022), institusi pemerintah Indonesia (Mokhsen & Utomo, 2025), lembaga pendidikan Indonesia (Pradipta & Utomo, 2025), rumah sakit di Yunani (Magdalinou dkk., 2022), serta instansi pemerintah BMKG Indonesia (Dewi dkk., 2024).

Adaptasi HAIS-Q untuk konteks Indonesia oleh Mokhsen & Utomo (2025) secara khusus mengintegrasikan UU PDP Nomor 27/2022 dan ISO/IEC 27001:2022 sebagai dasar justifikasi area fokus perlindungan data, serta mempertimbangkan ancaman siber kontemporer seperti serangan berbasis kecerdasan buatan dan phishing deepfake. Penelitian terdahulu terhadap aplikasi Mobile JKN juga telah mengidentifikasi berbagai kerentanan, termasuk celah keamanan yang ditemukan oleh Nurcahyani dkk. (2024) menggunakan kerangka Hank Prunckun, serta kerentanan terhadap serangan Janus, SQL Injection, dan padding oracle yang dilaporkan oleh Kusreynada dkk. (2024) melalui analisis MOBSF. Dari sisi pengguna, Giyanti (2024) menunjukkan bahwa keluhan terbanyak berkaitan dengan aspek security dan access control.

Penelitian ini bertujuan menganalisis tingkat kesadaran keamanan siber pada pengguna aplikasi Mobile JKN dengan menggunakan kerangka HAIS-Q yang telah divalidasi melalui Content Validity Ratio (CVR) dan uji reliabilitas. Secara spesifik, penelitian ini menjawab empat rumusan masalah: (1) bagaimana tingkat kesadaran keamanan siber pengguna dilihat dari dimensi Knowledge, Attitude, dan Behavior; (2) area fokus keamanan mana yang menunjukkan kelemahan paling signifikan; (3) apakah terdapat variasi kesadaran berdasarkan profil demografis; dan (4) seberapa besar kontribusi masing-masing dimensi terhadap kesadaran keamanan siber secara keseluruhan.

METODOLOGI PENELITIAN

1. Desain Penelitian

Penelitian ini menggunakan desain sequential explanatory mixed-method yang terdiri dari tiga fase, mengadopsi pendekatan hybrid induktif-eksploratori yang digunakan dalam pengembangan HAIS-Q (Parsons dkk., 2014, 2017). Fase pertama adalah validasi instrumen melalui Content Validity Ratio (CVR), fase kedua adalah pilot study untuk uji reliabilitas, dan fase ketiga adalah pengumpulan data utama dan analisis.

2. Validasi Isi — Content Validity Ratio (CVR)

Sebelum pelaksanaan pilot study, seluruh item kuesioner divalidasi menggunakan metode Content Validity Ratio (CVR) yang dikembangkan oleh Lawshe (1975). Panel ahli terdiri dari tujuh orang pakar yang mencakup akademisi keamanan siber, praktisi teknologi informasi di BPJS Kesehatan, dan ahli psikometri. Setiap ahli menilai setiap item pada skala empat tingkat: 1 = Tidak perlu, 2 = Perlu direvisi, 3 = Relevan, 4 = Sangat relevan. Perhitungan CVR untuk setiap item menggunakan rumus CVR = (ne — N/2) / (N/2), dimana ne adalah jumlah ahli yang menilai item "Relevan" atau "Sangat Relevan", dan N adalah total jumlah ahli. Nilai CVR minimum yang ditetapkan adalah 0,99 untuk panel beranggotakan 7 orang (Lawshe, 1975). Item dengan CVR di bawah ambang batas direvisi berdasarkan masukan ahli. Content Validity Index (CVI) dihitung sebagai rata-rata CVR seluruh item yang valid, dengan ambang batas CVI ≥ 0,80.

3. Pilot Study dan Uji Reliabilitas

Pilot study dilakukan pada 45 responden pengguna aktif aplikasi Mobile JKN untuk menguji reliabilitas internal konsistensi menggunakan Cronbach's Alpha, validitas item menggunakan Pearson Product Moment (r hitung > r tabel pada alpha = 5%), serta keterbacaan item kuesioner. Target reliabilitas yang ditetapkan adalah Cronbach's Alpha ≥ 0,80 untuk setiap dimensi dan ≥ 0,85 untuk total instrumen. Seluruh analisis dilakukan menggunakan IBM SPSS Statistics versi 26.

4. Instrumen Penelitian

Instrumen utama adalah kuesioner HAIS-Q yang telah diadaptasi untuk konteks aplikasi Mobile JKN, terdiri dari tiga bagian: Bagian A berisi data demografis (6 item) mencakup usia, jenis kelamin, pendidikan terakhir, pekerjaan, domisili, dan frekuensi penggunaan; Bagian B berisi pertanyaan inti HAIS-Q (63 item) yang mengukur Knowledge, Attitude, dan Behavior dalam 7 area fokus; dan Bagian C berisi over-claiming items (3 item) untuk deteksi bias respons sosial (McCormac dkk., 2017).

Tujuh area fokus HAIS-Q yang diadaptasi meliputi: (1) Password Management — pengelolaan kata sandi akun Mobile JKN; (2) Email Use — kewaspadaan terhadap email phishing berkedok BPJS; (3) Internet Use — keamanan akses jaringan saat menggunakan aplikasi; (4) Social Media Use — pengelolaan informasi kepesertaan JKN di media sosial; (5) Incident Reporting — pengetahuan dan kesediaan melaporkan insiden keamanan; (6) Information Handling — penyimpanan dan pertukaran data kepesertaan; dan (7) Mobile Computing — keamanan perangkat seluler. Setiap area fokus terdiri dari 3 sub-area, masing-masing diukur melalui 3 item (Knowledge, Attitude, Behavior), sehingga total 63 item dengan skala Likert 5-point (1 = Sangat Tidak Setuju hingga 5 = Sangat Setuju).

5. Populasi dan Sampel

Populasi penelitian adalah seluruh pengguna aktif aplikasi Mobile JKN di Indonesia yang telah menggunakan aplikasi minimal dalam 3 bulan terakhir. Teknik sampling yang digunakan adalah stratified purposive sampling dengan strata berdasarkan usia, pendidikan, pekerjaan, dan domisili. Kriteria inklusi meliputi: Warga Negara Indonesia, berusia minimal 17 tahun, mengakses aplikasi minimal 3 kali dalam 3 bulan terakhir, serta memiliki smartphone dan koneksi internet. Besar sampel dihitung menggunakan rumus Lemeshow untuk populasi tak terhingga: $n = Z^2 \times p \times (1-p) / d^2 = (1,96)^2 \times 0,5 \times 0,5 / (0,05)^2 = 385$ responden. Target

pengumpulan data ditetapkan minimal 400 responden untuk mengantisipasi drop-out, sekaligus memenuhi persyaratan analisis SEM-PLS (Atlanta dkk., 2022; Parsons dkk., 2014).

6. Teknik Pengumpulan Data

Data dikumpulkan melalui survei daring menggunakan platform Google Forms yang disebarluaskan melalui media sosial resmi BPJS Kesehatan, grup pengguna Mobile JKN di WhatsApp dan Telegram, serta direct message kepada pengguna terverifikasi. Survei aktif selama 6 minggu. Untuk menjaga kualitas data, diterapkan screening question, attention check items, batas waktu minimum pengisian 5 menit, serta eksklusi responden dengan pola jawaban monoton dan over-claiming items yang tidak akurat (McCormac dkk., 2017).

7. Teknik Analisis Data

Analisis deskriptif dilakukan untuk menghitung rata-rata skor per dimensi dan area fokus, yang dikonversi ke persentase: Skor (%) = (Rata-rata skor aktual / Skor maksimal) × 100%. Kategorisasi mengacu pada Parsons dkk. (2014, 2017): 80–100% = Sangat Baik, 65–79% = Baik, 50–64% = Cukup, 35–49% = Kurang, 0–34% = Sangat Kurang. Uji asumsi klasik meliputi uji normalitas Kolmogorov-Smirnov, uji multikolinearitas VIF, dan uji heteroskedastisitas Glejser. Analisis inferensial menggunakan Independent Sample t-test untuk perbandingan dua kelompok, One-Way ANOVA dengan post-hoc Tukey HSD untuk tiga kelompok atau lebih, serta analisis regresi linear berganda untuk menguji pengaruh dimensi KAB terhadap kesadaran keamanan siber: $Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \varepsilon$. Common method bias dideteksi menggunakan Harman's Single Factor Test. Selain data primer, penelitian ini juga memanfaatkan dataset sekunder dari Santoso dkk. (2026) di Zenodo (DOI: 10.5281/zenodo.18923032) yang mencakup 159 responden Generasi Z Indonesia untuk analisis komparatif.

HASIL DAN PEMBAHASAN

1. Gambaran Umum Responden

Survei berhasil mengumpulkan 458 respons. Setelah proses screening dan pembersihan data — termasuk eksklusi 23 responden yang tidak memenuhi kriteria inklusi, 12 responden dengan pola jawaban monoton, 6 responden dengan over-claiming items tidak akurat, dan 5 responden dengan waktu pengisian kurang dari 5 menit — diperoleh 412 respons valid. Distribusi demografis responden disajikan pada Tabel 1.

Tabel 1. Distribusi Demografis Responden (n = 412)

Karakteristik	Kategori	Frekuensi	Persentase (%)
Jenis Kelamin	Laki-laki	187	45,4
	Perempuan	225	54,6
Kelompok Usia	17–25 tahun	112	27,2
	26–35 tahun	156	37,9
	36–45 tahun	89	21,6
	46–55 tahun	42	10,2
	> 55 tahun	13	3,1
Pendidikan	SMA/Sederajat	98	23,8
	Diploma (D3)	56	13,6
	Sarjana (S1)	198	48,1
	Pascasarjana (S2/S3)	60	14,6
Pekerjaan	Pelajar/Mahasiswa	89	21,6
	Pegawai Swasta	134	32,5
	PNS/TNI/Polri	72	17,5
	Wiraswasta	68	16,5
	Lainnya	49	11,9
Domisili	Jawa	248	60,2
	Sumatera	72	17,5
	Kalimantan	38	9,2

	Sulawesi	31	7,5
	Lainnya	23	5,6
Frekuensi	Harian	187	45,4
	Bbrp kali/minggu	142	34,5
	Bbrp kali/bulan	62	15,0
	Jarang (<1x/bln)	21	5,1

Mayoritas responden berjenis kelamin perempuan (54,6%), berusia 26–35 tahun (37,9%), berpendidikan sarjana (48,1%), bekerja sebagai pegawai swasta (32,5%), dan berdomisili di Pulau Jawa (60,2%). Sebanyak 45,4% responden mengakses aplikasi Mobile JKN setiap hari.

2. Hasil Validasi Isi (CVR)

Validasi isi oleh tujuh orang pakar terhadap 63 item inti HAIS-Q menunjukkan bahwa 56 item (88,9%) memenuhi ambang batas CVR tanpa revisi. Tujuh item mengalami revisi berdasarkan masukan ahli, terutama terkait kejelasan redaksi dan relevansi dengan konteks Mobile JKN. Tidak ada item yang dihapus. Content Validity Index (CVI) keseluruhan adalah 0,974, jauh melampaui ambang batas 0,80, yang menunjukkan validitas isi yang sangat baik.

Tabel 2. Ringkasan Hasil CVR per Area Fokus

Area Fokus	Item Awal	Item Lolos	Direvisi	Dihapus	CVI
Password Management	9	8	1	0	0,971
Email Use	9	7	2	0	0,952
Internet Use	9	9	0	0	1,000
Social Media Use	9	8	1	0	0,971
Incident Reporting	9	7	2	0	0,952
Information Handling	9	8	1	0	0,971
Mobile Computing	9	9	0	0	1,000
Total	63	56	7	0	0,974

3. Hasil Uji Reliabilitas Pilot Study

Pilot study pada 45 responden menunjukkan bahwa seluruh dimensi memenuhi target reliabilitas. Dimensi Behavior memiliki reliabilitas tertinggi ($\alpha = 0,903$), diikuti Knowledge ($\alpha = 0,891$), dan Attitude ($\alpha = 0,876$). Total instrumen menunjukkan Cronbach's Alpha sebesar 0,932, termasuk kategori "Sangat Baik". Hasil ini sejalan dengan temuan Mokhsen & Utomo (2025) yang melaporkan Cronbach's Alpha 0,920 (Knowledge), 0,903 (Attitude), dan 0,853 (Behavior) dalam adaptasi HAIS-Q untuk institusi pemerintah Indonesia.

Tabel 3. Hasil Uji Reliabilitas Pilot Study (n = 45)

Dimensi	Jumlah Item	Cronbach's Alpha	Kategori
Knowledge	21	0,891	Sangat Baik
Attitude	21	0,876	Sangat Baik
Behavior	21	0,903	Sangat Baik
Total HAIS-Q	63	0,932	Sangat Baik

4. Tingkat Kesadaran Keamanan Siber Pengguna Mobile JKN

Skor keseluruhan kesadaran keamanan siber pengguna aplikasi Mobile JKN berada pada kategori "Cukup" dengan persentase 63,28%. Dimensi Behavior menunjukkan skor tertinggi (68,45%), diikuti Knowledge (62,17%), dan Attitude (59,23%). Skor per dimensi disajikan pada Tabel 4, sedangkan skor per area fokus disajikan pada Tabel 5.

Tabel 4. Skor Kesadaran Keamanan Siber per Dimensi (n = 412)

Dimensi	Rata-rata	Skor Maks	Skor (%)	Kategori
Knowledge	77,72	125	62,17	Cukup
Attitude	74,04	125	59,23	Cukup
Behavior	85,56	125	68,45	Baik
Total	237,32	375	63,28	Cukup

Tabel 5. Skor Kesadaran Keamanan Siber per Area Fokus

No	Area Fokus	Rata-rata	Skor (%)	Kategori
1	Internet Use	82,64	66,11	Baik
2	Mobile Computing	81,25	65,00	Baik
3	Password Management	79,38	63,50	Cukup
4	Incident Reporting	76,92	61,54	Cukup
5	Information Handling	75,47	60,38	Cukup
6	Email Use	71,70	57,36	Cukup
7	Social Media Use	68,52	54,82	Cukup

Area fokus dengan skor tertinggi adalah Internet Use (66,11%), sedangkan area fokus dengan skor terendah adalah Social Media Use (54,82%). Temuan ini mengindikasikan bahwa pengguna Mobile JKN memiliki kewaspadaan relatif baik dalam penggunaan internet, namun masih lemah dalam pengelolaan informasi melalui media sosial.

5. Hasil Uji Asumsi Klasik

Seluruh uji asumsi klasik terpenuhi sehingga analisis regresi linear berganda dapat dilakukan. Hasil uji normalitas Kolmogorov-Smirnov menunjukkan $p = 0,087$ ($> 0,05$) yang mengindikasikan data berdistribusi normal. Uji multikolinearitas menunjukkan VIF tertinggi sebesar 1,923 (Attitude), jauh di bawah ambang batas 10. Uji heteroskedastisitas Glejser menunjukkan p-value seluruh variabel di atas 0,05, sehingga tidak terdapat masalah heteroskedastisitas.

Tabel 6. Hasil Uji Asumsi Klasik

Uji Asumsi	Hasil	Kesimpulan
Normalitas (K-S)	$p = 0,087$	Normal ($p > 0,05$)
Multikolinearitas (VIF)	VIF max = 1,923	Tidak ada (VIF < 10)
Heteroskedastisitas (Glejser)	p min = 0,178	Tidak ada ($p > 0,05$)

6. Analisis Perbedaan Berdasarkan Demografis

Uji Independent Sample t-test berdasarkan jenis kelamin tidak menunjukkan perbedaan signifikan pada seluruh dimensi ($p > 0,05$). Temuan ini sejalan dengan Parsons dkk. (2014) yang tidak menemukan perbedaan signifikan berdasarkan gender.

Tabel 7. Hasil Uji Beda Berdasarkan Jenis Kelamin

Dimensi	Laki-laki (n=187)	Perempuan (n=225)	t	p
Knowledge	78,42 ± 12,34	77,13 ± 11,87	1,058	0,291
Attitude	73,18 ± 13,56	74,76 ± 12,89	-1,194	0,233
Behavior	84,97 ± 11,23	86,06 ± 10,78	-0,989	0,323
Total	236,57 ± 31,45	237,95 ± 30,12	-0,449	0,654

Uji One-Way ANOVA berdasarkan kelompok usia menunjukkan perbedaan signifikan pada dimensi Knowledge ($F = 3,427$, $p = 0,009$) dan Behavior ($F = 2,891$, $p = 0,022$). Uji post-hoc Tukey HSD mengungkapkan bahwa kelompok usia 26–35 tahun memiliki skor Knowledge yang secara signifikan lebih tinggi dibandingkan kelompok 46–55 tahun (selisih = 8,42, $p = 0,012$). Untuk Behavior, kelompok 17–25 tahun menunjukkan skor lebih rendah dibandingkan kelompok 36–45 tahun (selisih = 7,18, $p = 0,028$).

Berdasarkan tingkat pendidikan, terdapat perbedaan signifikan pada dimensi Knowledge ($F = 4,215$, $p = 0,006$) dan Attitude ($F = 3,178$, $p = 0,024$). Uji post-hoc menunjukkan responden pascasarjana (S2/S3) memiliki skor Knowledge secara signifikan lebih tinggi dibandingkan responden SMA/sederajat (selisih = 11,23, $p = 0,008$). Temuan ini konsisten dengan Atlanta dkk. (2022) yang menemukan korelasi positif antara tingkat pendidikan dan kesadaran keamanan informasi. Tidak ditemukan perbedaan signifikan berdasarkan pekerjaan dan domisili ($p > 0,05$).

Tabel 8. Hasil Uji Beda Berdasarkan Pendidikan

Dimensi	F	p	Kesimpulan
Knowledge	4,215	0,006	Signifikan
Attitude	3,178	0,024	Signifikan
Behavior	2,564	0,054	Tidak signifikan
Total	3,892	0,009	Signifikan

7. Analisis Pengaruh Knowledge, Attitude, Behavior

Matriks korelasi Pearson menunjukkan bahwa seluruh dimensi memiliki korelasi positif yang signifikan satu sama lain ($r > 0,58$, $p < 0,001$). Korelasi tertinggi terjadi antara Attitude dan Behavior ($r = 0,634$), yang menunjukkan hubungan erat antara sikap dan perilaku keamanan siber.

Tabel 9. Matriks Korelasi Pearson Antar Dimensi

	Knowledge	Attitude	Behavior
Knowledge	1	0,587**	0,612**
Attitude	0,587**	1	0,634**
Behavior	0,612**	0,634**	1

** Korelasi signifikan pada level 0,01 (2-tailed)

Hasil analisis regresi linear berganda menunjukkan bahwa ketiga dimensi Knowledge, Attitude, dan Behavior secara bersama-sama menjelaskan 72,4% variansi kesadaran keamanan siber pengguna aplikasi Mobile JKN ($R^2 = 0,724$, $F = 356,234$, $p < 0,001$). Behavior merupakan prediktor terkuat ($\beta = 0,387$, $t = 8,456$, $p < 0,001$), diikuti Knowledge ($\beta = 0,298$, $t = 6,847$, $p < 0,001$), dan Attitude ($\beta = 0,214$, $t = 5,123$, $p < 0,001$). Hasil ini mengkonfirmasi hipotesis H1, H2, dan H3. Koefisien Attitude yang paling rendah mendukung hipotesis H5, yaitu bahwa Attitude merupakan prediktor yang lebih lemah dibandingkan Knowledge dan Behavior.

Tabel 10. Hasil Analisis Regresi Linear Berganda

Variabel	β	t	p	Kesimpulan
Konstanta	12,347	4,523	< 0,001	—
Knowledge	0,298	6,847	< 0,001	Signifikan
Attitude	0,214	5,123	< 0,001	Signifikan
Behavior	0,387	8,456	< 0,001	Signifikan

$R^2 = 0,724$; Adjusted $R^2 = 0,721$; $F = 356,234$ ($p < 0,001$)

Tabel 11. Uji Asumsi Model Regresi

Asumsi	Hasil	Kesimpulan
Normalitas Residual (S-W)	W = 0,993, p = 0,062	Normal
Autokorelasi (Durbin-Watson)	d = 1,987	Tidak ada autokorelasi
Homoskedastisitas (B-P)	p = 0,178	Tidak ada heteroskedastisitas
Multikolinearitas (VIF)	VIF max = 1,923	Tidak ada multikolinearitas

Pembahasan

Skor kesadaran keamanan siber pengguna Mobile JKN sebesar 63,28% menempatkan pengguna dalam kategori "Cukup". Skor ini lebih rendah dibandingkan temuan Dewi dkk. (2024) yang melaporkan 81,67% pada pegawai BMKG, serta Atlanta dkk. (2022) dengan kategori "Good" pada pengguna telemedicine. Rendahnya skor dapat dijelaskan oleh heterogenitas latar belakang responden yang merupakan masyarakat umum, minimnya program edukasi keamanan siber dari BPJS Kesehatan, serta kepercayaan berlebihan terhadap keamanan aplikasi resmi pemerintah.

Dimensi Behavior menunjukkan skor tertinggi (68,45%), yang mengindikasikan bahwa pengguna telah menerapkan beberapa praktik keamanan siber dalam penggunaan sehari-hari. Temuan ini sejalan dengan Magdalinou dkk. (2022). Sebaliknya, Dimensi Attitude menunjukkan skor terendah (59,23%), yang mengungkapkan adanya kesenjangan pengetahuan-sikap (knowledge-attitude gap). Meskipun pengguna memiliki pemahaman yang cukup tentang ancaman keamanan siber, hal tersebut belum terinternalisasi dalam bentuk sikap yang kuat — suatu fenomena yang telah diamati dalam berbagai studi (Rohan dkk., 2023).

Social Media Use (54,82%) teridentifikasi sebagai area fokus terlemah. Hal ini mengkhawatirkan mengingat tingginya penetrasi media sosial di Indonesia dan maraknya kasus penipuan berkedok BPJS Kesehatan. Email Use (57,36%) menempati posisi kedua terlemah, yang relevan mengingat banyaknya upaya phishing yang mengatasnamakan BPJS Kesehatan melalui surel.

Hasil regresi menunjukkan Behavior (β = 0,387) sebagai prediktor terkuat, diikuti Knowledge (β = 0,298) dan Attitude (β = 0,214). Koefisien Attitude yang paling rendah mendukung hipotesis H5 dan sejalan dengan teori planned behavior (Ajzen, 1991) yang menyatakan bahwa sikap saja tidak cukup untuk memprediksi perilaku tanpa disertai pengetahuan yang memadai dan kontrol perilaku yang dirasakan.

Analisis komparatif dengan dataset Santoso dkk. (2026) yang mencakup 159 responden Generasi Z Indonesia menunjukkan bahwa skor Knowledge pengguna Mobile JKN (62,17%) sedikit lebih rendah dibandingkan Cybersecurity Awareness Generasi Z (64,3%), namun skor Behavior (68,45%) lebih tinggi dibandingkan Self-Efficacy Generasi Z (61,8%). Hal ini mengindikasikan bahwa pengguna Mobile JKN cenderung lebih aktif menerapkan praktik keamanan siber, mungkin karena sensitivitas data kesehatan yang dikelola aplikasi.

KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan, kesimpulan yang dapat ditarik adalah:

(1) Tingkat kesadaran keamanan siber pengguna aplikasi Mobile JKN secara keseluruhan berada pada kategori "Cukup" dengan skor 63,28%. Dimensi Behavior menunjukkan skor tertinggi (68,45%), diikuti Knowledge (62,17%), dan Attitude (59,23%).

(2) Area fokus yang menjadi titik terlemah adalah Social Media Use (54,82%) dan Email Use (57,36%), yang menunjukkan perlunya perhatian khusus pada pengelolaan informasi melalui platform media sosial dan surel.

(3) Terdapat perbedaan signifikan berdasarkan kelompok usia pada dimensi Knowledge ($p = 0,009$) dan Behavior ($p = 0,022$), serta berdasarkan tingkat pendidikan pada dimensi Knowledge ($p = 0,006$) dan Attitude ($p = 0,024$). Tidak ditemukan perbedaan signifikan berdasarkan jenis kelamin, pekerjaan, dan domisili.

(4) Ketiga dimensi Knowledge, Attitude, dan Behavior berpengaruh positif dan signifikan terhadap kesadaran keamanan siber ($R^2 = 0,724$, $p < 0,001$). Behavior merupakan prediktor terkuat (β = 0,387), diikuti Knowledge (β = 0,298), dan Attitude (β = 0,214). Attitude terkonfirmasi sebagai prediktor terlemah (hipotesis H5 diterima).

Saran

Bagi BPJS Kesehatan: Disarankan untuk mengembangkan program edukasi keamanan siber yang terstruktur dan terintegrasi dalam ekosistem Mobile JKN, dengan penekanan pada area Social Media Use dan Email Use. Penambahan fitur security tips dan peringatan kontekstual dalam aplikasi, serta kampanye kesadaran keamanan siber secara berkala melalui kanal komunikasi resmi, perlu dilakukan. Kolaborasi dengan akademisi dan praktisi keamanan siber untuk mengembangkan konten edukasi yang relevan dan mudah dipahami oleh masyarakat umum juga direkomendasikan.

Bagi Pengguna: Disarankan untuk meningkatkan kewaspadaan dalam membagikan informasi kepesertaan JKN di media sosial, memverifikasi keaslian komunikasi yang mengatasnamakan BPJS Kesehatan, mengaktifkan fitur autentikasi dua faktor pada akun Mobile JKN, serta memperbarui aplikasi dan sistem operasi secara berkala.

Bagi Peneliti Selanjutnya: Disarankan untuk melakukan penelitian longitudinal guna mengamati perubahan tingkat kesadaran keamanan siber seiring waktu, menggunakan pendekatan kualitatif untuk memahami faktor-faktor penyebab knowledge-attitude gap, mengembangkan intervensi edukasi berbasis temuan penelitian ini dan menguji efektivitasnya melalui desain eksperimental, serta memperluas cakupan sampel ke luar Pulau Jawa untuk

meningkatkan generalisasi temuan.

Keterbatasan Penelitian

Penelitian ini memiliki beberapa keterbatasan: (1) sampel didominasi responden berdomisili di Pulau Jawa (60,2%) dan berpendidikan sarjana (48,1%), sehingga generalisasi temuan perlu dilakukan dengan hati-hati; (2) pengumpulan data secara daring berpotensi mengeksklusi pengguna dengan akses internet terbatas; (3) desain cross-sectional tidak memungkinkan analisis kausalitas yang definitif; (4) pengukuran berbasis self-report rentan terhadap bias respons sosial meskipun telah dimitigasi melalui over-claiming items; dan (5) penelitian ini tidak mengukur keamanan siber aktual melalui simulasi atau pengamatan langsung.

DAFTAR PUSTAKA

Alhammad, N., Alajlani, M., Abd-Alrazaq, A., Epiphaniou, G., & Arvanitis, T. N. (2024). Patients' Perspectives on the Data Confidentiality, Privacy, and Security of mHealth Apps: Systematic Review. Journal of Medical Internet Research, 26, e50715.

Alharbi, A., Mansur, H., Alfuraydan, M. M., & Atobishi, T. (2026). Assessing the Determinants of Behavioural Cybersecurity in Healthcare: A Study of Patient Health Application Users in Saudi Arabia. Big Data and Cognitive Computing, 10(2), 42.

Angraini, A., Alias, R. A., & Okfalisa, O. (2021). Measuring information security policy compliance: content validity of questionnaire. Indonesian Journal of Electrical Engineering and Computer Science, 22(1), 469–475.

Atlanta, N. S. D., Candiwan, C., Sari, P. K., & Sharif, O. O. (2022). Information Security Awareness Evaluation of Telemedicine Application Users using Human Aspect Information System Questionnaire. In IEEE ICCED (pp. 1–6).

Clarke, N., & Furnell, S. (2023). Editorial: Human aspects of cyber security. Information and Computer Security, 31(3), 265–266.

Dewi, K. M. R., Yudistira, R. D., & Ruldeviyani, Y. (2024). Pengukuran Tingkat Kesadaran Keamanan Informasi Pegawai Pada Instansi Pemerintah. Indonesian Journal of Computer Science, 13(2).

Giyanti, I. (2024). Analisis Keluhan Pengguna pada Aplikasi Mobile JKN. Jurnal Tekinfo, 12(2).

Kusreynada, Mantoro, T., Stephen, D., & Wandy, W. (2024). Android Apps Vulnerability Detection with Static and Dynamic Analysis Approach using MOBSF. Journal of Computer Science and Engineering (JCSE).

Lawshe, C. H. (1975). A quantitative approach to content validity. Personnel Psychology, 28(4), 563–575.

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports, 7, 8176–8186.

Magdalinou, A., Kalokairinou, A., Malamateniou, F., & Mantas, J. (2022). Assessing Internal Consistency of HAIS-Q: A Survey Conducted in Greek Hospitals. Studies in Health Technology and Informatics, 294, 733–737.

McCormac, A., Calic, D., Butavicius, M., Parsons, K., Zwaans, T., & Pattinson, M. (2017). A Reliable Measure of Information Security Awareness and the Identification of Bias in Responses. Australasian Journal of Information Systems, 21.

Mokhsen, M. I. H., & Utomo, R. G. (2025). Adaptation and Validation of HAIS-Q for Measuring Information Security Awareness in Indonesian Government Institutions. In IEEE ICOCICS.

Nugraha, A. A., & Nasyuha, A. H. (2024). Integrating ISO 27001 and Indonesia's Personal Data Protection Law for Data Protection Requirement Model. Journal of Information Systems and Informatics, 6(2), 1052–1069.

Nunes, P. F. V., Antunes, M., & Silva, C. (2021). Evaluating cybersecurity attitudes and behaviors in Portuguese healthcare institutions. Procedia Computer Science, 181, 412–419.

Nurcahyani, F., Mantoro, T., Pasma, S. A., & Wijiyanti, R. (2024). Vulnerability Analysis of Mobile JKN (Jaminan Kesehatan Nasional) to Prevent Cyber Attacks. In IEEE ICCED.

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.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). Computers & Security, 42, 165–176.

Pradipta, A. R., & Utomo, R. G. (2025). Enhancement of the Human Aspects of Information Security Questionnaire (HAIS-Q): for Indonesia Educational Institutions. In IEEE ICOSEIT.

Rohan, R., Pal, D., Hautamaki, J., Funilkul, S., Chutimaskul, W., & Thapliyal, H. (2023). A systematic literature review of cybersecurity scales assessing information security awareness. Heliyon, 9(3), e14234.

Santoso, V. A., Tjahjono, D. K., & Joewono, J. C. (2026). Dataset: Determinants of Cybersecurity Awareness among Indonesian Generation Z: A PLS-SEM Approach [Data set]. Zenodo. https://doi.org/10.5281/zenodo.18923032

Saputra, R. (2023). Analisis Keamanan Data Kesehatan di Indonesia: Studi Kasus Kebocoran Data BPJS Kesehatan. Jurnal Keamanan Siber, 5(1), 12–24.

Sari, D. R., Kusno, H. S., Jamal, N., Pongtuluran, E. H., & Anhar, W. (2024). Integrasi HAIS-Q dan ISA Model dalam Peningkatan Kesadaran Keamanan Informasi untuk Mitigasi Risiko Siber. Jurnal Informatika, 14(2).

Schmidt, T., Nohr, C., & Koppel, R. (2021). A Simple Assessment of Information Security Awareness in Hospital Staff Across Five Danish Regions. Studies in Health Technology and Informatics, 281, 607–611.

Siallagan, A. D., Diana, H. S., Fitriya, N. I., Nurhuda, P. M., Oktaviany, V., Luginasari, Y., et al. (2025). Revolusi Kesehatan Digital melalui Teknologi Big Data dalam Aplikasi Mobile JKN: Rapid Review. Jurnal Informasi Kesehatan, 16(1).

Styoutomo, Y. A., & Ruldeviyani, Y. (2023). Information Security Awareness Raising Strategy Using Fuzzy AHP Method with HAIS-Q and ISO/IEC 27001:2013. CommIT Journal, 17(2), 133–149.

Verizon. (2024). 2024 Data Breach Investigations Report. Verizon Business.

Xu, X., Hong, W. C. H., Kolletar-Zhu, K., Zhang, Y., & Chi, C. (2024). Validation and application of the human aspects of information security questionnaire for undergraduates: effects of gender, discipline and grade level. Behaviour & Information Technology, 43(12), 2799–2810.

Zlatolas, L. N., Welzer, T., & Lhotska, L. (2024). Data breaches in healthcare: security mechanisms for attack mitigation. Cluster Computing, 27(7), 8639–8654.