A Multi-Wave Assessment of Information Security Awareness in Personal Device Use among Brazilian Users

Arthur C. Souza[1], **Lucila M. S. Bento**[1]

[1]Departamento de Informática e Ciência da Computação
Instituto de Matemática e Estatística
Universidade do Estado do Rio de Janeiro (UERJ)

arthcs@gmail.com, lucila.bento@ime.uerj.br

Abstract. *Information Security Awareness (ISA) instruments for Brazilian users are scarce, multi-wave evidence remains scarce, and the Knowledge–Attitude–Behavior (KAB) model has been validated mainly in corporate settings. We propose a self-assessment instrument applied across three waves ($n = 173$). The composite ISA score remained stable (∼65/100), but platform-automated behaviors (OS updates, MFA) improved while agency-dependent behaviors (password rotation, non-reuse, reporting) stagnated. Path analysis showed a dominant direct knowledge–behavior effect ($\beta = 0.46$), with attitudinal mediation explaining only 14.5%, contrasting with prior corporate findings. Self-declared concern declined despite intensified cyber-fraud reporting, plausibly reflecting security fatigue. Awareness campaigns should prioritize actionable knowledge over appeals to concern.*[1]

1. Introduction

Recent threat intelligence reports consistently place Brazil among the most targeted countries worldwide and the predominant focal point in Latin America for digital attacks [Labs 2026; CNN Brasil 2025]. Financial fraud has emerged as one of the most widespread manifestations of this threat landscape, and survey data indicate that around half of Brazilians experienced some form of fraud, with the majority of victims suffering financial damage [de Segurança Pública 2025b]. Instant-payment schemes have also become a central vector of cybercrime. Between July 2024 and June 2025, an estimated 24 million Brazilians were victimized by scams involving Pix or bogus bank slips, with losses nearing R$ 29 billion [Federal 2025; Datafolha 2025]. The 2025 Brazilian Public Security Yearbook further reports that fraud and digital scam cases now outnumber several traditional forms of in-person robbery in official crime statistics, highlighting the migration of victimization to online environments [de Segurança Pública 2025a]. Despite these technological and behavioral shifts, the human factor remains the dominant attack surface, with roughly 60% of breaches involving some human element such as error, social engineering, or misuse [Verizon 2025].

Information Security Awareness (ISA), understood as the combination of users' knowledge, attitudes, and behaviors regarding information protection [Hanus et al. 2018],

[1]Generative Artificial Intelligence tools, including ChatGPT, Grammarly, and Gemini, were used to support the textual revision of this work.

has therefore become a central object of cybersecurity research. While corporate-environment studies have proliferated, evidence on personal-context ISA in Brazil remains sparse. The recent study by [Henklain et al. 2024] is the closest precedent, characterizing ISA in 232 respondents from Brazil's Northern region and linking behavior to Big Five personality traits. Their work explicitly calls for studies covering more diverse samples, a gap that this paper seeks to help address.

Beyond geographic coverage, an even more underexplored question concerns cross-wave patterns: how do reported security behaviors differ across repeated cross-sectional waves as awareness campaigns proliferate and platforms increasingly automate security mechanisms (forced OS updates, mandatory MFA, default antivirus)? Cross-sectional studies cannot answer this question. Although our design does not follow the same individuals over time, repeated cross-sectional measurement with a stable instrument enables the observation of population-level cross-wave patterns in reported behaviors and attitudes.

A third underexplored question is theoretical. The Knowledge–Attitude–Behavior (KAB) model, operationalized for information security by [Parsons et al. 2013], predicts that knowledge influences behavior largely through attitude. Whether this mediation pattern transfers to personal contexts, where security knowledge is comparatively scarce and platform automation may weaken the relationship between motivation and action, has not been empirically tested.

In this context, these gaps motivate four contributions of this work:

1. A self-assessment instrument for personal-context ISA, theoretically grounded in international frameworks (NIST CSF, ISO/IEC 27002, CIS Controls) and prior validated questionnaires (HAIS-Q, SeBIS, KAB), adapted to the Brazilian reality and openly available for replication and extension.
2. One of the first multi-wave repeated cross-sectional assessments of ISA in Brazil, based on three data-collection waves (2023, 2024, 2025–2026) with 173 respondents. We document contrasting cross-wave patterns of *automated* and *agency-dependent* security behaviors.
3. A path-analytic test of the KAB model in a Brazilian personal-context sample. Our findings indicate that the strong attitude-mediation pattern reported for Australian corporate employees [Parsons et al. 2013] is substantially weaker in this setting, with knowledge exerting a dominant direct effect on behavior ($\beta = 0.46$) and attitudinal mediation accounting for only 14.5% of the total effect. This contrast may reflect the changing nature of personal-context ISA under platform automation.
4. A complementary geographic and analytical perspective to [Henklain et al. 2024]: while their study covered the Northern region using a personality-trait lens, our predominantly Southeastern sample with multi-wave and mediation-analytic lenses enables triangulation of findings about Brazilian users' security posture.

The remainder of this paper is organized as follows. Section 2 reviews related work on Information Security Awareness and personal-context security behavior. Section 3 presents the instrument design, data collection process, and analytical methodology. Section 4 reports the empirical findings. Section 5 interprets the results, with particular attention to the automation–agency distinction and the observed KAB mediation structure. Finally, Section 6 concludes the paper and outlines directions for future work.

2. Related Work

International standards such as ISO/IEC 27001/27002 [ISO 2022], the NIST Cybersecurity Framework [Pascoe et al. 2024] (NIST CSF), and the CIS Controls [Center for Internet Security 2024] provide widely adopted reference structures for information security management. Although primarily corporate, several of their principles (risk identification, protection, detection, response, and recovery) extend to personal contexts. [Bashofi and Salman 2022] discuss the integration of these frameworks for cybersecurity maturity assessment. In Brazil, the LGPD (Lei nº 13.709/2018) [Brasil 2018] regulates personal data protection and motivates citizen awareness of basic security hygiene. These frameworks provide the technical foundations upon which many ISA assessment models have subsequently been constructed.

Among these models, the KAB framework [Kruger and Kearney 2006] became one of the most influential approaches for operationalizing ISA. One of its best-known operationalizations is the Human Aspects of Information Security Questionnaire (HAIS-Q)[Parsons et al. 2013; Parsons et al. 2017], which evaluates security awareness across seven domains, including passwords, email, internet use, social media, mobile devices, information handling, and incident reporting. The instrument was developed using a hybrid inductive-exploratory approach combining qualitative interviews with quantitative questionnaire development. Following the rationale of [Karjalainen 2011], this approach acknowledges that information security behavior is shaped by multiple competing models, each capturing only part of the phenomenon. The Security Behavior Intentions Scale (SeBIS) [Egelman and Peer 2015] measures self-reported intentions across four dimensions (device securement, password generation, proactive awareness, and updating). Together, these instruments have supported a growing body of empirical ISA research in organizational and personal contexts.

In corporate environments, prior studies consistently report positive associations between security knowledge and secure behavior [Tariq et al. 2014; Bauer and Bernroider 2017; Wahyudiwan et al. 2017]. [Hanus et al. 2018] showed that employees susceptible to phishing had lower ISA. [Gioulekas et al. 2022] reported low to medium ISA among healthcare workers, while [Georgiadou et al. 2022] found acceptable ISA levels among home-office workers during COVID-19.

Outside organizational settings, ISA has also been investigated in personal-use and educational contexts. [Bitton et al. 2020] proposed a smartphone monitoring framework combining survey and behavioral telemetry. [Wash et al. 2017] tested whether self-reports match observed behavior, finding agreement in selected dimensions (passwords, internet). Several studies of university students [Chumaera et al. 2022; Salem et al. 2021; Senthilkumar and Easwaramoorthy 2017; Pósa and Grossklags 2022] consistently find that prior incident experience and professional contact with technology raise ISA, while password practices and Wi-Fi habits remain weak across populations.

Despite Brazil's prominence as a major target of cybercrime, academic ISA research in the country remains comparatively limited. The most recent and closest study is [Henklain et al. 2024], which characterized cybersecurity knowledge and behaviors among 232 respondents, predominantly from the Northern region (Roraima/Amazonas). They reported moderate-to-good knowledge but low frequency of secure behavior and identified associations between Big Five personality traits and ISA. The authors explicitly

recommend future studies covering more diverse samples and contexts.

The present work responds directly to that gap by (i) covering a different geographic region (predominantly Southeastern, urban), (ii) adopting a complementary analytical lens focused on cross-wave patterns rather than personality, and (iii) applying a partially overlapping but independently constructed instrument grounded in NIST CSF, CIS Controls, HAIS-Q, and SeBIS.

3. Methodology

This section describes the methodological workflow summarized in Figure 1: the Literature Review, Framework Mapping, and Expert Review stages, described jointly in Section 3.1, produced the final 15-item instrument; Section 3.2 then describes data collection across the three waves; and Section 3.3 describes the analytical strategy.

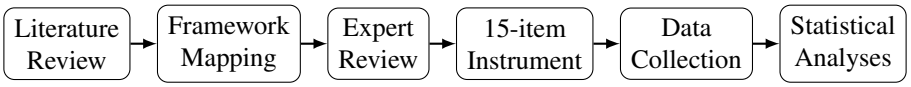

Figure 1. Overview of the methodological workflow.

3.1. Instrument Design

The instrument was developed through a literature-grounded hybrid inductive-exploratory process. We reviewed 23 ISA assessment studies identified through structured searches in ACM Digital Library, IEEE Xplore, and Wiley Online Library using the search string `("Security awareness" OR "Information Security awareness") AND ("Human Factors" OR "individual") AND ("assessing" OR "assessment" OR "evaluation") AND ("framework" OR "standard" OR "security controls")`, restricted to 2017–2023. The most frequently assessed ISA dimensions were then mapped to the NIST CSF, ISO/IEC 27002, and CIS Controls to ensure coverage of practically relevant behaviors. Although based on framework versions available up to 2023, these dimensions remain conceptually consistent with subsequent revisions.

To improve content validity, the instrument was refined through a hybrid inductive-exploratory process inspired by the HAIS-Q methodology [Parsons et al. 2013] and advocated by [Karjalainen 2011]. The process combined literature review with iterative evaluation by two researchers experienced in corporate information security awareness. Multiple rounds assessed item clarity, response scales, behavioral coverage, and alignment with the proposed dimensions. Following *respondent debriefing* and *cognitive testing* principles [DeMaio and Rothgeb 1996; Collins 2003], ambiguous or technically inaccurate items were revised before deployment.

The final instrument contains 15 items organized into four conceptual dimensions, together with demographic questions on gender, age, education, city size, professional field, and devices used. It was intentionally designed as a compact instrument to facilitate voluntary participation and reduce respondent burden across repeated waves. Table 1 summarizes its structure. The study was approved by the Research Ethics Committee of the Universidade do Estado do Rio de Janeiro.

Table 1. Instrument structure

Dimension	Item	Question (abbreviated)	Scale	Reference
Self-perception	Q1	Self-declared ISA knowledge	Likert 1–5	KAB
	Q2	Self-declared ISA concern	Likert 1–5	KAB
D1: Update & Protection	Q3	OS update frequency	Likert 1–5	CIS, NIST
	Q4	Antivirus scanning frequency	4-option freq.	CIS, NIST
D2: Passwords	Q5	Password rotation frequency	4-option freq.	HAIS-Q, SeBIS
	Q6	Password reuse across services	Yes/No	HAIS-Q, SeBIS
	Q7	Use of strong passwords	Yes/No	HAIS-Q, SeBIS
	Q8	Multi-factor authentication	Yes/No	SeBIS
	Q9	Password manager use	Yes/No	CIS
D3: Online Exposure	Q10	Following links from unknown sources	Yes/No	HAIS-Q
	Q11	Public Wi-Fi use	Yes/No	HAIS-Q
	Q12	Sharing personal info on social media	Yes/No	HAIS-Q
	Q13	Sharing personal info with third parties	Yes/No	HAIS-Q
D4: Active Awareness	Q14	Reporting suspicious behavior	Yes/No	HAIS-Q
	Q15	Alerting others about insecure behavior	Yes/No	KAB

3.2. Data Collection

Data were collected through Google Forms in three waves: W1 (Apr.–Nov. 2023; $n = 92$), W2 (Jun.–Sep. 2024; $n = 38$), and W3 (May 2025–Feb. 2026; $n = 43$), yielding a final dataset of 173 valid responses. Recruitment was non-probabilistic through social-network posts (LinkedIn, Facebook, Instagram) and email lists. Differences in sample size and composition across waves reflect the varying reach of these recruitment channels, as no quota or stratification procedure was applied. Participation was voluntary and conditional on informed consent ("*Termo de Consentimento Livre e Esclarecido*") presented before the questionnaire. All respondents were 18 years or older. Names and email addresses were collected solely for consent verification and dissociated from responses prior to analysis. Eight participants responded in both W1 and W2; none participated in all three waves. Responses were treated as independent samples; consequently, cross-wave differences reflect variation between samples rather than within-individual behavioral change.

Following the protocol proposed in [Parsons et al. 2013], the dataset was screened for suspicious cases indicative of inattentive responding. Adapting their criterion (53/63 = 84% uniformity) to our shorter instrument, we flagged respondents who answered identically across all 10 binary items. Six respondents (3.5%) met this stricter criterion. Because secure-behavior responses can be legitimately uniform for individuals with consistently cautious habits (e.g., a respondent who avoids all four exposure scenarios in D3), we examined these cases individually: their composite CSI Scores fall within the normal distribution (range 67–100), their Likert responses to Q1–Q3 show internal variation, and their demographic profiles match the broader sample. We therefore retained them. No respondent showed completely uniform Likert and binary responses simultaneously, which would have indicated true straight-lining.

Although the study spans three temporal waves over approximately three years, it should not be interpreted as a classical longitudinal panel design. The overwhelming majority of respondents differ across waves, and the analyses therefore characterize repeated cross-sectional population-level patterns rather than within-individual behavioral change. Our use of temporal comparisons is thus exploratory and descriptive, intended to identify broad cross-wave patterns rather than causal longitudinal dynamics.

3.3. Analytical Strategy

The analytical procedure was organized into five stages.

1. Instrument reliability was assessed through Cronbach's α, computed for each conceptual dimension and for the full 13-item behavioral scale. The two self-declaration items (Q1 and Q2) were excluded from the behavioral-scale reliability analysis. Because the instrument combines Likert, ordinal-frequency, and binary items, all behavioral variables were min–max normalized to the interval $[0, 1]$ before composite-score computation.
2. We constructed a composite 0–100 behavioral indicator, termed the *ISA Behavioral Score* (CSI Score), defined as the mean of the 13 normalized behavioral items, where higher values indicate more secure reported behavior.
3. Cross-wave comparisons across the three waves were conducted at both the composite and item levels. Distributions of the CSI Score and ordinal items were compared using the Kruskal–Wallis test, while binary items were analyzed using Pearson's chi-squared test, adopting $\alpha = 0.05$.
4. Demographic associations with the CSI Score were examined using Spearman's rank correlation for ordinal variables (age and education level) and the Mann–Whitney U test for binary group comparisons (gender and Exact-Sciences versus non-Exact-Sciences fields). The association between self-declared ISA knowledge (Q1) and the CSI Score was examined as evidence of convergent validity.
5. We conducted an exploratory path analysis of the KAB model following the procedure described by [Parsons et al. 2013]. Self-declared ISA knowledge (Q1) was mapped to the K component, self-declared concern (Q2) to the A component, and the CSI Score to the B component. Two regressions were estimated: $A = \beta_1 K$ and $B = \beta_2 K + \beta_3 A$. The Sobel test [Sobel 1982] was used to evaluate the statistical significance of the indirect effect $K \rightarrow A \rightarrow B$. Given the compact nature of the instrument and the use of single-item operationalization for K and A, the mediation analysis should be interpreted as exploratory rather than as a strict psychometric replication of prior KAB studies.

All analyses were conducted in Python 3.11 using pandas 2.x and SciPy 1.x. Threats to validity and interpretive limitations are discussed in Section 5.

4. Results

Results are organized in three stages: sample characterization and instrument reliability, KAB relationships and composite behavioral indicators (Section 4.1), and cross-wave item-level patterns with demographic associations (Section 4.2). Table 2 summarizes the demographic profile of the 173 respondents across the three waves.

Among the 173 respondents, most were male (67%), aged 30–49 (60%), had higher education (75%), and lived in cities with more than one million inhabitants (64%).

Table 2. Demographic profile of the sample by wave.

Variable	W1 ($n = 92$)	W2 ($n = 38$)	W3 ($n = 43$)	Total ($n = 173$)
Gender				
Male	62 (67%)	25 (66%)	29 (67%)	116 (67%)
Female	29 (32%)	13 (34%)	14 (33%)	56 (32%)
Age				
18–29	21 (23%)	4 (11%)	17 (40%)	42 (24%)
30–49	55 (60%)	24 (63%)	25 (58%)	104 (60%)
50+	16 (17%)	10 (26%)	1 (2%)	27 (16%)
Education				
Up to high school	14 (15%)	6 (16%)	2 (5%)	22 (13%)
Higher ed. (in progress/complete)	56 (61%)	20 (53%)	24 (56%)	100 (58%)
Postgraduate	22 (24%)	12 (32%)	17 (40%)	51 (29%)
Field (top)				
Exact Sciences	27 (29%)	10 (26%)	20 (47%)	57 (33%)
Other fields	65 (71%)	28 (74%)	23 (53%)	116 (67%)

Exact Sciences was the largest professional field (33%), and smartphones were the predominant device (98%).

The demographic composition remained broadly stable across waves, although W2 included a higher proportion of respondents aged 40–49, while W3 showed larger proportions of postgraduate and Exact-Sciences-affiliated participants. These demographic differences should be considered when interpreting cross-wave comparisons, as part of the observed variation may reflect differences in sample composition rather than changes in the broader population.

Table 3 reports Cronbach's α coefficients for the four conceptual dimensions and for the full behavioral scale. Internal-consistency coefficients were modest, with only D1 approaching conventional thresholds ($\alpha \approx 0.7$). This pattern is compatible with the inherently multifaceted nature of personal-context ISA, where behaviors such as password reuse, public Wi-Fi usage, and suspicious-content reporting may reflect distinct psychological and contextual mechanisms. Similar heterogeneity across dimensions has been reported in HAIS-Q-related studies [Parsons et al. 2017].

Table 3. Cronbach's α by instrument dimension ($n = 173$).

Dimension	k (items)	Cronbach's α
D1 – Update & Protection	2	0.66
D2 – Passwords	5	0.38
D3 – Online Exposure	4	0.47
D4 – Active Awareness	2	0.43
Full 13-item behavioral scale	13	0.57

To better characterize the low reliability of the Passwords dimension ($\alpha = 0.38$), we examined Spearman inter-item correlations among its five components. Correlations were uniformly weak (ρ from -0.12 to 0.28), and password non-reuse (Q6) showed a

non-significant item-total correlation ($\rho = 0.03$, $p = 0.670$), unlike the other four items (ρ from 0.16 to 0.33, all $p < 0.05$). Removing Q6 raised reliability to $\alpha = 0.40$ for the remaining four items. We had hypothesized, following the automation–agency framework of Section 5.1, that D2 might split into an ongoing-hygiene facet (Q5, Q6) and a setup/adoption facet (Q7–Q9); the data do not support this split ($\alpha = 0.18$ and 0.32, respectively, both below the full scale). The low reliability of D2 instead appears driven by Q6 behaving as a comparatively independent item. We recommend reconsidering this item in future revisions of the instrument.

Accordingly, the proposed instrument should be interpreted primarily as a compact, behavior-oriented multidimensional assessment tool rather than as a strictly unidimensional psychometric scale. Its objective is to provide broad coverage of relevant information-security behaviors in personal-use contexts while maintaining a questionnaire short enough to encourage voluntary participation across repeated survey waves. Therefore, the individual dimensions and item-level analyses are considered as important as the composite behavioral score itself.

4.1. KAB Relationships and Composite Behavioral Indicators

To examine the construct validity of the proposed instrument, we analyzed the relationship between self-declared ISA knowledge (Q1), self-declared concern (Q2), and the CSI Score within the KAB framework.

Spearman correlations revealed moderate positive associations between knowledge and behavior ($\rho = 0.535$, $p < 0.001$) and between concern and behavior ($\rho = 0.371$, $p < 0.001$), supporting the convergent validity of the instrument. Respondents reporting higher ISA knowledge also tended to report more secure behaviors, although the magnitude of the association remains compatible with the behavior–knowledge gap discussed in prior ISA studies [Bauer and Bernroider 2017].

We then conducted an exploratory path analysis following the procedure described by [Parsons et al. 2013]. The regression $A = \beta_1 K$ yielded $\beta_1 = 0.340$, $R^2 = 0.116$, $F(1, 171) = 22.37$, $p < 0.001$. The regression $B = \beta_2 K + \beta_3 A$ yielded $R^2 = 0.342$, $F(2, 170) = 44.15$, $p < 0.001$, with $\beta_2 = 0.464$ ($t = 7.01$, $p < 0.001$) for the direct effect of knowledge on behavior and $\beta_3 = 0.231$ ($t = 3.50$, $p < 0.001$) for the effect of concern on behavior. The indirect effect through attitude was 0.079, corresponding to 14.5% of the total effect, and the Sobel test indicated statistically significant mediation ($z = 2.81$, $p = 0.005$). Figure 2 summarizes the resulting path structure.

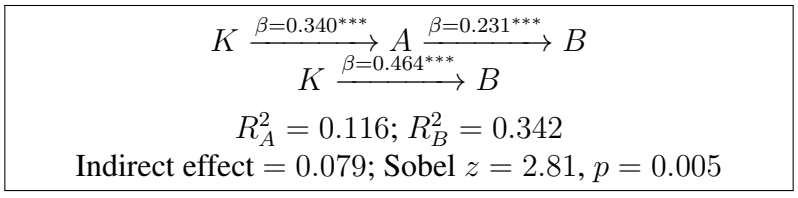

Figure 2. Exploratory path analysis of the KAB model ($n = 173$). $^{***}p < 0.001$.

The CSI Score presented mean $= 65.3$ (SD $= 15.9$), median $= 66.7$, and range $= 17$–100. The distribution was approximately normal with slight ceiling tendency. Comparisons across the three repeated cross-sectional waves revealed no statistically significant differences in the composite score ($H = 0.84$, $p = 0.658$), as summarized in Table 4.

Table 4. CSI Score across the three waves.

Wave	n	Mean	SD
W1 (2023)	92	64.6	16.8
W2 (2024)	38	64.7	15.4
W3 (2025–26)	43	67.1	14.6
Kruskal–Wallis: $H = 0.84$, $p = 0.658$			

Although the composite CSI Score remained relatively stable across waves, item-level analyses revealed distinct cross-wave patterns across security behaviors.

4.2. Cross-wave Item-level Patterns and Demographic Associations

Table 5 reports the item-level distributions across waves and significance tests.

Table 5. Item-level results across the three waves. Asterisks denote $p < 0.05$ (*), $p < 0.01$ (**), $p < 0.001$ (***).

Item	W1	W2	W3	Test	Stat	p
Q1 Self-declared knowledge (mean)	3.11	3.03	3.07	K-W	0.02	0.992
Q2 Self-declared concern (mean)	4.12	4.05	3.63	K-W	8.67	**0.013***
Q3 OS update frequency (mean)	3.45	3.45	4.28	K-W	14.59	**<0.001*****
Q4 Antivirus frequency (mean 1–4)	2.42	2.62	2.84	K-W	2.94	0.229
Q5 Password rotation freq (1–4)	1.78	1.61	1.40	K-W	6.73	**0.034***
Q6 Not reusing passwords (%)	38%	45%	30%	χ^2	1.83	0.401
Q7 Strong passwords (%)	93%	84%	88%	χ^2	2.82	0.245
Q8 MFA use (%)	82%	71%	91%	χ^2	5.16	0.076
Q9 Password manager (%)	37%	37%	37%	χ^2	0.00	0.999
Q10 Avoiding unknown links (%)	91%	92%	98%	χ^2	1.91	0.385
Q11 Avoiding public Wi-Fi (%)	59%	53%	56%	χ^2	0.42	0.811
Q12 Not sharing on social (%)	79%	79%	81%	χ^2	0.10	0.953
Q13 Not sharing w/ third party (%)	92%	95%	100%	χ^2	3.44	0.179
Q14 Reporting suspicious (%)	53%	71%	60%	χ^2	3.57	0.168
Q15 Alerting others (%)	80%	79%	74%	χ^2	0.63	0.728

The item-level analyses reveal heterogeneous cross-wave patterns across different security behaviors. Operating-system update frequency (Q3) increased substantially across waves, from 3.45 to 4.28 on the 1–5 scale ($H = 14.59$, $p < 0.001$). Antivirus-scanning frequency (Q4) showed progressively higher values across the three waves (2.42 $\rightarrow$ 2.84), although without statistical significance ($p = 0.229$). Multi-factor authentication adoption (Q8) reached 91% in W3, compared with 82% in W1 and 71% in W2 ($p = 0.076$). Avoidance of unknown links (Q10) remained consistently high across all waves (91–98%).

By contrast, password-related behaviors showed either stability or downward tendencies. Password-rotation frequency (Q5) showed significantly lower values in later waves ($H = 6.73$, $p = 0.034$), while the proportion of respondents reporting password non-reuse (Q6) declined from 45% in W2 to 30% in W3, although without statistical significance ($p = 0.401$). Self-declared concern with ISA (Q2) also decreased significantly

across the observation period ($H = 8.67$, $p = 0.013$). Password-manager adoption (Q9) remained unchanged at 37% throughout all waves.

Several behaviors remained consistently high and stable during the observation period, including strong-password use (Q7), avoidance of unknown links (Q10), and reluctance to share personal information with third parties (Q13). Similarly, avoidance of personal-information sharing on social networks (Q12) and alerting others about insecure behavior (Q15) remained relatively stable across the three waves.

We also examined demographic associations with the CSI Score. Men reported higher scores than women (67.5 vs. 60.9; Mann–Whitney $U = 4026$, $p = 0.011$). The largest demographic difference was associated with professional field: respondents from Exact Sciences ($n = 57$) presented substantially higher CSI Scores than respondents from other fields (74.5 vs. 60.8; $U = 5026$, $p < 0.001$). Education level showed weak but statistically significant positive association with the CSI Score ($\rho = 0.150$, $p = 0.049$), whereas age showed no significant association ($\rho = -0.050$, $p = 0.510$).

The comparatively higher CSI Scores among Exact-Sciences respondents are consistent with prior studies reporting positive associations between technical familiarity and information-security behavior [Aljedaani et al. 2021; Henklain et al. 2024].

5. Discussion

The results discussed in this section are interpreted as exploratory and hypothesis-generating, since the study does not directly measure platform-enforcement mechanisms, automation features, or exposure to awareness interventions.

5.1. The Automation–Agency Divergence

One of the most notable multi-wave patterns observed in this study is the divergence between two broad categories of security behavior. Behaviors commonly associated with platform-level automation or enforcement, such as automatic OS updates, default antivirus protection, mandatory MFA, and browser-level link warnings, generally showed higher frequencies in later waves. In contrast, behaviors requiring active user initiative, such as password rotation, password non-reuse, password-manager adoption, and suspicious-content reporting, showed relatively stable or lower frequencies in later waves.

To test whether this divergence is confounded by the changing educational and occupational composition of the sample, we regressed the automated and agency-dependent composites on wave (W1 as reference), education, and field (Exact Sciences vs. other). The W3 effect on automated behaviors remained significant after adjustment ($\beta = 0.113$, $p = 0.024$; unadjusted $\beta = 0.146$, $p = 0.005$), with Exact Sciences as an independent predictor ($\beta = 0.153$, $p < 0.001$). For agency-dependent behaviors, the wave effect was non-significant both before and after adjustment, but adjustment strengthened rather than attenuated the estimated decline ($\beta = -0.079$, $p = 0.079$, versus $\beta = -0.033$, $p = 0.490$ unadjusted), since education ($\beta = 0.041$, $p = 0.012$) and Exact Sciences ($\beta = 0.192$, $p < 0.001$) both predicted higher agency-dependent scores and W3 had more of both. Compositional shift therefore does not manufacture the automation–agency divergence; if anything, it partially masks the agency-side decline.

Although platform-enforcement mechanisms were not directly measured, the observed pattern is compatible with the hypothesis that they may influence some security

behaviors. If correct, this interpretation carries two practical implications. First, awareness campaigns should not evaluate success solely through aggregate adoption indicators, since these indicators may improve even when underlying awareness remains stable. Distinguishing automated from user-dependent behaviors may therefore provide a more informative view of awareness dynamics. Second, the behaviors that remained stagnant or regressive, particularly password rotation, password non-reuse, password-manager adoption, and suspicious-content reporting, may represent areas where future awareness-oriented interventions could have greater impact.

5.2. KAB Mediation Patterns in the Personal Context

The path analysis revealed a mediation structure that differs from the corporate-context pattern reported by [Parsons et al. 2013]. In our sample, the direct association between knowledge and behavior ($\beta = 0.464$) exceeded the indirect effect mediated through concern ($\beta = 0.079$), with only 14.5% of the total effect mediated by attitude, contrasting with the Australian corporate sample ($\beta_{K \to A} = 0.812$, $\beta_{A \to B} = 0.724$, $\beta_{K \to B} = 0.185$).

Two complementary interpretations may explain this contrast. First, in corporate environments, security knowledge is likely more homogeneous because employees are exposed to organizational policies and mandatory training. Behavioral differences may therefore depend more strongly on motivation to apply known practices. In personal contexts, however, security knowledge remains more unevenly distributed, making its direct association with behavior comparatively stronger.

A second interpretation relates to the increasing presence of platform-level automation. As platforms automate security-relevant decisions and enforce protective mechanisms more systematically, motivation alone may become less predictive of certain behaviors. Users may adopt MFA, for example, not necessarily because of elevated concern, but because banks, email providers, and social networks increasingly require it. What remains differentiated across users are behaviors that still depend on active knowledge and initiative beyond the platform-enforced baseline, such as recognizing phishing attempts, configuring password managers, or reporting suspicious content. This contrast also carries a methodological implication: mediation patterns reported in corporate-context KAB studies should not automatically be assumed to generalize to personal-context settings.

5.3. The Drop in Self-Declared Concern and the Causality Question

Another notable finding is the decline in self-declared concern regarding ISA (Q2: $4.12 \to 4.05 \to 3.63$, $p = 0.013$) during a period characterized by intensified national reporting on cyber-fraud and Pix-related scams. At least three non-exclusive interpretations may help explain this pattern.

One possible explanation is security fatigue, where continuous exposure to alarming reports about cybercrime gradually desensitizes users rather than increasing vigilance. Another is the perception that platforms increasingly absorb part of the security burden, reducing the need for constant personal attention. A third interpretation relates to the reverse-causality problem discussed by [Parsons et al. 2013]. Because many information-security threats are low-probability and high-consequence events, behaviors that repeatedly produce no visible negative outcome may become implicitly reinforced over time. Reusing passwords, ignoring update prompts, or connecting to public Wi-Fi without immediate consequences may gradually normalize these practices and reduce perceived risk.

Under this interpretation, the conventional KAB direction (knowledge → attitude → behavior) may coexist with an alternative feedback dynamic in which repeated behavior also influences perceived concern and risk perception. Because the present design is repeated cross-sectional rather than longitudinal, the study cannot distinguish between these explanations directly. Nevertheless, the observed pattern is compatible with all three mechanisms operating simultaneously.

5.4. Comparison with [Henklain et al. 2024]

The present findings align with [Henklain et al. 2024] in the broader observation that Brazilian users report moderate-to-good security knowledge alongside persistent insecure behaviors. At the same time, the studies offer complementary perspectives.

One distinction concerns regional composition. While [Henklain et al. 2024] focused predominantly on respondents from the Northern region of Brazil, the present study draws mainly from Southeastern urban participants. Taken together, the two studies broaden the current empirical picture of personal-context ISA in Brazil. Moreover, the recurrence of patterns such as weak password hygiene, ambivalence regarding public Wi-Fi, and avoidance of explicit personal-data sharing may reflect tendencies extending beyond specific regional contexts.

Another distinction lies in the analytical focus. Whereas [Henklain et al. 2024] emphasized personality traits and cross-sectional behavioral associations, the present work explores repeated cross-sectional temporal patterns and the relationship between knowledge, concern, and behavior within the KAB framework. This perspective becomes particularly relevant in contexts where platform automation and enforcement mechanisms may progressively reshape how awareness translates into behavior.

5.5. Implications for Awareness Initiatives

The findings have practical implications for the design of awareness initiatives in personal-use contexts. While [Parsons et al. 2013] emphasize the combination of knowledge and motivational factors in corporate settings, our results suggest that practical knowledge plays a stronger role in personal contexts. Awareness initiatives may therefore benefit from emphasizing actionable guidance, including password-manager adoption, MFA configuration, phishing recognition, and suspicious-message reporting, rather than abstract appeals to concern.

Another implication concerns the format of awareness interventions. Prior literature consistently highlights the advantages of contextualized and case-based approaches over generic exposition [Parsons et al. 2013]. In the Brazilian context, demonstrations involving Pix-related scams, phishing attempts, and real-world fraud scenarios may be more effective than generic recommendations detached from users' everyday experiences.

Password-management practices remain one of the weakest areas observed in the dataset. Password reuse remained frequent, password rotation declined across waves, and password-manager adoption remained stagnant at approximately one-third of respondents. These findings suggest that password-related behaviors continue to represent an important target for future awareness efforts and platform-design improvements. In contrast, MFA adoption appears increasingly associated with platform-level requirements,

reaching 91% in W3. Further increases may therefore depend less on persuasion alone and more on broader adoption of mandatory MFA mechanisms across services.

Finally, the substantial CSI Score gap between Exact-Sciences-affiliated respondents and participants from other fields suggests that uniform awareness campaigns may not affect all audiences equally. Tailored educational materials for non-technical audiences, which may currently receive less targeted cybersecurity guidance, are likely to produce more meaningful gains in personal-context ISA.

5.6. Limitations

This study has several limitations that should be considered when interpreting the results. The sample is non-probabilistic and participants were recruited through social networks and email lists, likely introducing homophily effects and over-representation of urban, highly educated, and technologically familiar respondents. Exact-Sciences-affiliated participants are substantially overrepresented relative to the broader Brazilian population, which likely upward-biases the observed CSI Scores. The findings should therefore be interpreted as exploratory evidence drawn from a specific recruitment context rather than as nationally representative estimates of Brazilian ISA.

All measures are self-reported and therefore subject to social-desirability bias, recall limitations, and self-perception inaccuracies [Wash et al. 2017]. In addition, the KAB path analysis relies on single-item measures of knowledge and concern, unlike validated multi-item instruments such as HAIS-Q. It should therefore be interpreted as an exploratory approximation of the KAB structure rather than a strict psychometric replication of [Parsons et al. 2013]. The CSI Score intentionally aggregates heterogeneous security behaviors reflecting complementary dimensions of personal information security rather than a single latent construct. Consequently, moderate internal-consistency coefficients were expected and should not be interpreted as evidence that the instrument lacks practical usefulness. Instead, they reflect the multidimensional nature of ISA, where behaviors such as password management, software updating, online exposure, and active awareness are only partially related and influenced by different cognitive, contextual, and technological factors.

Although the study spans three temporal waves, the design is repeated cross-sectional rather than longitudinal. Because most respondents differ across waves, cross-wave differences may partly reflect sample-composition variation rather than within-individual behavioral evolution. Moreover, the study does not directly measure exposure to awareness campaigns, platform-enforcement mechanisms, security incidents, or automation features. Interpretations involving security fatigue, automation, or motivational dynamics should therefore be understood as exploratory rather than causal conclusions.

Finally, the comparatively small size of W2 ($n = 38$) reduces statistical power for detecting small-to-moderate effects and increases uncertainty around some wave-specific comparisons. The study also involves multiple item-level hypothesis tests without formal correction for family-wise error rate, and marginal findings should therefore be interpreted cautiously. The compact nature of the instrument additionally limits the depth of each ISA dimension, although this was a deliberate trade-off to support voluntary participation and repeated application over time.

6. Conclusion

This paper presented a compact self-assessment instrument for Information Security Awareness in personal device use, grounded in NIST CSF, ISO/IEC 27002, CIS Controls, HAIS-Q, and SeBIS, and applied across three temporal waves involving 173 Brazilian respondents. Given the repeated cross-sectional design and non-probabilistic sample, the findings should be interpreted as exploratory and hypothesis-generating.

Three main findings emerged. First, although the composite CSI Score was stable across waves, item-level analyses revealed a divergence between behaviors associated with platform-level automation (OS updates, MFA, antivirus), which showed higher frequencies in later waves, and behaviors dependent on active user initiative (password rotation, non-reuse, reporting), which stagnated or declined. Second, the exploratory KAB path analysis showed a stronger direct knowledge–behavior association ($\beta = 0.464$) than indirect mediation through concern ($\beta = 0.079$; 14.5% of total effect), contrasting with the corporate-context mediation structure of [Parsons et al. 2013] and suggesting that practical knowledge may play a stronger role than motivational factors in personal-use settings. Third, self-declared concern declined significantly despite intensified national attention to cyber-fraud, a pattern compatible with security fatigue, increasing reliance on platform-level protections, and the reinforcement of insecure behaviors that produce no visible negative consequences.

Demographic analyses indicated that Exact-Sciences-affiliated respondents presented substantially higher CSI Scores, consistent with prior work on technical familiarity and ISA. The instrument showed moderate convergent validity ($\rho = 0.535$) and modest overall internal consistency ($\alpha = 0.57$), reflecting the multidimensional nature of personal-context ISA. The findings complement [Henklain et al. 2024] by adding a Southeastern, repeated cross-sectional, and mediation-oriented perspective to the emerging empirical picture of ISA in Brazil. To support replication, we release a reproducibility package with the anonymized dataset, questionnaire, codebook, and analysis scripts, available at `https://github.com/4LNx8kACFi3vRrzNhvhHxc/AwarenessSBSeg2026`.

Future work may explore five main directions: probabilistic and nationally representative sampling, including quota-based recruitment across educational and occupational strata to reduce the Exact-Sciences/urban skew observed in the present sample; formal psychometric validation of the instrument (for instance, confirmatory factor analysis or item response theory) once larger samples are available; integration of behavioral telemetry as proposed by [Bitton et al. 2020]; longitudinal panel designs capable of tracking within-individual behavioral change; and intervention studies focused on behaviors that remained resistant to improvement across waves, particularly password-management and suspicious-content-reporting practices.

References

[Aljedaani et al. 2021] Aljedaani, B., Ahmad, A., Zahedi, M., and Babar, M. A. (2021). Security awareness of end-users of mobile health applications: An empirical study. In *17th EAI International Conf. on Mobile and Ubiquitous Systems*, pages 125–136.

[Bashofi and Salman 2022] Bashofi, I. and Salman, M. (2022). Cybersecurity maturity

assessment design using NIST CSF, CIS controls v8 and ISO/IEC 27002. In *2022 IEEE Intl. Conf. on Cybernetics and Computational Intelligence*, pages 58–62.

[Bauer and Bernroider 2017] Bauer, S. and Bernroider, E. W. N. (2017). From information security awareness to reasoned compliant action: Analyzing information security policy compliance in a large banking organization. *SIGMIS Database*, 48(3):44–68.

[Bitton et al. 2020] Bitton, R., Boymgold, K., Puzis, R., and Shabtai, A. (2020). Evaluating the information security awareness of smartphone users. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–13.

[Brasil 2018] Brasil (2018). Lei nº 13.709, de 14 de agosto de 2018. lei geral de proteção de dados pessoais. Diário Oficial da União, Brasília, DF.

[Center for Internet Security 2024] Center for Internet Security (2024). CIS Critical Security Controls Version 8.1.

[Chumaera et al. 2022] Chumaera, M. M., Safitri, S., and Ayu, M. A. (2022). Assessing students' information security awareness through the knowledge, attitude, and behavior model. In *2022 IEEE 8th International Conference on Computing, Engineering and Design (ICCED)*, pages 1–6.

[CNN Brasil 2025] CNN Brasil (2025). Brasil foi um dos principais alvos de ataques digitais na américa latina em 2025. *CNN Brasil*, tecnologia. Dados de telemetria de ataques digitais na América Latina.

[Collins 2003] Collins, D. (2003). Pretesting survey instruments: an overview of cognitive methods. *Quality of Life Research*, 12(3):229–238.

[Datafolha 2025] Datafolha (2025). 24 milhões foram vítimas de golpe do pix ou boleto falso. *Levantamento Datafolha*. Dados reproduzidos em reportagem do G1 sobre golpes com Pix e boletos falsos.

[de Segurança Pública 2025a] de Segurança Pública, F. B. (2025a). 19º anuário brasileiro de segurança pública 2025. Relatório técnico. Dados consolidados de 2024 sobre criminalidade, incluindo fraudes e crimes digitais.

[de Segurança Pública 2025b] de Segurança Pública, F. B. (2025b). Fraudes financeiras no brasil geram perdas de cerca de r$ 10 bilhões em 2024. *Relatório de Identidade e Fraude 2025*. Dados citados em relatórios setoriais e cobertura de imprensa.

[DeMaio and Rothgeb 1996] DeMaio, T. J. and Rothgeb, J. M. (1996). Cognitive interviewing techniques: In the lab and in the field. In Schwartz, N. and Sudman, S., editors, *Answering questions: Methodology for determining cognitive and communicative processes in survey research*, pages 177–195. Jossey-Bass, San Francisco.

[Egelman and Peer 2015] Egelman, S. and Peer, E. (2015). Scaling the security wall: Developing a security behavior intentions scale (SeBIS). In *Proceedings of the 33rd Annual ACM Conf. on Human Factors in Computing Systems*, pages 2873–2882.

[Federal 2025] Federal, S. (2025). Mais de 24 milhões de pessoas foram vítimas de golpes pelo pix em um ano. *Rádio Senado*. Matéria baseada em pesquisa do DataSenado e dados do Fórum Brasileiro de Segurança Pública.

[Georgiadou et al. 2022] Georgiadou, A., Mouzakitis, S., and Askounis, D. (2022). Working from home during COVID-19 crisis: a cyber security culture assessment survey. *Security Journal*, 35:486–505.

[Gioulekas et al. 2022] Gioulekas, F., Stamatiadis, E., Tzikas, A., et al. (2022). A cybersecurity culture survey targeting healthcare critical infrastructures. *Healthcare*, 10(2).

[Hanus et al. 2018] Hanus, B., Windsor, J. C., and Wu, Y. (2018). Definition and multidimensionality of security awareness: Close encounters of the second order. *SIGMIS Database*, 49:103–133.

[Henklain et al. 2024] Henklain, M. H. O., Lobo, F. L., Feitosa, E. L., Cavalcante, L. G. D., Alencar, J. V. R. d., Bríglia, V. J. C., Araújo, G. M. d., and Alves, G. d. S. (2024). Caracterização de conhecimentos e comportamentos de cibersegurança: Estudo exploratório com dados predominantes do extremo norte brasileiro. In *Anais do XXIV Simpósio Brasileiro de Cibersegurança (SBSeg)*, pages 76–91. SBC.

[ISO 2022] ISO (2022). ISO/IEC 27001:2022 – information security, cybersecurity and privacy protection – information security management systems – requirements. International Organization for Standardization.

[Karjalainen 2011] Karjalainen, M. (2011). *Improving Employees' Information Systems (IS) Security Behaviour: Toward a Meta-Theory of IS Security Training and a New Framework for Understanding Employees' IS Security Behaviour*. PhD thesis, The University of Oulu, Finland.

[Kruger and Kearney 2006] Kruger, H. A. and Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security*, 25(4):289–296.

[Labs 2026] Labs, F. (2026). 2026 global threat landscape report. Technical report, Fortinet. Threat intelligence report on global cyber attack trends.

[Parsons et al. 2017] Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., and Zwaans, T. (2017). The human aspects of information security questionnaire (HAIS-Q): Two further validation studies. *Computers & Security*, 66:40–51.

[Parsons et al. 2013] Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., and Jerram, C. (2013). The development of the human aspects of information security questionnaire (HAIS-Q). In *Proceedings of the 24th Australasian Conference on Information Systems (ACIS)*, Melbourne, Australia.

[Pascoe et al. 2024] Pascoe, C., Quinn, S., and Scarfone, K. (2024). The nist cybersecurity framework (csf) 2.0.

[Pósa and Grossklags 2022] Pósa, T. and Grossklags, J. (2022). Work experience as a factor in cyber-security risk awareness: A survey study with university students. *Journal of Cybersecurity and Privacy*, 2(3):490–515.

[Salem et al. 2021] Salem, Y., Moreb, M., and Rabayah, K. S. (2021). Evaluation of information security awareness among palestinian learners. In *2021 International Conference on Information Technology (ICIT)*, pages 21–26.

[Senthilkumar and Easwaramoorthy 2017] Senthilkumar, K. and Easwaramoorthy, S. (2017). A survey on cyber security awareness among college students in tamil nadu. *IOP Conference Series: Materials Science and Engineering*, 263(4).

[Sobel 1982] Sobel, M. E. (1982). Asymptotic confidence intervals for indirect effects in structural equation models. *Sociological Methodology*, 13:290–312.

[Tariq et al. 2014] Tariq, M. A., Brynielsson, J., and Artman, H. (2014). The security awareness paradox: a case study. In *Proceedings of the 2014 IEEE/ACM International Conf. on Advances in Social Networks Analysis and Mining*, pages 704–711.

[Verizon 2025] Verizon (2025). 2025 data breach investigations report. Technical report, Verizon, New York, NY. Análise de mais de 12 mil violações de dados em 139 países.

[Wahyudiwan et al. 2017] Wahyudiwan, D. D. H., Sucahyo, Y. G., and Gandhi, A. (2017). Information security awareness level measurement for employee: Case study at ministry of research, technology, and higher education. In *2017 3rd International Conference on Science in Information Technology (ICSITech)*, pages 654–658.

[Wash et al. 2017] Wash, R., Rader, E., and Fennell, C. (2017). Can people self-report security accurately? agreement between self-report and behavioral measures. In *Proc. of the 2017 Conf. on Human Factors in Computing Systems*, pages 2228–2232.