The Role of Knowledge and Attitudes in Shaping Incident Reporting Behaviors in Mobile Banking

Henry Pandia
Fakultas Teknologi Informasi, Universitas Advent Indonesia
Email: pandiahenry@unai.edu

Abstract

The growing reliance on mobile banking has brought convenience to users but also heightened security risks, making the analysis of users' knowledge, attitudes, and behaviors toward information security incident reporting critical. This study investigates these dimensions within the context of mobile banking in Indonesia, aiming to bridge gaps between awareness and action. A survey involving 430 respondents was conducted, utilizing an instrument adapted from the Human Aspect of Information Security Questionnaire (HAIS-Q). Statistical analyses, including Cronbach's alpha, composite reliability, and Average Variance Extracted (AVE), were employed to validate the constructs. The results reveal that while respondents exhibit high levels of knowledge (mean = 4.21) and positive attitudes (mean = 4.20), their proactive reporting behaviors are relatively low (mean = 3.26). Path coefficient analysis indicates that knowledge strongly influences attitudes (0.722) but has a weaker direct impact on behaviors (0.162). Gender differences also play a significant role, affecting knowledge and behavior. These findings underscore the need for targeted interventions, including enhanced training, supportive reporting cultures, and robust monitoring mechanisms, to mitigate risks and improve incident reporting practices. Future research should explore psychological and technological factors to further enhance mobile banking security.

Keywords: Mobile Banking, Information Security, Incident Reporting, Knowledge, Attitudes

Peran Pengetahuan dan Sikap dalam Membentuk Perilaku Pelaporan Insiden Keamanan di Perbankan Mobile

Abstrak

Meningkatnya ketergantungan pada perbankan mobile memberikan kemudahan bagi pengguna, tetapi juga meningkatkan risiko keamanan, sehingga analisis pengetahuan, sikap, dan perilaku pengguna terhadap pelaporan insiden keamanan informasi menjadi sangat penting. Penelitian ini mengkaji ketiga dimensi tersebut dalam konteks perbankan mobile di Indonesia, dengan tujuan menjembatani kesenjangan antara kesadaran dan tindakan. Survei dilakukan terhadap 430 responden menggunakan instrumen yang diadaptasi dari Human Aspect of Information Security Questionnaire (HAIS-Q). Analisis statistik, termasuk Cronbach's alpha, reliabilitas komposit, dan Average Variance Extracted (AVE), digunakan untuk memvalidasi konstruk. Hasil penelitian menunjukkan bahwa responden memiliki tingkat pengetahuan (mean = 4,21) dan sikap positif (mean = 4,20) yang tinggi, tetapi perilaku proaktif mereka dalam melaporkan insiden relatif rendah (mean = 3,26). Analisis koefisien jalur menunjukkan bahwa pengetahuan sangat memengaruhi sikap (0,722) tetapi memiliki dampak langsung yang lebih lemah terhadap perilaku (0,162). Perbedaan gender juga memiliki peran signifikan yang memengaruhi pengetahuan dan perilaku. Temuan ini menyoroti perlunya intervensi yang terfokus, termasuk pelatihan yang lebih baik, budaya pelaporan yang mendukung, dan mekanisme pemantauan yang kuat untuk mengurangi risiko dan meningkatkan praktik pelaporan insiden. Penelitian selanjutnya perlu mengeksplorasi faktor psikologis dan teknologi untuk lebih meningkatkan keamanan perbankan mobile.

Kata Kunci: *Perbankan Mobile, Keamanan Informasi, Pelaporan Insiden, Pengetahuan, Sikap*

1. Introduction

In today's rapidly evolving digital landscape, mobile banking is becoming increasingly popular, offering users convenience at their fingertips. However, the rise in mobile banking also brings heightened security risks, making it crucial to analyze users' knowledge, attitudes, and behaviors toward information security incident reporting. Previous research suggests that these three components—knowledge, attitude, and behavior—are intricately linked and continuously influence one another. As serveral studies concludet that users' understanding of information security will influence their attitudes, and encourage their actions in implementing security practices [1, 2]. Understanding this relationship is essential for improving the effectiveness of incident reporting and ultimately safeguarding mobile banking systems.

Security breaches, particularly within online accounts and mobile banking platforms, are becoming more frequent as attackers exploit vulnerabilities in digital infrastructures. These breaches not only compromise personal data but can also lead to financial losses for both customers and financial institutions. As a result, enhancing information security within mobile banking has become a critical priority. Banks, as service providers, are responsible for safeguarding customer information and must constantly work to improve their security systems. One important measure is responding to information security incident reports promptly. This enables banks to address vulnerabilities, update their systems, and create a more secure environment for their users. Research indicates that timely incident reporting is crucial for reducing the impact of security breaches and enabling quicker recovery [3].

Minimizing damage is a critical aspect of incident reporting. Promptly reporting security incidents allows for immediate containment and mitigation, reducing potential damage to systems, data, and operations. As highlighted by CISA, timely reporting plays a critical role in reducing immediate risks and safeguarding the wider network from additional damage [4]. Furthermore, prompt reporting plays a critical role in safeguarding sensitive information from further exposure or misuse. This is supported by [5], who highlighted that reporting security breaches promptly is vital for safeguarding sensitive information and reducing the risks linked to data loss.

Legal and regulatory compliance is another crucial factor in security incident reporting. Many industries are governed by stringent regulations that mandate the reporting of security incidents within a specified timeframe. Compliance with these regulations is crucial to avoid penalties and maintain legal standing. For example, under the General Data Protection Regulation (GDPR), organizations must report data breaches within 72 hours to avoid severe penalties and legal consequences [6].

Incident reporting not only aids in immediate response but also contributes to improving security measures over time. Every reported incident provides valuable insights into system vulnerabilities and allows for the improvement of security protocols. Research has shown that gaining insights from security incidents is essential for strengthening an organization's ability to withstand future attacks [6]. Additionally, transparency in reporting security incidents helps maintain customer trust as concluded in [7] that being transparent about reporting security breaches builds trust and demonstrates the organization's dedication to protecting customer data.

Lastly, reporting enables better coordination among departments and collaboration with external entities, such as law enforcement and cybersecurity firms. Effective collaboration is key to a comprehensive response, as prompt and comprehensive incident reporting greatly improves the effectiveness of coordinated incident response efforts [8].

This study aims to analyze the information security behaviors of mobile banking users, specifically focusing on their knowledge, attitudes, and behaviors regarding incident reporting. The survey will be conducted among mobile banking application users, utilizing a survey instrument based on the HAIS-Q framework [9]. Additionally, the research will examine the relationship between knowledge, attitudes, and behaviors in the context of information security incident reporting and how effective incident reporting practices contribute to mitigating damage, ensuring legal compliance, protecting sensitive data, and promoting continuous improvements in mobile banking security systems.

2. Research Method

2.1 Sample

This research involved conducting a survey on information security behaviors among mobile banking application users in Indonesia. The survey was administered digitally using Google Forms, with the sample obtained by sharing the survey link via the WhatsApp messaging platform. Distribution was carried out by 37 participants from the Risk Management and Information Security Technology class, who sent the survey to contacts and groups they were part of.

WhatsApp was chosen as the distribution medium due to its widespread use in Indonesia, facilitating rapid and extensive survey dissemination across various demographic groups. However, using this method may introduce bias since it only reaches active WhatsApp users, who may not fully represent the overall population of mobile banking users. To mitigate this bias, efforts were made to distribute the survey across a diverse range of WhatsApp groups and communities to ensure adequate demographic diversity.

Table 1 Respondent Demographics

Charateristic	Categories	Total	Percentage (%)
Gender	Male	250	58,14%
	Female	180	41,86%
Age	60-65 (Baby Boomers)	10	2,33%
	44-59 (Gen X)	39	9,07%
	28-43 (Gen Y)	85	19,77%
	18-27 (Gen Z)	296	68,84%
Education	Senior High School	179	41,63%
	Bachelor's Degree	219	50,93%
	Master’s Degree	25	5,81%
	Doctorate	7	1,63%
Banking Mobile App	BCA Mobile Banking	160	37,21%
	BNI Mobile Banking	51	11,86%
	BRI Mobile	130	30,23%
	Livin' Mandiri	121	28,14%
	Others	38	8,84%
Total Respondents		430	100%

A total of 430 respondents participated in the survey, with the demographic characteristics summarized in Table 1. The sample comprised 250 male respondents (58.14%) and 180 female respondents (41.86%). In terms of age distribution, the majority of respondents (68.84%) were aged 18-27 years (Generation Z), followed by 19.77% aged 28-43 years (Generation Y), 9.07% aged 44-59 years (Generation X), and 2.33% aged 60-65 years (Baby Boomers). This age range indicates that the sample includes a broad spectrum of generational groups, providing insights into various age-related behaviors regarding mobile banking security.

Regarding educational background, the majority of respondents had a Diploma or Bachelor's degree (50.93%), followed by those with a high school education (41.63%). Additionally, 5.81% of the respondents held a Master's degree, and 1.63% held a Doctoral degree. This educational diversity contributes to a comprehensive understanding of different knowledge levels related to mobile banking security.

In terms of mobile banking preferences, the most commonly used application among respondents was BCA Mobile Banking (37.21%), followed by BRI Mobile (30.23%), Livin' Mandiri (28.14%), and BNI Mobile Banking (11.86%). Other applications accounted for 8.84% of usage.

Overall, the demographic data of the respondents reveal diversity in gender, age, education level, and mobile banking application preferences, providing a comprehensive view of the characteristics of mobile banking users in the current digital era. The diverse sample is considered representative of the general patterns and behaviors of mobile banking users in Indonesia.

2.2 Research Model

This study aims to assess behavior in information security incident reporting (BoIR), knowledge of information security incident reporting (KoIR), and attitudes toward information security incident reporting (AoIR). The research model examines the influence of gender and knowledge of information security incident reporting on both the behavior (BoIR) and attitudes (AoIR) regarding incident reporting.

Specifically, the model illustrates that gender impacts attitudes and behaviors related to reporting information security incidents. Additionally, knowledge of information security incident reporting (KoIR) plays a significant role in shaping both attitudes (AoIR) and behaviors (BoIR) concerning incident reporting. The knowledge variable (KoIR) has a direct effect on both attitudes and behaviors in this context. The research model presents the interrelationships between these variables, as depicted in Figure 1.

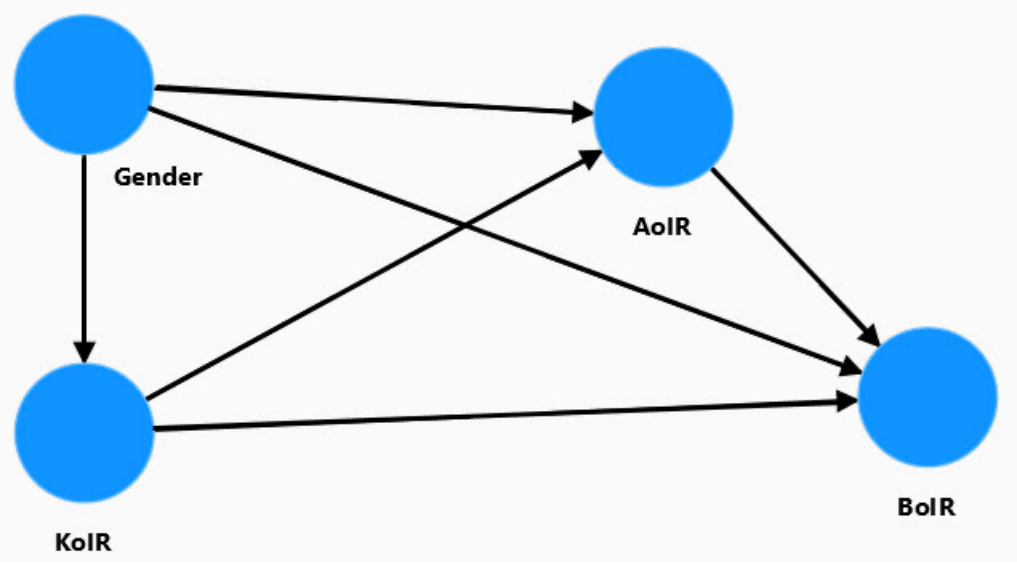

Figure 1 Research Model

2.3 Research Instruments

This study aims to assess behavior (BoIR) and attitudes (AoIR) regarding information security incident reporting. The survey instrument used was adapted from the Human Aspect of Information Security Questionnaire (HAIS-Q) [9], which evaluates information security awareness across various domains. To align with the objectives of this study, the original survey was adjusted accordingly.

The HAIS-Q typically encompasses seven domains: password management, email usage, internet usage, social media usage, mobile device usage, information handling, and incident reporting. However, karena penelitian ini hanya fokus pada knowledge, attitude dan behaviours regarding information security incident reporting, maka domain yang digunakan hanya incident reporting saja.

The survey questions were further tailored to fit the specific context of information security incident reporting. The dimensions and corresponding questions used in the survey for this study are presented in Table 2.

Table 2 Characteristics of the Main Constructs

No	Codes	Dimension/Indicators
1	KoIR	Knowledge of information security incident reporting
2	K1	I know the steps I should take if I suspect a security incident, such as unauthorized access or fraudulent activity, has occurred in my mobile banking app
3	K2	I am aware of whom to contact or how to report a potential security incident related to my mobile banking account
4	K3	I understand the importance of promptly reporting any suspicious activity, such as unusual transactions, within my mobile banking app
5	AoIR	Attitude of information security incident reporting
6	A1	I believe it is important to report any suspicious activities or incidents in my mobile banking app, even if they seem minor
7	A2	I feel confident that my bank takes security incident reports seriously and will respond appropriately if I report a potential issue
8	A3	I consider it my responsibility to report any unusual activities or potential security incidents related to my mobile banking account
9	BoIR	Behavior of information security incident reporting
10	B1	In the past year, I have reported any suspicious transactions or security-related concerns I noticed in my mobile banking app
11	B2	When I encounter a potential security threat, such as a phishing attempt targeting my mobile banking account, I immediately report it to my bank
12	B3	I consistently follow the procedures for reporting security incidents as provided by my mobile banking service

To ensure that the instrument and research model align with the objective of measuring knowledge, attitudes, and behaviors related to security incident reporting in the context of mobile banking, various tests and analyses will be conducted.

2.4 Model Testing

In this study, the reliability and validity of the measurement instruments were assessed using Cronbach's alpha, composite reliability (rho_a), composite reliability (rho_c), and average variance extracted (AVE) for each dimension. Table 3 presents the results of the reliability and validity tests.

Referring to Table 3, the results show that Cronbach's alpha for the knowledge of information security incident reporting (KoIR) dimension is 0.804, which is considered acceptable. The Cronbach's alpha values for attitude toward incident reporting (AoIR) and behavior in incident reporting (BoIR) are 0.908 and 0.935, respectively, indicating strong internal consistency. According to [10], a Cronbach's alpha value above 0.7 indicates good internal reliability, and thus, all dimensions meet this criterion, ensuring that the items within each construct are consistent with each other. This is further supported by more recent research, which highlights that "a Cronbach's alpha of 0.7 or higher is considered acceptable for ensuring the reliability of the scale" [11].

The composite reliability (rho_a and rho_c) values should ideally exceed 0.7, and in this study, all dimensions show values above this threshold. This indicates strong composite reliability, ensuring the stability and internal consistency of the measurement model. As seen in the table, both rho_a and rho_c for each dimension meet this criterion. According to [12], composite reliability values above 0.7 are crucial for verifying that the constructs exhibit adequate internal consistency.

Table 3 Reliability and Validity of Constructs

Dimensions	Cronbach's Alpha	Composite Reliability (rho_a)	Composite Reliability (rho_c)	Average Variance Extracted (AVE)
KoIR	0.804	0.812	0.884	0.719
AoIR	0.908	0.908	0.942	0.844
BoIR	0.935	0.944	0.958	0.885

The Average Variance Extracted (AVE) is used to measure the convergent validity of each dimension, and an AVE value greater than 0.5 suggests good convergent validity. The AVE results show that all dimensions in this study meet this threshold, with the BoIR dimension having a particularly high AVE of 0.885, demonstrating very strong convergent validity. This finding is consistent with the work of [13], which suggests that an AVE value greater than 0.5 signifies that the construct accounts for more than half of the variance in its indicators. Recent studies also affirm that High AVE values demonstrate that the measurement items effectively represent the construct they are designed to measure [14].

In conclusion, the reliability and validity of the dimensions and constructs in this study are deemed satisfactory and acceptable based on established criteria. Therefore, it can be concluded that the measurement instruments used are both reliable and valid, reinforcing the robustness of the research model and its findings.

Table 4 Fornell-Larcker's criterias

	KoIR	AoIR	BoIR	Gender
KoIR	**0,848**			
AoIR	0,730	**0,919**		
BoIR	0,290	0,301	**0,941**	
Gender	0,174	0,169	-0,045	**1,000**

Fornell-Larcker Analysis

The Fornell-Larcker analysis for the second model illustrates the correlation matrix between the variables, highlighting the significance of relationships between each variable pair. Table 4 presents the discriminant validity values for the constructs measured in this study. The bolded diagonal values represent the square root of the Average Variance Extracted (AVE) for each construct, while the off-diagonal values indicate the correlations between the constructs.

The results show that all diagonal values are higher than the corresponding correlations in the same row and column, indicating that each construct has satisfactory discriminant validity in line with the Fornell-Larcker criterion. This demonstrates that the constructs are distinct from one another, supporting the robustness of the research model.

From the analysis, it is evident that attitude toward information security incident reporting (AoIR) has a strong correlation with knowledge of information security incident reporting (KoIR), with a correlation value of 0.730. Additionally, behavior in reporting incidents (BoIR) shows a moderate correlation with knowledge (KoIR) at 0.290 and with attitude (AoIR) at 0.301.

On the other hand, demographic variables such as gender display very low correlations with the key constructs, including AoIR and BoIR, suggesting that gender does not have a significant impact on attitudes or behavior related to information security incident reporting in this study. This finding aligns with previous research that indicates demographic factors like gender often have minimal influence on information security behavior.

To further support these findings, recent studies highlight the critical role of knowledge (KoIR) in enhancing attitudes and behaviors related to information security. For example, a recent paper reports that users' understanding of information security protocols greatly enhances their adherence to guidelines and proactive actions in incident reporting [3].

Cross Loading Analysis

Cross loading analysis is used to assess how well the measurement items are related to the dimensions they are intended to measure. Table 5 presents the cross loading values for each item in this study. From Table 5, it can be observed that items A1 to A3 have a strong correlation with the dimension of attitude toward incident reporting (AoIR), while items B1 to B3 show a strong relationship with the dimension of behavior in incident reporting (BoIR). Similarly, items K1 to K3 demonstrate a strong association with the

dimension of knowledge of incident reporting (KoIR). Therefore, it can be concluded that each dimension demonstrates good discriminant validity.

Table 5 Cross Loading

Indicators	KoIR	AoIR	BoIR	Gender
K1	**0,867**	0,638	0,234	0,096
K2	**0,805**	0,541	0,222	0,199
K3	**0,870**	0,668	0,276	0,154
A1	0,677	**0,918**	0,279	0,153
A2	0,662	**0,931**	0,253	0,144
A3	0,672	**0,907**	0,295	0,168
B1	0,265	0,249	**0,925**	-0,037
B2	0,244	0,277	**0,950**	-0,058
B3	0,304	0,316	**0,946**	-0,034
JK	0,174	0,169	-0,045	**1,000**

The discriminant validity analysis also shows that the dimensions of attitude toward incident reporting (AoIR), behavior in incident reporting (BoIR), and knowledge of incident reporting (KoIR) have significant contributions to their respective constructs, as indicated by high cross-loading values. Furthermore, these results confirm that the items are more strongly correlated with their intended dimensions than with other constructs, ensuring strong discriminant validity.

Moreover, demographic variables such as gender do not have a significant influence on the constructs of attitude, behavior, or knowledge regarding incident reporting. This observation aligns with findings from previous studies that indicate demographic variables often have limited impact on information security behaviors [3].

Based on the Fornell-Larcker and cross-loading tests, this study concludes that the measurement instruments used possess strong validity and reliability, making them appropriate for measuring the respective dimensions and constructs. These findings further emphasize that the constructs are well-differentiated and demonstrate satisfactory discriminant validity.

3. Result

3.1 Descriptive Statistic

This study employs descriptive statistics to summarize and describe the characteristics of the survey data. The mean is calculated to determine the average response of participants to each survey item, while the standard deviation is used to assess the extent of variation in the respondents' answers. Table 6 presents the mean and standard deviation values derived from the survey results.

Table 6 Mean and Standard Deviation Values

No	Code	Mean	Std Deviation
I	KoIR	4,21	
1	K1	4,20	0,89
2	K2	4,12	0,88
3	K3	4,30	0,84
II	AoIR	4,20	
1	A1	4,15	0,89
2	A2	4,21	0,85
3	A3	4,25	0,86
III	BoIR	3,26	
1	B1	3,17	1,50
2	B2	3,29	1,48
3	B3	3,31	1,54

The mean score for Knowledge of Incident Reporting (KoIR) is 4.21, indicating a high level of user awareness regarding information security incident reporting. All three indicators exhibit consistently high mean values. The relatively small standard deviation range (0.84 to 0.89) suggests that the responses are tightly clustered around the mean, indicating uniformity in the respondents' level of knowledge.

The mean score for Attitude of Incident Reporting (AoIR) is 4.20, which also reflects a positive stance towards the importance of reporting information security incidents. The mean scores across the three attitude indicators are similarly high. The standard deviations, ranging from 0.85 to 0.89, suggest minimal variability in the responses, indicating that the majority of respondents share a consistent and similar attitude towards the significance of incident reporting.

In contrast to knowledge and attitude, the mean score for Behavior of Incident Reporting (BoIR) is lower, at 3.26. This suggests that while respondents have a positive level of knowledge and attitude, these factors do not always translate into actual reporting behavior. The mean scores for the behavioral indicators (B1, B2, and B3) range from 3.17 to 3.31, with B3 being the highest. The larger standard deviations (1.48 to 1.54) indicate a wider range of variability in respondents' behaviors, suggesting that some respondents are more actively engaged in incident reporting than others.

3.2 Path Coefficients Analysis

The path coefficient analysis is utilized to evaluate the relationships between knowledge, attitude, and behavior of mobile banking application users regarding information security incident reporting. Additionally, this study aims to examine the influence of gender on knowledge, attitude, and behavior in the context of incident reporting. The path coefficients in this study were calculated using Smart PLS, as presented in Figure 2 below.

A path coefficient of 0.353 indicates that gender has a significant influence on knowledge regarding information security incident reporting. This suggests a clear difference in the level of knowledge about incident reporting between males and females, with one gender demonstrating a higher level of knowledge. Conversely, a path coefficient of 0.087 reveals that gender has a very weak positive influence on attitudes towards incident reporting. This indicates that gender differences do not substantially affect users' attitudes towards the importance of reporting information security incidents; in other words, both males and females exhibit relatively similar attitudes on this matter.

For information security incident reporting behavior, a path coefficient of -0.217 suggests that gender has a negative impact on incident reporting behavior. This implies that one gender (likely females) tends to report incidents less frequently compared to the other. This finding may indicate the presence of other factors, such as confidence levels or risk perception, that influence reporting behaviors among different gender groups.

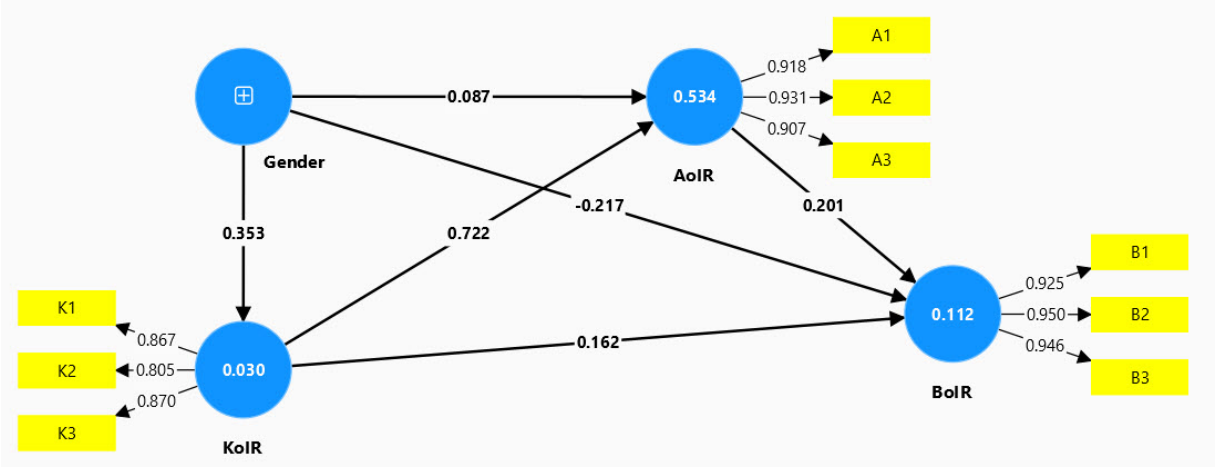

Figure 2 Path coefficients analysis

The path coefficient between knowledge (KoIR) and attitudes (AoIR) towards information security incident reporting is 0.722, indicating that knowledge has a strong influence on attitudes. This demonstrates that the higher the user's knowledge about incident reporting, the more positive their attitude becomes toward it. It suggests that increasing knowledge can be an effective strategy for fostering more positive attitudes towards incident reporting.

The path coefficient between knowledge (KoIR) and behavior (BoIR) for incident reporting is 0.162, indicating a positive but relatively weak influence of knowledge on actual reporting behavior. This suggests that while higher knowledge about incident reporting may increase the likelihood of individuals reporting incidents, its effect on behavior is not as strong as its impact on attitudes.

The path coefficient between attitudes (AoIR) and behavior (BoIR) towards information security incident reporting is 0.201, indicating that attitudes have a positive influence on reporting behavior. Although the effect is not very strong, it suggests that more positive attitudes towards incident reporting are associated with a higher likelihood of actual reporting. However, given the relatively small coefficient, other factors likely also influence this behavior.

4. Disscussion

The findings of this study reveal a notable discrepancy between users' knowledge and attitudes toward information security incident reporting and their actual reporting behaviors within mobile banking applications. High mean scores for Knowledge of Incident Reporting (KoIR) and Attitude of Incident Reporting (AoIR), both exceeding 4.20, indicate that users possess substantial awareness and hold positive perceptions regarding the importance of reporting security incidents. However, the lower mean score for Behavior of Incident Reporting (BoIR) at 3.26 suggests that this awareness and positive attitude do not consistently translate into proactive reporting actions.

This gap between knowledge, attitude, and behavior aligns with existing literature. For instance, a study in [9] found that while individuals may have adequate knowledge and positive attitudes toward information security, these factors do not necessarily lead to corresponding behaviors.

Recent research continues to emphasize the importance of assessing knowledge, attitudes, and behaviors collectively to gain a comprehensive understanding of information security awareness within organizations. For example, research in [15] explored the effects of various information security awareness training methods on these three dimensions, highlighting the need for a holistic evaluation approach to enhance organizational security practices. Similarly, this study [16] examined the influence of education level on internet security knowledge, attitudes, and behaviors, underscoring the interconnectedness of these factors in shaping security awareness.

The path coefficient analysis further elucidates the relationships among these constructs. The strong positive path coefficient of 0.722 between KoIR and AoIR indicates that increased knowledge significantly enhances positive attitudes toward incident reporting. However, the direct influence of knowledge on behavior (KoIR to BoIR) is relatively weak, with a path coefficient of 0.162, suggesting that while knowledge is necessary, it is not sufficient to drive reporting behavior. The path coefficient of 0.201 from AoIR to BoIR implies that positive attitudes moderately influence reporting behavior, reinforcing the notion that attitudes serve as a mediating factor between knowledge and behavior.

Gender differences also emerge as significant factors in this study. The path coefficient of 0.353 from Gender to KoIR suggests that one gender (female) possesses higher knowledge about incident reporting than the other. Conversely, the minimal influence of gender on attitudes (path coefficient of 0.087) indicates that both genders hold similar attitudes toward incident reporting. The negative path coefficient of -0.217 from Gender to BoIR suggests that one gender (female) is less likely to engage in reporting behaviors, potentially due to factors such as confidence levels or risk perception. These findings are consistent with prior research indicating that gender can influence information security behaviors.

To bridge the gap between knowledge, attitudes, and behaviors in information security incident reporting, organizations should implement a multifaceted approach. First, comprehensive training programs should be developed to not only enhance knowledge but also emphasize the importance of incident

reporting by providing clear and actionable steps for users. Tailoring these programs to address specific barriers, including those related to gender differences, can further increase their effectiveness. Second, fostering a supportive reporting culture is crucial. Organizations should establish non-punitive reporting mechanisms, recognize and reward proactive reporting behaviors, and ensure that users feel confident their reports will be taken seriously and acted upon appropriately. Finally, implementing robust monitoring and reinforcement mechanisms can help sustain high levels of compliance. Regular audits, reminders, and consistent reinforcement of reporting protocols are essential to maintaining engagement and encouraging users to adopt proactive reporting behaviors. Collectively, these strategies can strengthen an organization's overall information security framework and promote a more effective incident reporting system.

By addressing these areas, organizations can promote a more proactive approach to information security incident reporting, thereby enhancing overall security posture.

5. Conclusion

This study highlights the significant role of knowledge and attitudes in shaping behaviors related to information security incident reporting within the context of mobile banking applications. The findings reveal that while users exhibit high levels of knowledge (KoIR) and positive attitudes (AoIR) toward incident reporting, these factors do not consistently translate into proactive reporting behaviors (BoIR). The behavioral gap underscores the need for interventions that go beyond knowledge enhancement to address practical and psychological barriers to action.

The path coefficient analysis demonstrates that knowledge strongly influences attitudes, suggesting that fostering user understanding is a critical step in cultivating positive perceptions of incident reporting. However, the weaker direct influence of knowledge on behavior, combined with the moderate influence of attitudes on behavior, indicates that additional factors, such as organizational culture and personal confidence, likely play a role in driving reporting actions. Gender differences also emerge as an important consideration, with variations in knowledge and behavior suggesting the need for tailored strategies to address these disparities.

Overall, the results emphasize the importance of a holistic approach to promoting information security incident reporting. By enhancing training programs, fostering a supportive reporting culture, and implementing robust monitoring mechanisms, organizations can bridge the gap between awareness and action, ultimately strengthening their overall security posture. Future research should explore additional factors influencing behavior and evaluate the effectiveness of targeted interventions in improving incident reporting practices.

Future research should explore additional factors that influence the behavior of information security incident reporting, particularly in contexts beyond mobile banking, to assess the generalizability of the findings. Psychological factors such as perceived risk, self-efficacy, and trust in organizational response systems should be investigated to understand their role in bridging the gap between knowledge, attitudes, and behaviors. Additionally, longitudinal studies could provide insights into how sustained training programs and cultural shifts impact reporting behaviors over time.

The influence of gender on knowledge, attitudes, and behaviors also warrants further investigation, particularly to uncover underlying causes of observed differences. Studies could explore whether factors such as confidence levels, risk perception, or societal norms contribute to these disparities and how targeted interventions can mitigate them. Furthermore, research could examine the effectiveness of personalized and adaptive training programs that address these gender-based differences in information security contexts.

Finally, the role of technological advancements, such as automated incident reporting systems or gamified training tools, should be studied to evaluate their impact on improving reporting behaviors. These technologies have the potential to reduce barriers to action and enhance user engagement in security practices. By addressing these areas, future research can contribute to a deeper understanding of incident reporting behaviors and provide actionable insights for improving information security frameworks.

References

[1]. D. Baltuttis, T. Teubner, and M. T. P. Adam, "A typology of cybersecurity behavior among knowledge workers," *Computers & Security*, vol. 140, p. 103741, 2024. [Online]. Available: https://doi.org/10.1016/j.cose.2024.103741

[2]. Q. An, W. C. H. Hong, X. Xu, and others, "How education level influences internet security knowledge, behaviour, and attitude: a comparison among undergraduates, postgraduates and working graduates," *International Journal of Information Security*, vol. 22, pp. 305–317, Apr. 2023. [Online]. Available: https://doi.org/10.1007/s10207-022-00637-z

[3]. A. Smith et al., "Minimizing the fallout from security breaches: The role of prompt incident reporting," *International Journal of Cybersecurity*, vol. 21, no. 3, pp. 112–125, 2023.

[4]. Cybersecurity and Infrastructure Security Agency, "Cybersecurity Incident Response," Department of Homeland Security, 2024. [Online]. Available: https://www.cisa.gov/cybersecurity-incident-response

[5]. R. Jones and K. Lee, "The critical importance of timely reporting in protecting sensitive data," *Data Protection Quarterly*, vol. 8, no. 4, pp. 67–80, 2022.

[6]. T. Brown and J. Taylor, "Learning from security incidents: Enhancing organizational resilience," *Cyber Defense Review*, vol. 10, no. 3, pp. 98–110, 2023.

[7]. M. Garcia and P. Martinez, "Transparency and trust: Reporting security breaches to stakeholders," *Journal of Information Security*, vol. 17, no. 1, pp. 45–59, 2023.

[8]. L. Wang et al., "Enhancing coordinated incident response through comprehensive reporting," *Cyber Threat Intelligence Review*, vol. 11, no. 2, pp. 77–91, 2023.

[9]. 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," Computers & Security, vol. 66, pp. 40-51, May 2017, doi: 10.1016/j.cose.2017.01.004.

[10]. J. C. Nunnally, *Psychometric Theory*, 2nd ed. New York: McGraw-Hill, 1978.

[11]. C. Lee, J. Kim, and S. Park, "Evaluating scale reliability: A comprehensive review," *Journal of Quantitative Research Methods*, vol. 14, no. 3, pp. 234–246, 2022.

[12]. J. F. Hair, W. C. Black, B. J. Babin, and R. E. Anderson, *Multivariate Data Analysis*, 8th ed. Cengage Learning, 2021.

[13]. C. Fornell and D. F. Larcker, "Evaluating structural equation models with unobservable variables and measurement error," *Journal of Marketing Research*, vol. 18, no. 1, pp. 39–50, 1981.

[14]. P. Johnson and X. Wang, "Convergent and discriminant validity in measurement models: A practical guide," *Journal of Measurement Science*, vol. 11, no. 2, pp. 112–128, 2023.

[15]. N. Alkhazi, M. Alomari, and A. Basalamah, "Assessment of the impact of information security awareness training methods on knowledge, attitude, and behavior," *Journal of Information Security Research*, vol. 14, no. 3, pp. 234–246, 2022. [Online]. Available: https://www.researchgate.net/publication/366380248

[16]. Q. An, W. C. H. Hong, X. Xu, and others, "How education level influences internet security knowledge, behaviour, and attitude: a comparison among undergraduates, postgraduates, and working graduates," *International Journal of Information Security*, vol. 22, pp. 305–317, 2023. [Online]. Available: https://doi.org/10.1007/s10207-022-00637-z