el-Qist
Journal of Islamic Economics and Business (JIEB)
P-ISSN : 2252-7907 I E-ISSN : 2716-0335

El-Qist: Journal of Islamic Economics and Business
Vol. 15 No. 2 (October 2025), 127-153
P-ISSN 2252-7907 | E-ISSN 2716-0335
DOI : /10.15642/ elqist.2025.15.2.127-153

Cybersecurity Behavior as a Reflection of *Ḥifẓ al-Māl* in Islamic Banking: A Behavioral Model Based on Protection Motivation Theory

Muhammad Wandisyah R. Hutagalung
UIN Syekh Ali Hasan Ahmad Addary Padangsidimpuan
Email: wandisyah@uinsyahada.ac.id

Saparuddin Siregar
UIN Sumatera Utara Medan
Email: saparuddin.siregar@uinsu.ac.id

Mhd Furqan
UIN Sumatera Utara Medan
Email: mfurqan@uinsu.ac.id

Ismail Pulungan
UIN Sunan Kalijaga Yogyakarta
Email: maellpalevi@gmail.com

Furkan Elce
Istanbul University
Email: furkan.elce@gmail.com

Corresponding Author: Muhammad Wandisyah R. Hutagalung
Article History: Received July 22, 2025; Received in revised fromSeptember 30, 2025: Accepted September 29, 2025; Published; October 31, 2025
How to Cite this Article: Hutagalung, Muhammad Wandisyah R, Saparuddin Siregar, Mhd. Furqan, Ismail Pulungan, and Furkan Elce. 2025. "Cybersecurity Behavior as a Reflection of Ḥifẓ al-māl in Islamic Banking: A Behavioral Model Based on Protection Motivation Theory". *El-Qist: Journal of Islamic Economics and Business (JIEB)* 15 (2). Surabaya, Indonesia:127-45. https://doi.org/10.15642/elqist.2025.15.2.127-153.

Abstract: This study examines psychological determinants of cybersecurity protection behavior among Islamic banking customers by applying Protection Motivation Theory (PMT) within a *maqāṣid al-sharīʿah* framework. Using a quantitative survey (N = 384) and PLS-SEM, it tests the effects of perceived vulnerability, severity, self-efficacy, response efficacy, response cost, and social influence, as well as the moderating role of cybersecurity education. Results show that vulnerability, severity, response efficacy, and social influence significantly predict protection behavior, while self-efficacy and response cost do not. Cybersecurity education has no significant moderating effect. The model explains 69.6% of the variance, indicating strong explanatory power. The study contributes by linking PMT to Islamic economic principles, particularly *ḥifẓ al-māl* and *amānah*. It suggests that Islamic banks need community-based, values-driven cybersecurity education to foster sustainable protective behavior.

Keywords: Cybersecurity, Islamic Banking, Protection Motivation Theory, Protection Behavior, *ḥifẓ al-māl*, Cybersecurity Education.

Introduction

The development of digital technology has revolutionized the financial industry landscape, including the Islamic banking sector. The digitalization of services such as mobile banking and internet banking has expanded financial access for the public and significantly promoted Islamic financial inclusion, particularly in Indonesia. However, this digital transformation has also introduced new risks in the form of increasing cybersecurity threats, such as phishing, identity theft, and account takeover. The 2023 report from the National Cyber and Crypto Agency (BSSN) recorded a 43% increase in cyberattacks targeting mobile banking users in Indonesia, including those using Islamic banks, indicating a high level of vulnerability to digital threats—especially due to users' low cybersecurity awareness.

From the perspective of *maqāṣid al-sharīʿah*, digital security holds important moral and spiritual dimensions. The protection of wealth (*ḥifẓ al-māl*) is not only related to economic interests but also forms part of the ethical responsibility within the Islamic financial system. Islamic banks are not merely tasked with providing financial services; they also bear the trust (*amānah*) to safeguard the public good (*maṣlaḥah*). Masruchin's findings suggest that Islamic e-banking transactions have the potential to enhance *maqāṣid* by offering convenience, security, and access to Sharia-compliant financial services.[1]

In the *maqāṣid al-sharīʿah* framework, every objective arises to prevent a potential violation. With respect to ḥifẓ al-māl (protection of wealth), the violations include unlawful appropriation of property (*ghaṣb*), fraud and deception (*iḥtiyāl/ghurūr*), transgression of rights (*iʿtidaʾ*), and negligence that causes waste of wealth (*taḍyīʿ al-māl*).[2] In Islamic digital banking, such violations manifest as cybercrimes, including hacking, phishing, identity theft, and user negligence in protecting credentials. Thus, cybersecurity protection behavior is not merely a technical precaution but an ethical and religious obligation to actualize ḥifẓ al-māl.

Recent studies in the Middle East and South Asia further highlight the importance of linking cybersecurity to *maqāṣid al-sharīʿah*. For example, research in Jordan and Saudi Arabia emphasizes that protecting customer assets in mobile banking is both a technical necessity and a moral duty[3], yet most of these works focus more on usability and risk perception than on *maqāṣid* integration. Similarly, studies in Saudi Arabia and Malaysia underline that awareness of cybersecurity among Muslim users remains moderate, with gaps in connecting protective behavior to the ethical obligations of *ḥifẓ al-māl* and *amānah*.[4] Compared to those contexts, this study

[1] Masruchin Masruchin et al., "Enhancing Maqasid Syariah through E-Banking: A Qualitative Analysis of Syariah-Compliant Financial Transactions," *Indonesian Journal of Law and Economics Review* 18, no. 3 (2023): 6–14, https://doi.org/10.21070/ijler.v18i3.934.

[2] Imam Al-Ghazali, *Al-Mustashfa Jilid 2: Rujukan Utama Ushul Fikih*, vol. 2 (Pustaka Al-Kautsar, 2022).

[3] Habib Ullah Khan et al., "Utilizing Bio Metric System for Enhancing Cyber Security in Banking Sector: A Systematic Analysis," IEEE Access 11 (2023): 80181–98, https://doi.org/10.1109/ACCESS.2023.3298824.

[4] Amar Johri and Shailendra Kumar, "Exploring Customer Awareness towards Their Cyber Security in the Kingdom of Saudi Arabia: A Study in the Era of Banking Digital Transformation," Human Behavior and Emerging Technologies 2023 (2023), https://doi.org/10.1155/2023/2103442.

contributes a distinctive perspective by examining cybersecurity behavior in Indonesia—where digital Islamic banking adoption is rapidly expanding—while explicitly integrating Protection Motivation Theory (PMT) with *maqāṣid al-sharīʿah* to bridge technical, ethical, and spiritual dimensions.

PMT itself, first developed by Rogers and refined by Maddux and Rogers, explains how individuals are motivated to adopt protective behavior through two core mechanisms: threat appraisal (perceived vulnerability and perceived severity) and coping appraisal (response efficacy, self-efficacy, and response cost).[5] Empirical studies confirm that perceived vulnerability and severity positively drive protective intentions, while response efficacy and self-efficacy enhance adoption, and response cost hinders it.[6] In addition, recent studies extend PMT by incorporating social influence, wherein junctive and descriptive norms shape security behavior in organizational and banking contexts.[7]

From an Islamic perspective, PMT remains underexplored in relation to the *maqāṣid al-sharīʿah* framework.[8] Research has begun to connect cybersecurity to *ḥifẓ al-māl* and *amānah*[9] yet most discussions remain descriptive and normative. A critical extension would be to conceptualize *amānah* (trust) and *al-nuṣrah* (mutual support) not only as ethical implications but also as potential constructs or mediating variables. *Amānah* could mediate the relationship between coping appraisal and protective behavior, as trust reinforces confidence in one's ability to act. *Al-nuṣrah*, on the other hand, reflects communal responsibility, potentially mediating the effect of social influence on intention by framing cybersecurity as a collective duty (*farḍ kifāyah*). Such integration would extend PMT through an Islamic lens, framing protective behavior in digital banking as both a rational-cognitive and ethical-spiritual duty.

Based on the above, this study aims to analyze the psychological factors that influence the digital protective behavior of Islamic bank customers by adopting the PMT framework, as well as to evaluate the role of cybersecurity education as a moderating variable. This research also examines how Islamic values, particularly *ḥifẓ al-māl, amānah*, and *al-nuṣrah*, affect customers' protective motivation. Thus, the study not only offers an empirical contribution to understanding user behavior in the digital era but also expands the theoretical scope of PMT within the framework of Islamic economics, providing a contextual and normatively grounded approach through the integration of *maqāṣid al-sharīʿah*.

---

[5] James E. Maddux and Ronald W. Rogers, "Protection Motivation and Self-Efficacy: A Revised Theory of Fear Appeals and Attitude Change," *Journal of Experimental Social Psychology* 19, no. 5 (1983): 469–79, https://doi.org/10.1016/0022-1031(83)90023-9.

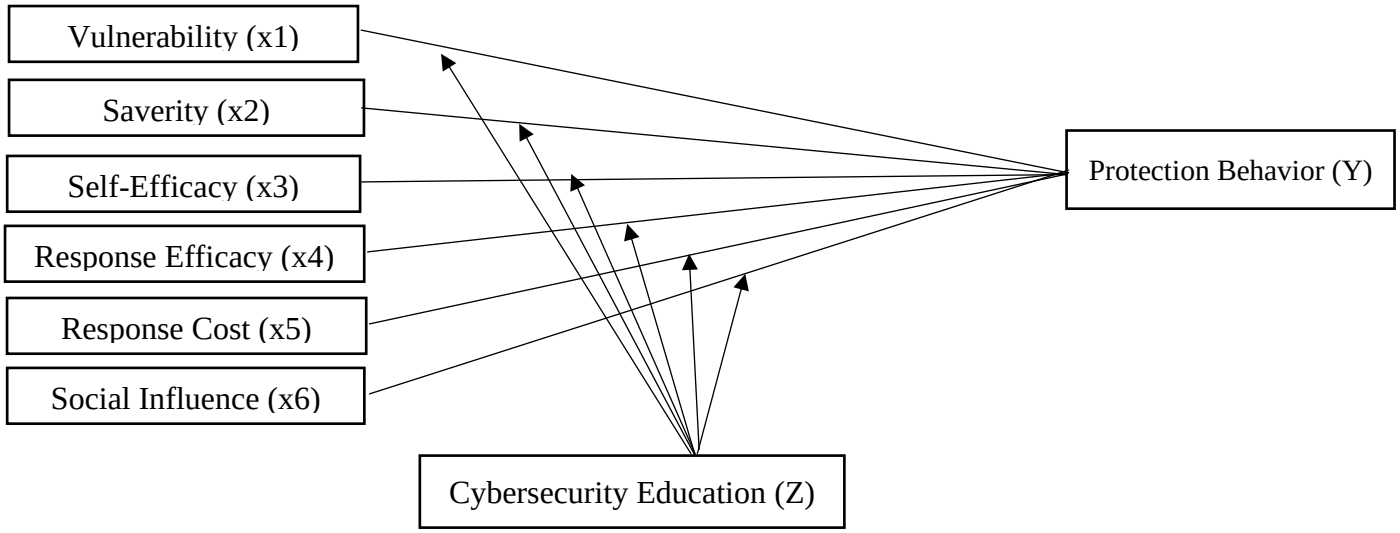
[6] Asma Alshaikh, "The Impact of KWL Plus Strategy on the Development of Perceived Self-Efficacy among Students in the Biology Department at Prince Sattam Bin Abdul-Aziz University (PSAU)—Al-Kharj Governorate," *The International Journal of Pedagogy and Curriculum* 30, no. 1 (2023): 37–53, https://doi.org/10.18848/2327-7963/CGP/v30i01/37-53.

[7] Zizhong Zhang and Xiaoxue Zhang, "Why Not Use Facial Recognition Payment? From the Perspective of the Extended Protection Motivation Theory," *Journal of Retailing and Consumer Services* 81 (2024), https://doi.org/10.1016/j.jretconser.2024.104016.

[8] Hisam Ahyani et al., "Protecting Yourself from Online Fraud and Hacking: An Islamic Perspective," *Abdurrauf Journal of Islamic Studies* 4, no. 1 (2025): 46–65, https://doi.org/10.58824/arjis.v4i1.277.

[9] Ahyani et al.

Theoretical Framework



Research Method

This study employs a quantitative approach with a cross-sectional survey design to analyze the factors influencing digital protection behavior among Islamic banking customers. This approach was chosen as it enables the researcher to examine the relationships between variables within the framework of Protection Motivation Theory (PMT) and to evaluate the role of cybersecurity education as a moderating variable.

The study population consists of Islamic banking customers in North Sumatra who actively use digital channels such as mobile and internet banking. A purposive sampling technique was used to select respondents who met the criteria of being active users of digital services for at least the past six months. A total of 384 valid responses were collected and deemed suitable for analysis. The research was conducted in North Sumatra for several reasons. As of October 2023, Islamic banking assets in the province reached approximately Rp 22.83 trillion, growing 12.54% YoY, representing 6.70% of total banking assets. The region also recorded DPK of Rp 21.12 trillion and a financing volume of Rp 16.60 trillion. These figures show that although North Sumatra's market share is slightly below the national average (7.38% in March 2024), its rapid growth and penetration of digital services make it a highly relevant context for examining protection behavior in Islamic digital banking. Nevertheless, since the sample was limited to one province, the findings should be interpreted with caution when generalizing to the wider Indonesian context, as variations in digital literacy, banking penetration, and cybersecurity awareness may exist across regions.

The research instrument was a structured questionnaire using a 5-point Likert scale, adapted from PMT constructs (perceived severity, perceived vulnerability, response efficacy, self-efficacy, response cost, and social influence), along with indicators of cybersecurity education. Cybersecurity education was operationalized through items assessing respondents' exposure to training and awareness programs provided by banks, universities, or community organizations. The content typically included topics such as phishing awareness, password management, data privacy, and safe use of mobile banking. However, these programs were generally short (often one

to two sessions) and irregular in intensity, relying more on one-off campaigns than on continuous education. The limited depth and frequency of exposure offer essential context for interpreting the moderating effect of cybersecurity education in this study.

The questionnaire was tested for validity and reliability before being widely distributed through digital platforms. Data were analyzed using Structural Equation Modeling–Partial Least Squares (SEM-PLS) with SmartPLS 4. The measurement model (outer model) was evaluated to assess convergent validity, construct reliability, and discriminant validity. The structural model (inner model) was then evaluated to assess the strength of relationships between variables, the coefficient of determination (R^2), predictive relevance (Q^2), and the moderating role of cybersecurity education.

Result

Outer Model Evaluation (Measurement Model)

Loading Factor

The outer loadings represent the extent to which each observed indicator reflects its corresponding latent construct. Following the guidelines by Hair et al., indicators with loading values below 0.70 were considered for removal to ensure convergent validity.

In this study, most indicators exceeded the recommended threshold. Four indicators—PS4 (Perceived Severity), RC3 and RC4 (Response Cost), and PB3 (Protection Behavior)—were removed due to low loadings. After model refinement, all retained indicators exhibited strong loadings, ranging from 0.721 to 0.895 across constructs. Interaction terms representing the moderating effect of cybersecurity education consistently returned perfect loadings (1.000), which is expected in moderation modeling using SmartPLS.

These results confirm the model's convergent validity and support retaining all final indicators. A complete list of the outer loadings before and after indicator removal is presented in Appendix A.

Outer loading reflects the contribution of each indicator to its respective latent construct. According to Hair et al., a loading value above 0.70 indicates acceptable convergent validity.[10]

In this study, most indicators surpassed that threshold, demonstrating strong representation of their constructs. However, four indicators—PS4, RC3, RC4, and PB3—had loading values below 0.70 and were therefore excluded to enhance the measurement model's statistical validity and ensure acceptable AVE and reliability scores.

Composite Reliability (CR)

Composite Reliability (CR) is a widely accepted measure of internal consistency in Partial Least Squares Structural Equation Modeling (PLS-SEM). Unlike Cronbach's Alpha, CR accounts for the actual loading of each indicator, making it more accurate

[10] Joseph F. Hair, Jr. et al., *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM) [3 Ed]*, *Sage Publishing*, vol. 3, 2022.

for assessing construct reliability. A CR value above 0.70 indicates satisfactory reliability. [11]

In this study, all constructs met this criterion, with CR values ranging from 0.840 to 0.919. The highest reliability was observed in Protection Behavior (0.919), followed by Response Efficacy (0.907), Perceived Vulnerability (0.883), and Self-Efficacy (0.879). Even constructs with relatively lower scores, such as Perceived Severity and Social Influence, still exceeded the minimum threshold. The complete CR values for all constructs are presented in Appendix B.

Cronbach's Alpha

Cronbach's Alpha is a traditional indicator of internal consistency that assesses how well a set of items collectively measures a latent reflective construct. Although more conservative than Composite Reliability, an Alpha value of 0.70 or higher is generally considered acceptable. [12]

In this study, all constructs exceeded this threshold. The highest internal consistency was found in Protection Behavior (0.894), followed by Response Efficacy (0.864) and Cybersecurity Education (0.820). Constructs with lower but acceptable Alpha values, such as Perceived Severity (0.716) and Response Cost (0.715), also demonstrated sufficient reliability after the removal of low-loading indicators.

These findings, consistent with the results from Composite Reliability and outer loadings, confirm that the constructs are measured reliably and that the model is appropriate for further structural analysis. Full Cronbach's Alpha values are presented in Appendix C.

Average Variance Extracted (AVE)

Average Variance Extracted (AVE) assesses convergent validity by indicating how much variance in the observed indicators is captured by their underlying latent construct. An AVE value of 0.50 or higher indicates that the construct captures at least 50% of the variance from its indicators, confirming adequate convergent validity.

In this study, all constructs met the AVE threshold. The strongest convergent validity was observed in Perceived Vulnerability (0.791), Response Cost (0.778), and Response Efficacy (0.710). Other constructs—including Protection Behavior, Perceived Severity, Cybersecurity Education, and Social Influence—also surpassed the 0.50 benchmark.

These results confirm that the constructs are well represented by their indicators and that the measurement model demonstrates strong convergent validity. Complete AVE values are presented in Appendix D.

Heterotrait-Monotrait Ratio (HTMT)

After establishing convergent validity through AVE, discriminant validity was assessed using the Heterotrait-Monotrait Ratio of Correlations (HTMT), a robust

[11] Hair, Jr. et al.

[12] Mohsen Tavakol and Reg Dennick, "Making Sense of Cronbach's Alpha," *International Journal of Medical Education* 2 (2011): 53–55, https://doi.org/10.5116/ijme.4dfb.8dfd.

criterion proposed by Henseler et al. HTMT values below 0.90 indicate adequate discriminant validity for conceptually related constructs, while a stricter threshold of 0.85 may be applied in more conservative contexts.

In this study, all HTMT values among the primary constructs—Cybersecurity Education, Perceived Severity, Perceived Vulnerability, Protection Behavior, Response Cost, Response Efficacy, Self-Efficacy, and Social Influence—fell below the 0.90 threshold, ranging from 0.555 to 0.888. The highest correlation (0.888) was observed between Cybersecurity Education and Social Influence, which still remained within acceptable limits. Moderator interactions also exhibited low HTMT values (0.021–0.648), confirming the distinctiveness of all constructs in the model.

In summary, the measurement model fulfilled all reliability and validity criteria. Outer loadings exceeded 0.70 after removing weak indicators, while Composite Reliability and Cronbach's Alpha values were above 0.70, confirming internal consistency. All AVE values surpassed 0.50, and HTMT values indicated discriminant validity. The full HTMT matrix is presented in Appendix E. Hence, the model is statistically sound and suitable for structural model analysis.

Inner Model (Structural Model Evaluation)

Collinearity (VIF)

Before proceeding to structural model evaluation, it is necessary to assess multicollinearity among the exogenous variables. Multicollinearity can inflate standard errors and distort path coefficient estimates, leading to biased interpretations. In PLS-SEM, the Variance Inflation Factor (VIF) is commonly used for this purpose. A VIF value below 5.0 is generally acceptable, with a more conservative threshold of 3.3 sometimes applied. [13]

In this study, all indicators had VIF values between 1.358 and 2.567, which are well within acceptable limits. While some indicators in constructs such as Protection Behavior and Response Efficacy exhibited relatively higher VIFs (close to 2.5), none exceeded critical thresholds. All interaction terms, derived as standardized product indicators, had VIF values of exactly 1.000, confirming the absence of collinearity between moderating terms and their source constructs.

These results confirm that the model does not suffer from multicollinearity and is thus suitable for reliable structural path analysis. Detailed VIF values are presented in Appendix F.

Path Coefficients

After verifying the absence of multicollinearity through VIF analysis, the evaluation moved to the structural model, emphasizing the path coefficients. These coefficients indicate the strength and direction of relationships between latent variables, where values closer to ±1 reflect stronger relationships. To assess statistical significance, this study employed the bootstrapping method with 5,000 resamples,

[13] Agus Purwanto and Yuli Sudargini, "Partial Least Squares Structural Squation Modeling (PLS-SEM) Analysis for Social and Management Research : A Literature Review," *Journal of Industrial Engineering & Management Research* 2, no. 4 (2021): 114–23.

yielding robust t-statistics and p-values for hypothesis testing at a 95% confidence level.

The results demonstrate that Perceived Vulnerability, Perceived Severity, Response Efficacy, and Social Influence exert a positive and statistically significant influence on Protection Behavior. These findings support the core assumptions of the Protection Motivation Theory (PMT), confirming that both the perception of threat and belief in the effectiveness of protective actions, as well as encouragement from others, are strong motivators for security-related behavior among Islamic bank customers.

Conversely, Self-Efficacy and Response Cost did not show significant effects. This suggests that internal confidence and perceived inconvenience are not major drivers of protective behavior in this context, possibly due to improved user experience and automation in digital banking systems.

Regarding the moderating role of Cybersecurity Education, none of the six hypothesized interactions showed statistically significant effects. This suggests that current cybersecurity education efforts may not significantly modify the influence of PMT constructs on behavior. The lack of significance could stem from content that is too generic, insufficiently contextualized, or disconnected from users' actual experiences and motivations.

In sum, the path coefficient analysis supports several key theoretical relationships while also revealing important practical limitations in current educational strategies. Full statistical results—including path coefficients, t-values, and p-values—are presented in Appendix G.

R^2 (Coefficient of Determination)

The coefficient of determination (R^2) is a central metric for evaluating the explanatory power of the structural model in PLS-SEM. It reflects the proportion of variance in the endogenous construct—in this case, Protection Behavior—that is explained by all the exogenous variables in the model.

According to Hair et al., R^2 values of 0.75, 0.50, and 0.25 are considered substantial, moderate, and weak, respectively. [14] In this study, the R^2 for Protection Behavior was 0.696, indicating that nearly 70% of the variance in users' cybersecurity behavior is explained by the PMT constructs and their interactions with cybersecurity education. This level of explanatory power falls within the moderate to strong range, which is generally acceptable in behavioral and social science research, especially within a predictive modeling context.

An adjusted R^2 value of 0.685 was also recorded. While adjusted R^2 is typically used in parametric models, in PLS-SEM it serves only as a reference, since the focus lies more on maximizing predictive relevance than on parameter estimation.

Overall, these results suggest that the model captures the majority of variance in the outcome variable and provides a solid empirical foundation for both theoretical

[14] Hair, Jr. et al., *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM) [3 Ed]*.

implications and practical recommendations. Full R^2 and adjusted R^2 values are presented in Appendix H.

f^2 (Effect Size)

To assess the practical contribution of each exogenous construct in explaining the endogenous variable, this study conducted an effect size (f^2) analysis. The f^2 statistic measures the magnitude of change in R^2 when a specific predictor is included or excluded from the model. While path coefficients indicate statistical significance, f^2 provides insight into the practical importance of each construct.

According to Hair et al., f^2 values are interpreted as follows: ≥ 0.35 indicates a large effect, 0.15–0.34 a moderate effect, 0.02–0.14 a small effect, and < 0.02 is considered negligible. [15]

In this study, Cybersecurity Education showed the strongest effect ($f^2 = 0.171$), representing a moderate and meaningful contribution to explaining Protection Behavior. This was followed by Perceived Severity ($f^2 = 0.055$) and Perceived Vulnerability ($f^2 = 0.033$)—both falling within the small but practically relevant range. Social Influence and Response Efficacy also showed small effects, reinforcing their theoretical salience within the Protection Motivation Theory (PMT) framework. By contrast, Response Cost and Self-Efficacy recorded f^2 values below 0.01, suggesting a minimal contribution to behavioral variance. Regarding moderation effects, all interactions between Cybersecurity Education and the main constructs showed minimal effect sizes ($f^2 < 0.02$), with the highest being the interaction with Social Influence ($f^2 = 0.012$). This indicates a marginal moderation effect, consistent with expectations for interaction terms in behavioral models.

In summary, f^2 results suggest that Cybersecurity Education, Perceived Severity, and Social Influence are the most practically impactful constructs in shaping protective behavior among Islamic digital banking users. A complete breakdown of effect size values is provided in Appendix I.

Q^2 (Predictive Relevance)

Following the assessment of explanatory power through R^2 and f^2, the model's predictive relevance was evaluated using the Q^2 statistic, calculated via the blindfolding procedure in SmartPLS. Q^2 measures the model's capability to predict omitted data points for the endogenous construct—in this case, Protection Behavior.

According to Hair et al., a Q^2 value greater than zero ($Q^2 > 0$) indicates that the model has predictive relevance. A value of zero or below indicates no predictive capability.

In this study, all Q^2 values for the Protection Behavior indicators exceeded the minimum threshold, ranging from 0.386 to 0.492. The highest predictive accuracy was observed for PB7 ($Q^2 = 0.492$) and PB6 ($Q^2 = 0.475$), confirming the model's robustness in predicting behavior across different items.

[15] David J. Ketchen, "A Primer on Partial Least Squares Structural Equation Modeling," *Long Range Planning* 46, no. 1–2 (2013): 184–85, https://doi.org/10.1016/j.lrp.2013.01.002.

These results indicate that the model not only explains variance effectively through R^2 but also demonstrates strong out-of-sample predictive ability. This enhances the model's external validity and supports its practical application in forecasting digital protection behavior among Islamic banking customers. Detailed Q^2 values are presented in Appendix J.

PLSPredict

After establishing model validity through R^2, f^2, and Q^2 analyses, the final step in evaluating the structural model involves assessing its out-of-sample predictive performance using the PLSpredict procedure. This method assesses the model's predictive power by comparing its cross-validated prediction errors with those of a linear regression benchmark (LM).

The model's predictive accuracy is measured using two key metrics: Root Mean Square Error (RMSE) and Mean Absolute Error (MAE). Lower values indicate better predictive performance.

In this study, PLSpredict results showed that the PLS-SEM model performed comparably—and in some cases slightly better—than the LM model in predicting the observed indicators of Protection Behavior. For instance, indicators PB6 and PB7 exhibited lower RMSE values in PLS-SEM than in LM, suggesting more accurate prediction. Although the LM model slightly outperformed PLS-SEM for PB1 and PB2, the error differences were negligible.

Overall, these results confirm that the PLS-SEM model has adequate predictive power, supporting its use for forecasting protection behavior in Islamic digital banking contexts. This reinforces the model's external validity and practical applicability for guiding cybersecurity strategies and behavioral interventions in financial institutions. Detailed PLSpredict results are presented in Appendix K.

Model Fit (SRMR)

Model fit evaluation is an important step in structural model analysis using Partial Least Squares Structural Equation Modeling (PLS-SEM). Although PLS-SEM is primarily prediction-oriented, certain fit indices—especially the Standardized Root Mean Square Residual (SRMR)—are still useful for assessing how well the model reproduces observed data patterns.

SRMR reflects the average difference between the empirical and model-implied correlation matrices. A value below 0.10 is generally considered acceptable, while a value under 0.08 indicates a very good fit (Henseler et al., 2016). Unlike CB-SEM, PLS-SEM does not require exact model fit, but SRMR serves as a helpful diagnostic to confirm model adequacy.

In this study, the SRMR value for both the saturated and estimated models was 0.060, which meets the criteria for a good fit. This suggests that the structural model aligns well with the observed data and supports the validity of the proposed relationships among constructs.

Additional fit statistics, including d_ULS, d_G, chi-square, and NFI, are also within acceptable limits and further support the model's adequacy. Detailed fit indices are presented in Appendix L.

Discussion

The influence of perceived vulnerability on the protection behavior of Islamic bank customers

The significant effect of perceived vulnerability on protective behavior supports the core proposition of Protection Motivation Theory (PMT),[16] which views threat appraisal as a primary determinant of security-related actions. Prior studies consistently highlight that individuals who perceive themselves as vulnerable to cyber threats are more likely to implement protective measures.[17] Ifinedo showed that higher perceived vulnerability leads to stronger adoption of cybersecurity practices,[18] Jansen and Leukfeldt found that susceptibility to phishing increased the use of preventive measures such as two-factor authentication.[19] Similarly, Herath and Rao concluded that greater awareness of cyber risks enhances compliance with security policies.[20] These findings collectively reinforce that vulnerability perception functions as an early cognitive trigger for digital self-protection.

From the perspective of *maqāṣid al-sharīʿah*, this result reflects the obligation to preserve wealth (ḥifẓ al-māl) by preventing harm before it occurs. Recognizing one's vulnerability to fraud, hacking, or identity theft is aligned with the moral duty to avoid taḍyīʿ al-māl (waste or loss of wealth) and to maintain the trust (*amānah*) inherent in financial transactions. In this sense, perceived vulnerability is not only a psychological driver but also a spiritual awareness that encourages Muslims to act cautiously in the digital financial environment, thereby fulfilling both personal responsibility and communal protection.

The influence of perceived severity of threats on the protection behavior of Islamic bank customers.

The significant role of perceived severity aligns with previous findings showing that when users recognize the serious consequences of cyber threats, they are more likely to implement protective actions. Mkilia and Sife demonstrated that perceived

---

16 Ronald W. Rogers, "A Protection Motivation Theory of Fear Appeals and Attitude Change1," *The Journal of Psychology* 91, no. 1 (1975): 93–114, https://doi.org/10.1080/00223980.1975.9915803.

17 James E. Maddux and Ronald W. Rogers, "Protection Motivation and Self-Efficacy: A Revised Theory of Fear Appeals and Attitude Change," *Journal of Experimental Social Psychology* 19, no. 5 (1983): 469–79, https://doi.org/10.1016/0022-1031(83)90023-9.

18 Princely Ifinedo, "Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory," Computers and Security 31, no. 1 (2012): 83–95, https://doi.org/10.1016/j.cose.2011.10.007.

19 Jurjen Jansen and Rutger Leukfeldt, "Phishing and Malware Attacks on Online Banking Customers in the Netherlands: A Qualitative Analysis of Factors Leading to Victimization," International Journal of Cyber Criminology 10, no. 1 (2016): 79–91, https://doi.org/10.5281/zenodo.58523.

20 Tejaswini Herath and H. Raghav Rao, "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations," *European Journal of Information Systems* 18, no. 2 (2009): 106–25, https://doi.org/10.1057/ejis.2009.6.

severity predicts cybersecurity behavior among mobile banking users in Tanzania,[21] while Tambariki et al. confirmed similar effects in Indonesia, where severe risk perception motivates adoption of measures such as two-factor authentication.[22]

From the perspective of *maqāṣid al-sharīʿah*, acknowledging the severity of potential digital threats is part of fulfilling the obligation of ḥifẓ al-māl. Seeing cyberattacks as capable of causing major harm (mafsadah) compels individuals to take preventive action, thereby avoiding taḍyīʿ al-māl (waste or loss of wealth). This reflects not only rational self-protection but also a moral responsibility to preserve wealth as an *amānah* entrusted to them.The study confirms that perceived severity has a positive and significant influence on protection behavior among Islamic banking customers.

The influence of Self-Efficacy of threats on the protection behavior of Islamic bank customers.

The non-significant effect of self-efficacy suggests that while customers may feel confident in their ability to handle cyber threats, such confidence does not always lead to protective behavior. This finding is consistent with Mkilia et al., who observed that self-efficacy is not a dominant predictor of cybersecurity practices when users lack adequate technical skills.[23] Similarly, Ley Sylvester et al. found that individuals often overestimate their ability to detect threats such as phishing, leading to complacency and weak security behavior.[24]

From the perspective of *maqāṣid al-sharīʿah*, this outcome highlights a gap in the realization of *amānah*. Confidence without action reflects negligence in safeguarding entrusted wealth, which can result in *taḍyīʿ al-māl* (loss of assets). In the context of Islamic banking, the absence of protective action despite high self-confidence may undermine both personal responsibility and the collective obligation to maintain security. Thus, enhancing actual competence through continuous training is essential to align self-efficacy with the duty of *ḥifẓ al-māl*.

The influence of response efficacy on the protection behavior of Islamic bank customers.

The significant positive influence of response efficacy aligns not only with Mkilia et al., but is further supported by Vafaei-Zadeh et al., who found that response efficacy and self-efficacy both significantly enhance cybersecurity awareness among

21 Emmanuel Lameck Mkilia et al., "Cybersecurity Risks and Customers' Protective Behavior on Usage of Mobile Banking Services: Evidence from Selected Banks in Tanzania," *Local Administration Journal* 16, no. 3 (2023): 329–54, https://so04.tci-thaijo.org/index.php/colakkujournals/article/view/264954.
22 Canitgia Tambariki et al., "Drivers of Banking Consumers' Cybersecurity Behavior: Applying the Extended Protection Motivation Theory," *GATR Journal of Management and Marketing Review* 9, no. 1 (2024): 01–12, https://doi.org/10.35609/jmmr.2024.9.1(1).
23 Lameck Mkilia et al., "Cybersecurity Risks and Customers' Protective Behavior on Usage of Mobile Banking Services: Evidence from Selected Banks in Tanzania."
24 F. Ley Sylvester, "Mobile Device Users' Susceptibility to Phishing Attacks," *International Journal of Computer Science and Information Technology* 14, no. 1 (2022): 1–18, https://doi.org/10.5121/ijcsit.2022.14101.

online banking users in Malaysia.[25] A similar pattern is found in "How cybercrime sentiment shapes mobile banking adoption", where users' belief in the effectiveness of security features (and trust) helps mediate adoption behavior in Islamic banking contexts.[26]

From the *maqāṣid al-sharīʿah* perspective, response efficacy reflects the value of *amānah*: belief in protective mechanisms as reliable tools to guard entrusted wealth. This belief is essential for fulfilling the obligation of *ḥifẓ al-māl*, because only when users trust that security measures are effective will they consistently act to prevent harm (mafsadah) and loss of wealth.

The influence of perceived response cost on the protection behavior of Islamic bank customers.

The non-significant effect of response cost in this study suggests that perceived barriers such as time, inconvenience, or effort are not major deterrents for Islamic banking customers when adopting protective behaviors. This is consistent with findings from "Measuring User Perceived Security of Mobile Banking Applications", which show that users prioritize trust and perceived security over inconvenience when deciding to adopt.[27] Similarly, Factors Influencing Choice of Islamic Digital Banking reports that in the Islamic banking context in Indonesia, many cost-related concerns do not significantly deter adoption of digital banking services when perceived benefits like trust, accessibility, and convenience are high.[28]

From the *maqāṣid al-sharīʿah* perspective, the willingness to accept minor inconvenience or cost reflects the principle of *amānah* and the obligation to preserve wealth (*ḥifẓ al-māl*). In other words, when customers believe protective measures are trustworthy and essential, they may endure some inconvenience as part of their moral duty to prevent *mafsadah* and ensure digital financial transactions uphold the trust given to them.

The influence of social influence on the protection behavior of Islamic bank customers.

The finding that social influence significantly predicts protective behavior among Islamic banking customers aligns with studies such as "Perceived Benefits, Trust, and Social Influence in FinTech Payment Services," which likewise highlight the role of social endorsement in encouraging the adoption of digital financial tools. It also

[25] Razib Chandra Chanda et al., "Assessing Cybersecurity Awareness among Bank Employees: A Multi-Stage Analytical Approach Using PLS-SEM, ANN, and FsQCA in a Developing Country Context," *Computers and Security* 149 (2025): 104208, https://doi.org/10.1016/j.cose.2024.104208.
[26] Yenny Kornitasari, Langlang Jati Sura, and Dita Nurul Aini Mustika Dewi, "How Cybercrime Sentiment Shapes Mobile Banking Adoption in Islamic Banking," *Jurnal Ekonomi & Keuangan Islam* 10, no. 2 (2024): 217–32, https://doi.org/10.20885/jeki.vol10.iss2.art6.
[27] Richard Apau, Elzbieta Titis, and Harjinder Singh Lallie, "Towards a Better Understanding of Mobile Banking App Adoption and Use: Integrating Security, Risk, and Trust into UTAUT2," *Computers* 14, no. 4 (2025), https://doi.org/10.3390/computers14040144.
[28] Alex Fahrur Riza and Dwi Marlina Wijayanti, "Strengthening a Sustainable Islamic Financial Industry through Digital Banking," *Journal of Islamic Marketing* 15, no. 11 (June 3, 2024): 2732–58, https://doi.org/10.1108/JIMA-01-2023-0025.

resonates with Behavioural Insights Into Cybersecurity Practices Among Digital Banking Consumers in South Africa, where subjective norms (social influence) emerged as a strong predictor of cybersecurity behavioral intention.[29]

From the *maqāṣid al-sharīʿah* perspective, these findings emphasize that social influence serves not merely as external pressure but as an instrument of shared moral responsibility.[30] When peers, family, religious leaders, or trusted communities promote safe digital practices, they help fulfill the duty of *farḍ kifāyah* to protect communal wealth (*ḥifẓ al-māl*). Collective endorsement fosters *al-nuṣrah* (mutual support), reinforcing that cybersecurity in Islamic banking is a communal obligation, not solely an individual choice.

Cybersecurity education moderates the relationship between perceived vulnerability and the protection behavior of Islamic bank customers.

The non-significant moderating role of cybersecurity education suggests that when customers already perceive themselves as vulnerable, this perception alone is sufficient to trigger protective behavior, regardless of additional educational input. This pattern is consistent with Bansal et al., who showed that highly personal threat perceptions often override the influence of formal training, and with Addula in 2021, who noted that in mobile banking contexts, users tend to react directly to perceived risks without waiting for structured educational reinforcement.[31]

From the perspective of *maqāṣid al-sharīʿah*, this finding implies that personal awareness of potential harm can itself be a strong motivator for ḥ*ifẓ al-māl*. However, the absence of a moderating effect does not diminish the value of cybersecurity education. Instead, it highlights the need for educational programs that go beyond awareness-raising and focus on practical competence and ethical responsibility (*amānah*). Effective training should not only inform but also empower customers to consistently implement protective measures, thereby aligning individual perceptions of risk with communal efforts to prevent *mafsadah* and safeguard wealth.

Cybersecurity education moderates the relationship between perceived severity of threats and the protection behavior of Islamic bank customers.

The absence of a significant moderating effect of cybersecurity education indicates that when customers already perceive cyber threats as severe, they tend to take protective action independently. This suggests that strong personal threat awareness may outweigh the additional influence of general educational programs. Similar conclusions were drawn by Tambariki et al., who found that high levels of

[29] Luan Vardari and Kujtim Hameli, "Perceived Benefits, Trust and Social Influence in FinTech: Pathways to Adoption and Satisfaction in a Developing Economy," *Global Knowledge, Memory and Communication*, September 11, 2025, https://doi.org/10.1108/GKMC-02-2025-0137.
[30] Jasser Auda, "Maqasid Al-Shariah As Philosophy of Islamic Law," 2008, 1–332.
[31] G. Bansal, F.M. Zahedi, and D. Gefen, *The Moderating Influence of Privacy Concern on the Efficacy of Privacy Assurance Mechanisms for Building Trust: A Multiple-Context Investigation | L'effet Modérateur Du Souci de Confidentialité Sur l'efficacité Des Mécanismes de Respect de La Vie Privée À*, *ICIS 2008 Proceedings - Twenty Ninth International Conference on Information Systems*, 2008.

threat perception reduce the marginal impact of formal training,[32] and by Khan et al., who emphasized that generic education often lacks effectiveness when it is not personalized or context-specific.[33]

From the *maqāṣid al-sharīʿah* perspective, this highlights an important gap: while ḥifẓ al-māl motivates individuals to act when they recognize severe risks, the principle of *amānah* requires institutions to provide education that is practical, contextual, and ethically grounded. Cybersecurity education should therefore move beyond awareness campaigns to emphasize skills, real-life scenarios, and moral responsibility, ensuring that protective behavior is not only reactionary but also proactive and sustainable.

Cybersecurity education moderates the relationship between self-efficacy and the protection behavior of Islamic bank customers.

The absence of a significant moderating effect of cybersecurity education on the relationship between self-efficacy and protective behavior suggests that confidence alone, even when supplemented by general education, is insufficient to drive consistent security practices. This finding is consistent with Guo et al., who observed that self-reported confidence without hands-on skill development limits the effectiveness of cybersecurity education, and with Kumar & Ekstrom, who noted that confidence lacking technical depth often remains superficial and does not translate into behavioral change.[34]

From the *maqāṣid al-sharīʿah* perspective, this underscores a gap between perceived ability and actual responsibility. While self-efficacy reflects personal readiness, the principle of *amānah* requires that confidence be supported by real competence to safeguard wealth (*ḥifẓ al-māl*). Cybersecurity education, therefore, must be designed not only to raise awareness but also to provide practical training and ethical grounding, ensuring that digital confidence is matched with actionable skills to prevent *mafsadah* and uphold trust in Islamic financial transactions.

Cybersecurity education moderates the relationship between response efficacy and the protection behavior of Islamic bank customers.

The finding that cybersecurity education does not significantly moderate the relationship between response efficacy and protective behavior suggests a gap between belief and practice. Customers may already recognize that measures such as OTP, two-factor authentication, and regular app updates are effective, yet existing educational programs do little to amplify this belief into stronger security habits. In other words,

[32] Tambariki et al., "Drivers of Banking Consumers' Cybersecurity Behavior: Applying the Extended Protection Motivation Theory."
[33] Naurin Farooq Khan et al., "Evaluating Protection Motivation Based Cybersecurity Awareness Training on Kirkpatrick's Model," *Computers and Security* 125 (2023): 103049, https://doi.org/10.1016/j.cose.2022.103049.
[34] Johri and Kumar, "Exploring Customer Awareness towards Their Cyber Security in the Kingdom of Saudi Arabia: A Study in the Era of Banking Digital Transformation."

knowledge of effectiveness alone does not necessarily translate into action when the education offered remains abstract or generic.

This result resonates with Apau & Singh[35] and Alalwan,[36] who emphasized that formal education often falls short when it is overly technical or disconnected from users' everyday realities. To be impactful, cybersecurity education must be practical, contextual, and directly relevant to daily banking practices, bridging the gap between awareness and consistent protective behavior.

From the *maqāṣid al-sharīʿah* perspective, the weakness of current educational approaches indicates an incomplete fulfillment of *amānah*. While users may trust in the utility of protective tools, institutions carry the responsibility to equip them with actionable knowledge that ensures effective implementation. Only then can the ethical mandate of ḥifẓ al-māl be realized, not as passive awareness but as active protection against harm (*mafsadah*) in digital financial transactions.

Cybersecurity education moderates the relationship between response cost and the protection behavior of Islamic bank customers.

The lack of a moderating effect of cybersecurity education on the relationship between response cost and protective behavior suggests that training efforts have not significantly changed customer perceptions of inconvenience, time demands, or technical complexity. Users still prioritize transaction convenience over the extra effort needed for stronger protection, reducing the impact of education on their willingness to adopt security measures.

This outcome aligns with Hsu[37] and Chanda et al.[38], who observed that when education is too generic or detached from users' practical realities, it fails to reduce perceptions of cost. Customers are more likely to dismiss additional steps if they view them as slowing down their banking experience, regardless of the potential security benefits.

From the perspective of *maqāṣid al-sharīʿah*, this finding underscores the ethical responsibility of institutions in fulfilling *amānah*. Simply delivering information is not sufficient; education must be designed to demonstrate that minor inconveniences are justified as part of the duty to safeguard wealth (*ḥifẓ al-māl*) and prevent *mafsadah*. In this sense, effective cybersecurity education in Islamic banking should normalize protective behavior as an ethical obligation, not an optional burden.

[35] Richard Apaua and Harjinder Singh Lallie, "Measuring User Perceived Security of Mobile Banking Applications," 2022, 1–36, http://arxiv.org/abs/2201.03052.
[36] Ali Abdallah Alalwan et al., "Consumer Adoption of Mobile Banking in Jordan: Examining the Role of Usefulness, Ease of Use, Perceived Risk and Self-Efficacy," *Journal of Enterprise Information Management* 29, no. 1 (February 1, 2016): 118–39, https://doi.org/10.1108/JEIM-04-2015-0035.
[37] Yilin Hu and Carol Hsu, "Effect of Perceived Cost, Altruistic and Egoistic Benefits on Security Policy Compliance Intention: A Rational Choice Persepective," *PACIS 2021 Proceedings*, 2021, 1–8, https://aisel.aisnet.org/pacis2021/156.
[38] Chanda et al., "Assessing Cybersecurity Awareness among Bank Employees: A Multi-Stage Analytical Approach Using PLS-SEM, ANN, and FsQCA in a Developing Country Context."

Cybersecurity education moderates the relationship between social influence and the protection behavior of Islamic bank customers.

The non-significant moderating effect of cybersecurity education on the relationship between social influence and protective behavior suggests that institutional training remains secondary to community dynamics. In collectivist settings such as Indonesia, individuals are more inclined to follow the recommendations and practices of family, peers, religious leaders, and trusted networks than to respond to one-way educational messages from banks.

This result echoes Hong et al., who found that community-based influence often surpasses formal education in shaping cybersecurity behavior. In practice, users in this study were more likely to adopt tools such as OTP or two-factor authentication after encouragement from their social environment rather than from institutional campaigns.[39]

From the *maqāṣid al-sharīʿah* perspective, this highlights the communal dimension of security practices. Social influence can embody *farḍ kifāyah*, where collective awareness and mutual reinforcement ensure broader protection of wealth (*ḥifẓ al-māl*). At the same time, the inability of institutional education to strengthen this effect signals a need for Islamic banks to reposition cybersecurity training as participatory and community-driven, aligning with the principle of *amānah* to safeguard assets entrusted to the financial system.

Overall, the findings of this study indicate that perceived vulnerability, perceived severity, response efficacy, and social influence emerge as the most consistent drivers of protective behavior in Islamic digital banking. In contrast, self-efficacy and response cost show no meaningful effect, while cybersecurity education fails to moderate the key relationships within the PMT framework. With an explanatory power of 69.6%, the model highlights that protective behavior is driven mainly by risk perception and social influence, rather than technical self-confidence or perceived inconvenience.

From the *maqāṣid al-sharīʿah* perspective, these findings reaffirm the centrality of ḥ*ifẓ al-māl* as both an individual and collective obligation. Confidence in the efficacy of security measures reflects the principle of *amānah* (trust and moral responsibility), while the strong role of social influence illustrates the value of al-nuṣrah (mutual support) and the communal nature of *farḍ kifāyah* in safeguarding wealth. Conversely, the weak role of cybersecurity education indicates that technical training alone is insufficient unless it also engages ethical motivation and community-based learning.

Theoretically, this research enriches Protection Motivation Theory by embedding it within the Islamic economic framework, showing that responses to digital threats are shaped not only by technical and cognitive factors but also by ethical

[39] Yuxiang Hong and Steven Furnell, "Understanding Cybersecurity Behavioral Habits: Insights from Situational Support," *Journal of Information Security and Applications* 57 (January 7, 2021): 102710, https://doi.org/10.1016/j.jisa.2020.102710.

and social imperatives.[40] Practically, it underscores the need for Islamic banks to design security strategies that are participatory, value-driven, and socially anchored, ensuring that digital protection becomes both a behavioral norm and a moral commitment among Muslim customers.

Conclusion

This study concludes that among Islamic bank customers, several key factors—such as perceived vulnerability, perceived severity, response efficacy, and social influence—have a significant positive impact on protection behavior in digital banking environments. Conversely, self-efficacy and response cost show no significant direct effects, suggesting that confidence or perceived effort alone may not necessarily motivate protective digital behaviors. Furthermore, while cybersecurity education is essential, the findings reveal that it fails to significantly moderate the relationship between most predictor variables and protection behavior, including self-efficacy, response efficacy, response cost, and social influence.

These insights suggest that current cybersecurity education efforts by Islamic banks are not yet sufficiently contextual, personalized, or impactful to strengthen customer protective behavior. Customers are often more influenced by real-world experiences, perceived threats, and social networks than by generic educational messages.

Recommendations include the urgent need for Islamic banks to redesign their cybersecurity education strategies to be more practical, emotionally engaging, and socially embedded. This can be achieved by incorporating real-case simulations, interactive content, and community-based campaigns involving trusted figures such as religious leaders or digital banking ambassadors. Banks should also invest in user-friendly security features and rewards-based learning systems to reduce the perception of response cost. Finally, regulators and banks must collaborate to create cybersecurity literacy programs that go beyond awareness—empowering customers with the technical skills and motivation to protect themselves consistently in an increasingly complex digital landscape.

Acknowledgment

The authors would like to express their sincere gratitude to the Ministry of Religious Affairs of the Republic of Indonesia for its generous support in both the presentation of this paper at AICIS+ 2025 and its subsequent publication.

References

Ahyani, Hisam, Sérgio António Neves Lousada, Sartono Sartono, Andrey Kotyazhov, and Miftakhul Huda. “Protecting Yourself from Online Fraud and Hacking: An Islamic Perspective.” *Abdurrauf Journal of Islamic Studies* 4, no. 1 (2025): 46–65. https://doi.org/10.58824/arjis.v4i1.277.

Al-Ghazali, Imam. *Al-Mustashfa Jilid 2: Rujukan Utama Ushul Fikih*. Vol. 2. Pustaka Al-Kautsar, 2022.

[40] Mohammad Hashim Kamali, “Between Separation and Unity: The Interplay of Law and Morality in Islamic Jurisprudence,” in *Sharia Law In The Twenty-First Century* (World Scientific, 2022), 21–46.

Alalwan, Ali Abdallah, Yogesh K. Dwivedi, Nripendra P.P. Rana, and Michael D. Williams. "Consumer Adoption of Mobile Banking in Jordan: Examining the Role of Usefulness, Ease of Use, Perceived Risk and Self-Efficacy." *Journal of Enterprise Information Management* 29, no. 1 (February 1, 2016): 118–39. https://doi.org/10.1108/JEIM-04-2015-0035.

Alshaikh, Asma. "The Impact of KWL Plus Strategy on the Development of Perceived Self-Efficacy among Students in the Biology Department at Prince Sattam Bin Abdul-Aziz University (PSAU)—Al-Kharj Governorate." *The International Journal of Pedagogy and Curriculum* 30, no. 1 (2023): 37–53. https://doi.org/10.18848/2327-7963/CGP/v30i01/37-53.

Apau, Richard, Elzbieta Titis, and Harjinder Singh Lallie. "Towards a Better Understanding of Mobile Banking App Adoption and Use: Integrating Security, Risk, and Trust into UTAUT2." *Computers* 14, no. 4 (2025). https://doi.org/10.3390/computers14040144.

Apaua, Richard, and Harjinder Singh Lallie. "Measuring User Perceived Security of Mobile Banking Applications," 2022, 1–36. http://arxiv.org/abs/2201.03052.

Bansal, G., F.M. Zahedi, and D. Gefen. *The Moderating Influence of Privacy Concern on the Efficacy of Privacy Assurance Mechanisms for Building Trust: A Multiple-Context Investigation | L'effet Modérateur Du Souci de Confidentialité Sur l'efficacité Des Mécanismes de Respect de La Vie Privée À. ICIS 2008 Proceedings - Twenty Ninth International Conference on Information Systems*, 2008.

Chanda, Razib Chandra, Ali Vafaei-Zadeh, Haniruzila Hanifah, and Davoud Nikbin. "Assessing Cybersecurity Awareness among Bank Employees: A Multi-Stage Analytical Approach Using PLS-SEM, ANN, and FsQCA in a Developing Country Context." *Computers and Security* 149 (2025): 104208. https://doi.org/10.1016/j.cose.2024.104208.

Hair, Jr., Joseph F., G. Tomas M. Hult, Christian M. Ringle, Sarstedt, and Marko. *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM) [3 Ed]. Sage Publishing*. Vol. 3, 2022.

Herath, Tejaswini, and H. Raghav Rao. "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations." *European Journal of Information Systems* 18, no. 2 (2009): 106–25. https://doi.org/10.1057/ejis.2009.6.

Hong, Yuxiang, and Steven Furnell. "Understanding Cybersecurity Behavioral Habits: Insights from Situational Support." *Journal of Information Security and Applications* 57 (January 7, 2021): 102710. https://doi.org/10.1016/j.jisa.2020.102710.

Hu, Yilin, and Carol Hsu. "Effect of Perceived Cost, Altruistic and Egoistic Benefits on Security Policy Compliance Intention: A Rational Choice Persepective." *PACIS 2021 Proceedings*, 2021, 1–8. https://aisel.aisnet.org/pacis2021/156.

Ifinedo, Princely. "Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory." *Computers and Security* 31, no. 1 (2012): 83–95. https://doi.org/10.1016/j.cose.2011.10.007.

Jansen, Jurjen, and Rutger Leukfeldt. "Phishing and Malware Attacks on Online Banking Customers in the Netherlands: A Qualitative Analysis of Factors Leading to Victimization." *International Journal of Cyber Criminology* 10, no. 1 (2016): 79–91. https://doi.org/10.5281/zenodo.58523.

Jasser Auda. "MAQASID AL-SHARIAH AS PHILOSOPHY OF ISLAMIC LAW," 2008, 1–332.

Johri, Amar, and Shailendra Kumar. "Exploring Customer Awareness towards Their Cyber Security in the Kingdom of Saudi Arabia: A Study in the Era of Banking Digital Transformation." *Human Behavior and Emerging Technologies* 2023 (2023). https://doi.org/10.1155/2023/2103442.

Kamali, Mohammad Hashim. "Between Separation and Unity: The Interplay of Law and Morality in Islamic Jurisprudence." In *Sharia Law In The Twenty-First Century*, 21–46. World Scientific, 2022.

Ketchen, David J. "A Primer on Partial Least Squares Structural Equation Modeling." *Long Range Planning* 46, no. 1–2 (2013): 184–85. https://doi.org/10.1016/j.lrp.2013.01.002.

Khan, Habib Ullah, Muhammad Zain Malik, Shah Nazir, and Faheem Khan. "Utilizing Bio Metric System for Enhancing Cyber Security in Banking Sector: A Systematic Analysis." *IEEE Access* 11 (2023): 80181–98. https://doi.org/10.1109/ACCESS.2023.3298824.

Khan, Naurin Farooq, Naveed Ikram, Hajra Murtaza, and Mehwish Javed. "Evaluating Protection Motivation Based Cybersecurity Awareness Training on Kirkpatrick's Model." *Computers and Security* 125 (2023): 103049. https://doi.org/10.1016/j.cose.2022.103049.

Kornitasari, Yenny, Langlang Jati Sura, and Dita Nurul Aini Mustika Dewi. "How Cybercrime Sentiment Shapes Mobile Banking Adoption in Islamic Banking." *Jurnal Ekonomi & Keuangan Islam* 10, no. 2 (2024): 217–32. https://doi.org/10.20885/jeki.vol10.iss2.art6.

Lameck Mkilia, Emmanuel, Emmanuel Lameck, Mkilia Jones, T Kaleshu, and Alfred S Sife. "Cybersecurity Risks and Customers' Protective Behavior on Usage of Mobile Banking Services: Evidence from Selected Banks in Tanzania." *Local Administration Journal* 16, no. 3 (2023): 329–54. https://so04.tci-thaijo.org/index.php/colakkujournals/article/view/264954.

Maddux, James E., and Ronald W. Rogers. "Protection Motivation and Self-Efficacy: A Revised Theory of Fear Appeals and Attitude Change." *Journal of Experimental Social Psychology* 19, no. 5 (1983): 469–79. https://doi.org/10.1016/0022-1031(83)90023-9.

Masruchin, Masruchin, Arief Wicaksono, Nur Manna Silvia, and Amelia Eka Dimawan. "Enhancing Maqasid Syariah through E-Banking: A Qualitative Analysis of Syariah-Compliant Financial Transactions." *Indonesian Journal of Law and Economics Review* 18, no. 3 (2023): 6–14. https://doi.org/10.21070/ijler.v18i3.934.

Purwanto, Agus, and Yuli Sudargini. "Partial Least Squares Structural Squation Modeling (PLS-SEM) Analysis for Social and Management Research : A Literature Review." *Journal of Industrial Engineering & Management Research* 2, no. 4 (2021): 114–23.

Riza, Alex Fahrur, and Dwi Marlina Wijayanti. "Strengthening a Sustainable Islamic Financial Industry through Digital Banking." *Journal of Islamic Marketing* 15, no. 11 (June 3, 2024): 2732–58. https://doi.org/10.1108/JIMA-01-2023-0025.

Rogers, Ronald W. "A Protection Motivation Theory of Fear Appeals and Attitude Change1." *The Journal of Psychology* 91, no. 1 (1975): 93–114. https://doi.org/10.1080/00223980.1975.9915803.

Sylvester, F. Ley. "Mobile Device Users' Susceptibility to Phishing Attacks." *International Journal of Computer Science and Information Technology* 14, no. 1 (2022): 1–18. https://doi.org/10.5121/ijcsit.2022.14101.

Tambariki, Canitgia, Octavianie Bernadette Sondakh, Virgino Agassie Dondokambey, and Evelyn Hendriana. "Drivers of Banking Consumers' Cybersecurity Behavior:

Applying the Extended Protection Motivation Theory." *GATR Journal of Management and Marketing Review* 9, no. 1 (2024): 01–12. https://doi.org/10.35609/jmmr.2024.9.1(1).

Tavakol, Mohsen, and Reg Dennick. "Making Sense of Cronbach's Alpha." *International Journal of Medical Education* 2 (2011): 53–55. https://doi.org/10.5116/ijme.4dfb.8dfd.

Vardari, Luan, and Kujtim Hameli. "Perceived Benefits, Trust and Social Influence in FinTech: Pathways to Adoption and Satisfaction in a Developing Economy." *Global Knowledge, Memory and Communication*, September 11, 2025. https://doi.org/10.1108/GKMC-02-2025-0137.

Zhang, Zizhong, and Xiaoxue Zhang. "Why Not Use Facial Recognition Payment? From the Perspective of the Extended Protection Motivation Theory." *Journal of Retailing and Consumer Services* 81 (2024). https://doi.org/10.1016/j.jretconser.2024.104016.

Appendix

A. Outer Loadings of Final Measurement Model

Indicators	Outer loadings
PV2 <- Perceived Vulnerability	0.882
PV1 <- Perceived Vulnerability	0.897
PS4 <- Perceived Severity	0.812
PS3 <- Perceived Severity	0.802
PS2 <- Perceived Severity	0.789
PS1 <- Perceived Severity	0.727
SI4 <- Social Influence	0.757
SI3 <- Social Influence	0.730
SI2 <- Social Influence	0.754
SI1 <- Social Influence	0.795
SE3 <- Self Efficacy	0.824
SE2 <- Self Efficacy	0.876
SE1 <- Self Efficacy	0.824
RE4 <- Response Efficacy	0.850
RE3 <- Response Efficacy	0.877
RE2 <- Response Efficacy	0.796
RE1 <- Response Efficacy	0.847
RC4 <- Response Cost	0.796
RC3 <- Respon Cost	0.773
RC2 <- Response Cost	0.802
RC1 <- Response Cost	0.829
PB7 <- *Protection Behavior*	0.829
PB6 <- *Protection Behavior*	0.826
PB5 <- *Protection Behavior*	0.812
PB4 <- *Protection Behavior*	0.831
PB3 <- *Protection Behavior*	0.796
PB2 <- *Protection Behavior*	0.767

PB1 <- *Protection Behavior*	0.747
Cybersecurity Education x Social Influence -> Cybersecurity Education x Social Influence	1.000
Cybersecurity Education x Self Efficacy -> Cybersecurity Education x Self Efficacy	1.000
Cybersecurity Education x Response Efficacy -> Cybersecurity Education x Response Efficacy	1.000
Cybersecurity Education x Response Cost -> Cybersecurity Education x Response Cost	1.000
Cybersecurity Education x Perceived Vulnerability -> Cybersecurity Education x Perceived Vulnerability	1.000
Cybersecurity Education x Perceived Severity -> Cybersecurity Education x Perceived Severity	1.000
EKS5 <- Cybersecurity Education	0.717
EKS4 <- Cybersecurity Education	0.810
EKS3 <- Cybersecurity Education	0.785
EKS2 <- Cybersecurity Education	0.728
EKS1 <- Cybersecurity Education	0.759

Indicators	**Outer loadings**
EKS1 <- Cybersecurity Education	0.755
EKS2 <- Cybersecurity Education	0.723
EKS3 <- Cybersecurity Education	0.784
EKS4 <- Cybersecurity Education	0.812
EKS5 <- Cybersecurity Education	0.721
PB1 <- *Protection Behavior*	0.753
PB2 <- *Protection Behavior*	0.757
PB4 <- *Protection Behavior*	0.834
PB5 <- *Protection Behavior*	0.834
PB6 <- *Protection Behavior*	0.830
PB7 <- *Protection Behavior*	0.843
PS1 <- Perceived Severity	0.760
PS2 <- Perceived Severity	0.807
PS3 <- Perceived Severity	0.825
PV1 <- Perceived Vulnerability	0.895
PV2 <- Perceived Vulnerability	0.883
RC1 <- Response Cost	0.885
RC2 <- Response Cost	0.880
RE1 <- Response Efficacy	0.848
RE2 <- Response Efficacy	0.794
RE3 <- Response Efficacy	0.876
RE4 <- Response Efficacy	0.851
SE1 <- Self Efficacy	0.821
SE2 <- Self Efficacy	0.876

SE3 <- Self Efficacy	0.827
SI1 <- Social Influence	0.795
SI2 <- Social Influence	0.757
SI3 <- Social Influence	0.728
SI4 <- Social Influence	0.756
Cybersecurity Education x Response Efficacy -> Cybersecurity Education x Response Efficacy	1.000
Cybersecurity Education x Perceived Severity -> Cybersecurity Education x Perceived Severity	1.000
Cybersecurity Education x Self Efficacy -> Cybersecurity Education x Self Efficacy	1.000
Cybersecurity Education x Response Cost -> Cybersecurity Education x Response Cost	1.000
Cybersecurity Education x Social Influence -> Cybersecurity Education x Social Influence	1.000
Cybersecurity Education x Perceived Vulnerability -> Cybersecurity Education x Perceived Vulnerability	1.000

B. Composite Reliability (CR) of Constructs

Variable	Composite reliability (rho_c)
Cybersecurity Education	0.872
Perceived Severity	0.840
Perceived Vulnerability	0.883
Protection Behavior	0.919
Response Cost	0.875
Response Efficacy	0.907
Self Efficacy	0.879
Social Influence	0.845

C. Internal Consistency Measures (Cronbach's Alpha)

Variable	Cronbach's alpha
Cybersecurity Education	0.820
Perceived Severity	0.716
Perceived Vulnerability	0.735
Protection Behavior	0.894
Response Cost	0.715
Response Efficacy	0.864
Self Efficacy	0.794
Social Influence	0.755

D. AVE

Variable	Average variance extracted (AVE)
Perceived Vulnerability	0.791

Perceived Severity	0.636
Self Efficacy	0.709
Response Efficacy	0.710
Response Cost	0.778
Social Influence	0.577
Cybersecurity Education	0.577
Protection Behavior	0.655

E. HTMT

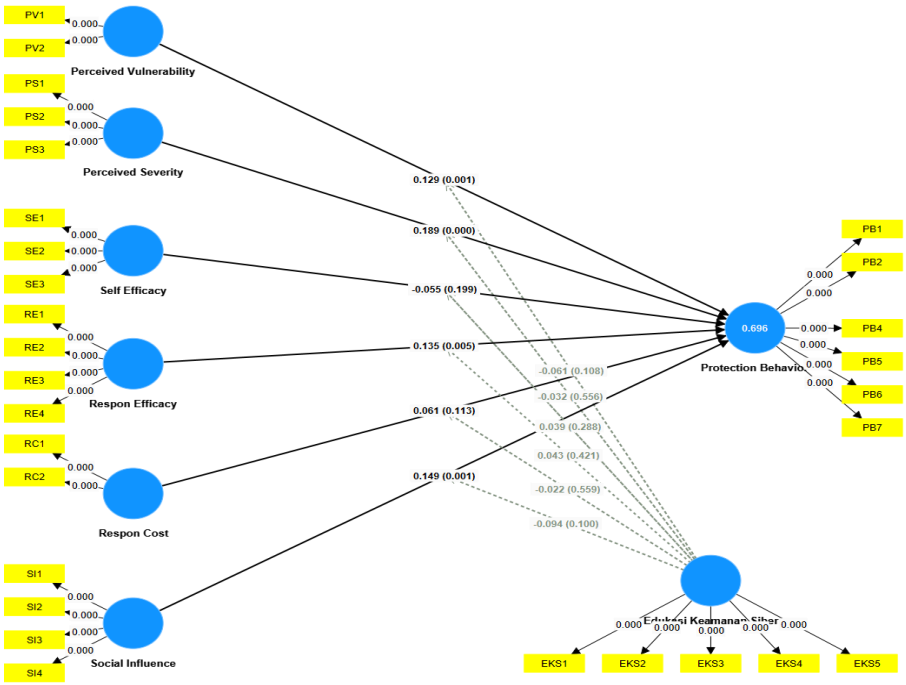
Variable	EKS	PS	PV	PB	RC	RE	SE	SI	EKSx PV	EKSx PS	EKSx SE	EKSx RE	EKSx RC	EKSx SI
EKS														
PS	0.747													
PV	0.566	0.762												
PB	0.840	0.825	0.679											
RC	0.765	0.737	0.555	0.722										
RE	0.747	0.754	0.659	0.757	0.812									
SE	0.835	0.736	0.657	0.702	0.798	0.820								
SI	0.888	0.807	0.658	0.839	0.770	0.786	0.803							
EKSxPV	0.074	0.140	0.090	0.173	0.062	0.187	0.087	0.059						
EKSxPS	0.097	0.237	0.156	0.211	0.066	0.208	0.129	0.074	0.457					
EKSxSE	0.101	0.122	0.092	0.123	0.079	0.134	0.159	0.035	0.446	0.479				
EKSxRE	0.125	0.204	0.203	0.223	0.094	0.315	0.141	0.133	0.541	0.594	0.648			
EKSxRC	0.077	0.083	0.063	0.122	0.069	0.084	0.078	0.054	0.294	0.456	0.563	0.602		
EKSxSI	0.079	0.065	0.063	0.194	0.057	0.129	0.021	0.149	0.412	0.596	0.541	0.638	0.539	

F. VIF

Indicator	VIF
EKS1	1.894
EKS2	1.864
EKS3	1.966
EKS4	1.824
EKS5	1.385
PB1	1.856
PB2	1.839
PB4	2.567
PB5	2.509
PB6	2.327
PB7	2.396
PS1	1.358
PS2	1.474
PS3	1.393
PV1	1.510
PV2	1.510
RC1	1.448

RC2	1.448
RE1	2.075
RE2	1.801
RE3	2.419
RE4	2.027
SE1	1.609
SE2	1.931
SE3	1.644
SI1	1.602
SI2	1.441
SI3	1.392
SI4	1.412
Cybersecurity Education *x Respon Efficacy*	1.000
Cybersecurity Education *x Perceived Severity*	1.000
Cybersecurity Education *x Self Efficacy*	1.000
Cybersecurity Education *x Respon Cost*	1.000
Cybersecurity Education *x Social Influence*	1.000
Cybersecurity Education *x Perceived Vulnerability*	1.000

G. Path Coeficients



H. Coeficients Determinant

	R-square	R-square adjusted
Protection Behavior	0.696	0.685

I. Effect Size

	f-square
Cybersecurity Education -> *Protection Behavior*	0.171
Perceived Severity -> *Protection Behavior*	0.055
Perceived Vulnerability -> *Protection Behavior*	0.033
Respon Cost -> *Protection Behavior*	0.006
Respon Efficacy -> *Protection Behavior*	0.020
Self Efficacy -> *Protection Behavior*	0.004
Social Influence -> *Protection Behavior*	0.027
Cybersecurity Education x Perceived Vulnerability -> *Protection Behavior*	0.008
Cybersecurity Education x Perceived Severity -> *Protection Behavior*	0.001
Cybersecurity Education x Self Efficacy -> *Protection Behavior*	0.002
Cybersecurity Education x Respon Efficacy -> *Protection Behavior*	0.002
Cybersecurity Education x Respon Cost -> *Protection Behavior*	0.001
Cybersecurity Education x Social Influence -> *Protection Behavior*	0.012

J. Predictive Relevance

	Q^2predict
PB1	0.393
PB2	0.386
PB4	0.427
PB5	0.422
PB6	0.475
PB7	0.492

K. PLSPredict

	PLS-SEM_RMSE	PLS-SEM_MAE	LM_RMSE	LM_MAE
PB1	0.560	0.467	0.568	0.458
PB2	0.611	0.507	0.620	0.493
PB4	0.560	0.431	0.558	0.425
PB5	0.556	0.431	0.550	0.430
PB6	0.550	0.444	0.570	0.446
PB7	0.521	0.410	0.528	0.417

L. Model Fit

	PLS-SEM_RMSE	PLS-SEM_MAE	LM_RMSE	LM_MAE
PB1	0.560	0.467	0.568	0.458
PB2	0.611	0.507	0.620	0.493
PB4	0.560	0.431	0.558	0.425
PB5	0.556	0.431	0.550	0.430
PB6	0.550	0.444	0.570	0.446
PB7	0.521	0.410	0.528	0.417