# PROTECTIVE TRANSACTION BEHAVIOR IN PPOB SERVICES USING PROTECTION MOTIVATION THEORY

**Haikal Saputra[1*], Khairul Imtihan[2], Mardi[3]**

[1*,2,3]Department of Information Systems, STMIK Lombok, Praya, Lombok Tengah, Indonesia
Jln. Basuki Rahmat No.105 Praya Lombok Tengah 83511

[1*]haikalsapoetra1@gmail.com, [2]khairulimtihan31@gmail.com, [3]mardisambelia@gmail.com

## Abstract

*Routine Payment Point Online Bank (PPOB) transactions require users to make security decisions that are not fully addressed by technology acceptance and satisfaction research. This study examines the associations of threat and coping appraisals with protection intention and self-reported protective transaction behavior using Protection Motivation Theory (PMT). A cross-sectional survey of 489 PPOB users in West Nusa Tenggara, Indonesia, was analyzed using partial least squares structural equation modeling (PLS-SEM). The model explained 52.0% of the variance in protection intention and 54.9% in protective transaction behavior. Response efficacy was the strongest positive predictor of protection intention (β = 0.372, p < 0.001), followed by perceived severity (β = 0.133). Perceived vulnerability and security self-efficacy were not statistically significant. Response cost exhibited an unexpected positive association (β = 0.295, p < 0.001), contradicting the hypothesized negative direction. Protection intention was strongly associated with reported protective behavior (β = 0.741, p < 0.001). Significant indirect associations through protection intention were observed for response efficacy, response cost, and perceived severity. The findings suggest prioritizing clear explanations of effective security precautions in PPOB services. Interpretation remains constrained by cross-sectional self-reports and insufficient discriminant validity between severity and vulnerability (HTMT = 0.939).*

**Keywords:** PPOB; Protection Motivation Theory; Transaction Security; Protection Intention; Protective Behavior.

## Abstrak

Transaksi melalui layanan Payment Point Online Bank (PPOB) menuntut pengguna mengambil keputusan keamanan yang belum sepenuhnya dijelaskan oleh penelitian penerimaan teknologi dan kepuasan pengguna. Penelitian ini menguji hubungan penilaian ancaman dan kemampuan penanggulangan dengan niat perlindungan serta perilaku perlindungan transaksi yang dilaporkan pengguna berdasarkan Protection Motivation Theory (PMT). Data survei cross-sectional dari 489 pengguna PPOB di Nusa Tenggara Barat dianalisis menggunakan partial least squares structural equation modeling (PLS-SEM). Model menjelaskan 52,0% varians niat perlindungan dan 54,9% varians perilaku perlindungan transaksi. Efektivitas tindakan perlindungan menunjukkan hubungan positif terkuat dengan niat perlindungan (β = 0,372, p < 0,001), diikuti persepsi keseriusan ancaman (β = 0,133). Persepsi kerentanan dan efikasi diri keamanan tidak menunjukkan hubungan signifikan. Biaya respons justru berhubungan positif (β = 0,295, p < 0,001), berlawanan dengan hipotesis negatif. Niat perlindungan berhubungan kuat dengan perilaku perlindungan yang dilaporkan (β = 0,741, p < 0,001). Hubungan tidak langsung yang signifikan melalui niat perlindungan ditemukan untuk efektivitas respons, biaya respons, dan persepsi keseriusan ancaman. Temuan ini mendukung pentingnya penjelasan yang jelas mengenai efektivitas langkah keamanan PPOB. Interpretasi tetap dibatasi oleh desain survei satu periode, data laporan diri, serta validitas diskriminan yang belum memadai antara keseriusan ancaman dan kerentanan (HTMT = 0,939).

**Kata kunci:** PPOB; Teori Motivasi Perlindungan; Keamanan Transaksi; Niat Perlindungan; Perilaku Perlindungan.

## 1. INTRODUCTION

The expansion of digital payment services has transformed how individuals conduct routine financial transactions, creating new opportunities for accessibility, efficiency, and financial inclusion. In Indonesia, this transformation has been accompanied by substantial growth in digital payment activities. Bank Indonesia [1] reported that digital payment transaction volume reached 4.66 billion transactions in November 2025, representing a year-on-year increase of 41.12%. The growing integration of digital payments into everyday financial activities has also heightened the importance of transaction security and consumer protection. According to the Financial Services Authority of Indonesia [2], the Indonesia Anti-Scam Centre received 343,402 fraud reports between November 2024 and November 2025, reflecting broader concerns about financial fraud across the digital financial ecosystem. Although these figures do not specifically represent Payment Point Online Bank (PPOB) incidents, they underscore the importance of understanding how individuals recognize transaction-related threats and respond through appropriate protective practices.

PPOB-based digital transaction services constitute an important part of this evolving payment environment by facilitating routine transactions, including mobile credit purchases, electricity payments, internet and water utility bills, installment payments, and electronic wallet top-ups. These services may be accessed through dedicated applications, digital payment platforms, or agent-assisted channels, allowing users to complete different financial obligations through interconnected transaction mechanisms. Their routine and multifaceted characteristics introduce security considerations that extend beyond service accessibility and transaction convenience. Users may encounter suspicious payment links, unauthorized requests for authentication credentials, misleading payment information, or potential account misuse. Consequently, safe participation in PPOB services depends not only on technological safeguards implemented by service providers but also on users' decisions to verify transaction information, protect authentication credentials, and recognize potentially fraudulent activities.

Existing research on digital financial services has predominantly examined technological acceptance, perceived usefulness, service quality, trust, satisfaction, and continued usage. These perspectives have provided substantial insights into the factors associated with favorable evaluations of digital payment platforms. For example, Ansori and Nugroho [3] demonstrated the importance of security-related perceptions and trust in explaining the continuance usage intention of Indonesian mobile payment users. However, favorable perceptions of a service do not necessarily establish whether individuals consistently undertake protective actions when facing transaction-related threats. Trust in a payment provider and confidence in one's own ability to identify fraudulent activities represent different dimensions of digital financial engagement. Similarly, satisfaction or an intention to continue using a service should not be treated as evidence that users verify payment recipients, protect authentication information, or review transaction records. These distinctions highlight the need to examine protective security behavior as an outcome in its own right rather than treating security exclusively as an antecedent of technology acceptance or service continuance.

Protection Motivation Theory (PMT) provides a theoretical foundation for examining the cognitive evaluations associated with such behavior. Initially proposed by Rogers [4] and subsequently extended by Maddux and Rogers [5], PMT explains protective motivation through the interrelated processes of threat appraisal and coping appraisal. Threat appraisal concerns the perceived severity of adverse consequences and the perceived likelihood of experiencing a threat. Coping appraisal involves beliefs about the effectiveness of protective responses, individuals' confidence in their ability to perform those responses, and the associated costs or inconveniences. Applied to PPOB transactions, these evaluations may influence whether users intend to implement security practices such as verifying official service channels, checking payment information, safeguarding personal identification numbers and one-time passwords, and avoiding suspicious transaction links. The theory therefore offers a basis for examining how perceived threats and protective capabilities are associated with intentions and reported security practices within routine digital financial activities.

Previous cybersecurity research has provided empirical support for the relevance of PMT, although the relative importance of its components varies across behavioral and technological settings. Johnston and Warkentin [6] demonstrated that security-related beliefs, including response efficacy and self-efficacy, contribute to individuals' intentions to comply with recommended protective actions. Ifinedo [7] similarly incorporated PMT into an explanatory model of information security policy compliance. More recently, Kiran et al. [8] investigated cybersecurity behaviors involving computers and smartphones and identified threat severity, response efficacy, and self-efficacy as relevant explanatory factors. Karayel and Saygılı [9] further examined smartphone security intentions across operating systems, revealing differences in how threat and coping appraisals relate to protective motivation. These studies indicate that PMT offers a useful theoretical framework for understanding

cybersecurity behavior, while also suggesting that relationships among its constructs may depend on the characteristics of the technology, users, and security activities under investigation.

Evidence from financial service environments further illustrates the contextual variability of protective motivation. Alrawhani et al. [10] examined information security policy compliance among banking employees and found significant relationships involving perceived severity, response efficacy, and self-efficacy, whereas perceived vulnerability and response cost were not statistically significant. In a related but distinct financial context, Seini et al. [11] investigated security behavior and continuance usage in Ghanaian mobile money services, demonstrating the relevance of protective efficacy beliefs to secure service use. These studies establish that PMT is not limited to general computer security and has already been applied to financial technologies. Nevertheless, organizational security compliance, smartphone protection, and mobile money continuance represent different behavioral settings. Their findings cannot automatically establish how threat appraisal and coping appraisal are associated with protective practices among customers conducting multiple categories of routine PPOB transactions.

Three interconnected research issues therefore warrant further investigation. First, the contextual applicability of PMT requires examination within PPOB services, where transaction verification, authentication protection, and the identification of suspicious payment information are embedded in recurring financial activities. Findings obtained from employees complying with institutional security policies or individuals securing personal devices may not directly reflect the considerations of customers protecting individual financial transactions. Second, the relationships between threat appraisal, coping appraisal, and protective behavior remain empirically heterogeneous. In particular, the relative contributions of perceived vulnerability, security self-efficacy, and response cost require further examination rather than assuming that their relationships will be uniform across digital payment environments. Third, the distinction between protection intention and protective behavior deserves explicit attention. While individuals may recognize the importance of security precautions and intend to perform them, this does not necessarily establish the extent to which those precautions are implemented during routine transactions.

The third issue also has important methodological implications. Much of the empirical literature on cybersecurity behavior relies on self-reported intentions or practices rather than independently observed actions. Van 't Hoff-de Goede et al. [12], using a population-based survey experiment, demonstrated substantial differences between self-reported protective online behavior and actual behavior. Their findings highlight the need to distinguish perceived capability, behavioral intention, and reported action when evaluating security-related conduct. Accordingly, examining the relationship between protection intention and self-reported protective transaction behavior may provide useful explanatory evidence, but such evidence should not be interpreted as direct verification of secure transactions or as proof that protective intentions cause subsequent behavior.

Against this background, the present study develops and evaluates a PMT-based conceptual model to examine protective transaction behavior among PPOB users in West Nusa Tenggara, Indonesia. The model incorporates five antecedent constructs-Perceived Severity, Perceived Vulnerability, Response Efficacy, Security Self-Efficacy, and Response Cost-and examines their relationships with Protection Intention. Protection Intention is subsequently specified as an antecedent of Protective Transaction Behavior, while its role as an indirect pathway between the five PMT constructs and reported protective behavior is also evaluated. Using cross-sectional questionnaire data from 489 PPOB users, the proposed relationships are examined through Partial Least Squares Structural Equation Modeling (PLS-SEM).

This study seeks to answer three related questions: how are threat appraisal and coping appraisal associated with protection intention among PPOB users; which of these appraisals demonstrate meaningful relationships with users' protective motivation; and to what extent is protection intention associated with self-reported protective transaction behavior? The study makes three intended contributions. First, it extends the contextual examination of PMT to a multifaceted digital payment setting in which users encounter different transaction types and security requirements. Second, it examines the distinct relationships of threat appraisal and coping appraisal with protection intention while explicitly distinguishing intention from self-reported protective behavior. Third, it provides an empirical basis for identifying security-related perceptions that may inform user education, transaction verification guidance, and the design of more understandable protective procedures in PPOB services. By focusing on protective transaction practices rather than technology acceptance or continuance intention, the study offers a complementary perspective on the human factors associated with cybersecurity in everyday digital financial transactions.

## 2. RESEARCH METHODOLOGY

### 2.1 Research Design

This study employed a quantitative explanatory design using a cross-sectional questionnaire survey to examine the factors associated with protective security behavior among users of Payment Point Online Bank (PPOB)-based digital transaction services. The research was grounded in Protection Motivation Theory (PMT), which provides a theoretical framework for understanding individuals' protective responses to perceived threats through threat appraisal and coping appraisal [4], [5]. The quantitative approach was adopted to examine the proposed relationships among security-related perceptions, protection intention, and self-reported protective transaction behavior. Partial Least Squares Structural Equation Modeling (PLS-SEM) was selected because the research involved multiple latent constructs, simultaneous structural relationships, and the examination of specific indirect effects. This approach supports the assessment of measurement quality and the estimation of relationships within an integrated explanatory model [13], [14], [15], [16].

The study focused on individual users who had experience conducting transactions through PPOB-based digital services. PPOB transactions encompass routine financial activities, including mobile credit purchases, electricity payments, internet bills, e-wallet top-ups, and other digital payment services. Such transactions provide a relevant context for examining protective security practices because users may encounter threats involving fraudulent payment information, unauthorized account access, suspicious transaction links, and misuse of authentication credentials. The unit of analysis was the individual PPOB user rather than the service provider or transaction platform. The study examined respondents' perceptions and reported security practices at a single observation period. Accordingly, the structural relationships were interpreted as theoretically specified statistical associations rather than evidence of causal effects[17], [18] .

### 2.2 Conceptual Framework and Hypotheses Development

The conceptual framework was developed by adapting Protection Motivation Theory to the security context of PPOB-based digital transactions. PMT was originally introduced to explain how individuals respond to perceived threats and was subsequently extended to incorporate beliefs regarding their ability to undertake protective actions [4], [5]. The theory distinguishes between two primary cognitive appraisal processes. Threat appraisal concerns individuals' evaluations of the seriousness of potential adverse consequences and their perceived likelihood of experiencing those consequences. Coping appraisal concerns evaluations of the effectiveness, feasibility, and perceived costs of protective responses.

Previous information security research has demonstrated the relevance of these appraisal processes in understanding security-related intentions and behavior. Johnston and Warkentin [6] examined how threat-related communications and protective beliefs were associated with information security behavior. Ifinedo [7] subsequently incorporated PMT into an explanatory model of information security policy compliance, while Vance et al. [19] examined the contribution of protection motivation and habitual security practices. More recently, Kiran et al. [8] investigated the explanatory and predictive capabilities of PMT in cybersecurity behavior involving computers and smartphones.

Building on these theoretical foundations, the present study specified seven constructs: Perceived Severity (SEV), Perceived Vulnerability (VUL), Response Efficacy (REF), Security Self-Efficacy (SSE), Response Cost (RCO), Protection Intention (PIN), and Protective Transaction Behavior (PTB). Perceived Severity represents users' assessments of the potential seriousness of security-related consequences, whereas Perceived Vulnerability reflects their subjective likelihood of experiencing digital transaction threats. Both constructs represent the threat appraisal component of PMT. Users who perceive security incidents as serious or consider themselves susceptible to such incidents were expected to report stronger intentions to undertake protective actions. Accordingly, positive relationships were hypothesized between Perceived Severity and Protection Intention (H1) and between Perceived Vulnerability and Protection Intention (H2).

The coping appraisal component was represented by Response Efficacy, Security Self-Efficacy, and Response Cost. Response Efficacy refers to users' beliefs that recommended security measures can effectively reduce transaction-related threats. Security Self-Efficacy concerns users' confidence in their ability to implement those measures, including identifying suspicious messages, verifying transaction information, and protecting authentication credentials. Both constructs were hypothesized to have positive relationships with Protection Intention (H3 and H4, respectively).

Response Cost reflects the perceived time, effort, inconvenience, and practical burden associated with implementing transaction security measures. Consistent with PMT, greater perceived protection costs were expected to be associated with weaker intentions to undertake protective actions. Therefore, a negative

relationship between Response Cost and Protection Intention was hypothesized (H5).

Protection Intention was positioned as the immediate antecedent of Protective Transaction Behavior. Within this framework, intention reflects users' willingness and plans to implement security practices, whereas behavior represents protective actions they report having performed during PPOB transactions. A positive relationship between Protection Intention and Protective Transaction Behavior was hypothesized (H6).

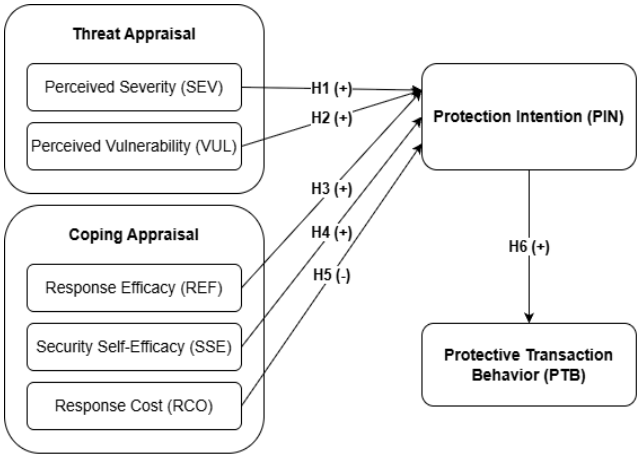



**Figure 1.** Proposed conceptual framework based on Protection Motivation Theory.

Figure 1 illustrates the proposed conceptual framework, comprising five antecedent relationships with Protection Intention and one relationship linking Protection Intention to Protective Transaction Behavior. The model also specifies Protection Intention as the indirect pathway through which the five PMT antecedents are associated with Protective Transaction Behavior. No direct relationships from these antecedents to Protective Transaction Behavior were included in the estimated model.

### 2.3 Questionnaire Development and Measurement

The research instrument was structured around seven constructs operationalized through 28 measurement indicators, with four indicators assigned to each construct. The conceptual definitions and measurement content were informed by established PMT research and previous applications in information security and cybersecurity behavior [6], [7], [8]. The indicator statements were contextualized to reflect protective security practices associated with PPOB-based digital transactions. The measurement items addressed three conceptually distinct areas: threat-related perceptions, evaluations of protective responses, and security-related intention and behavior.

Threat appraisal was measured using Perceived Severity and Perceived Vulnerability. The Perceived Severity indicators assessed the seriousness of potential financial losses, unauthorized account use, personal data breaches, and manipulated payment information. Perceived Vulnerability measured users' subjective susceptibility to fraudulent transactions, authentication misuse, suspicious payment links, and other digital transaction threats. Coping appraisal was measured using Response Efficacy, Security Self-Efficacy, and Response Cost. Response Efficacy assessed the perceived effectiveness of verifying official transaction channels, checking payment information, protecting authentication credentials, and avoiding suspicious payment links. Security Self-Efficacy measured respondents' perceived capability to identify suspicious digital payment activities and implement appropriate security responses. Response Cost captured the additional time, effort, inconvenience, and reduced practicality associated with performing protective security procedures.

Protection Intention was operationalized through four indicators assessing respondents' intentions to use verified PPOB channels, recheck payment information, protect authentication credentials, and verify the authenticity of transaction-related messages or links during future transactions. Protective Transaction Behavior was assessed through four indicators referring to security practices reported during the preceding three months. These practices included using official PPOB channels, checking payment recipients and transaction amounts, maintaining the confidentiality of PINs and one-time passwords, and reviewing transaction records for unauthorized activities.

The distinction between Protection Intention and Protective Transaction Behavior was maintained through their temporal reference and measurement focus. Intention items addressed respondents' plans or commitments regarding future security practices, whereas behavioral items concerned actions reported for the preceding three months. The behavioral measure therefore represented self-reported protective practices rather than independently observed security behavior. In the estimated PLS-SEM specification, all seven constructs were treated as reflectively measured latent variables. The measurement items and corresponding outer loadings are presented in Table 1 of the Results section.

### 2.4 Population and Data Collection

The population of interest comprised individuals with experience using PPOB-based digital transaction services in West Nusa Tenggara, Indonesia. Data were collected through a questionnaire survey conducted between March and June 2026. Following data screening, 489 valid responses were retained for the final analysis. The respondents were drawn from different localities within West Nusa Tenggara, providing a study context encompassing users with

varied backgrounds and experiences of PPOB-based transactions. The unit of analysis remained the individual user, with attention directed toward security-related perceptions, protection intention, and reported protective practices.

The analytical sample consisted of the 489 respondents included in the PLS-SEM estimation. As the study employed a cross-sectional design, all constructs were evaluated using information collected during a single survey period.

### 2.5 Data Analysis Procedures

Data analysis was conducted using Partial Least Squares Structural Equation Modeling (PLS-SEM) with SmartPLS. The analytical procedure followed a two-stage approach comprising measurement model assessment and structural model assessment, consistent with established PLS-SEM reporting recommendations [20], [21], [22], [23].

#### 2.5.1 Measurement Model Assessment

The measurement model was evaluated to examine indicator reliability, internal consistency reliability, convergent validity, and discriminant validity. Indicator reliability was assessed using standardized outer loadings. Values of approximately 0.708 or higher were considered desirable because they indicate that the latent construct explains at least half of an indicator's variance. Internal consistency reliability was examined using Cronbach's alpha, composite reliability rho_a, and composite reliability rho_c. Coefficients of at least 0.70 were considered acceptable, while values substantially above 0.95 would suggest potential redundancy among indicators.

Convergent validity was assessed using Average Variance Extracted (AVE). An AVE of at least 0.50 was used as the criterion for determining whether a construct explained a sufficient proportion of the variance in its indicators. Discriminant validity was evaluated primarily using the heterotrait–monotrait ratio (HTMT), following Henseler et al. [24]. A threshold of 0.85 was considered conservative, whereas 0.90 was used as a more permissive criterion for theoretically related constructs. The HTMT assessment was supplemented by inspection of the Fornell–Larcker criterion and indicator cross-loadings. The measurement assessment was intended to identify whether the specified indicators adequately represented their corresponding constructs and whether the constructs could be empirically distinguished. The results of these assessments are reported in Tables 1–3.

#### 2.5.2 Structural Model Assessment

After examining the measurement properties, the structural model was assessed to estimate the relationships specified in the conceptual framework. Collinearity among predictor constructs was evaluated using inner variance inflation factors (VIF). Values below 5.0 were considered indicative of the absence of severe collinearity, while estimates exceeding the more conservative benchmark of 3.0 were examined with additional caution. The model's explanatory power was evaluated using the coefficient of determination ($R^2$) and adjusted $R^2$ for the endogenous constructs, Protection Intention and Protective Transaction Behavior. These statistics were used to determine the proportion of variance accounted for by the respective predictors.

The incremental contribution of each exogenous construct was examined using effect size $f^2$, with conventional benchmarks of 0.02, 0.15, and 0.35 representing small, medium, and large effects, respectively. Predictive relevance was evaluated using Stone–Geisser's $Q^2$ obtained through the blindfolding procedure. Positive $Q^2$ values were interpreted as evidence of cross-validated predictive relevance under this procedure. However, this assessment was distinguished from out-of-sample predictive evaluation, which requires additional methods such as PLSpredict. The results of the explanatory power and predictive relevance assessment are presented in Table 4.

#### 2.5.3 Hypothesis Testing

The significance of the proposed structural relationships was evaluated using a nonparametric bootstrapping procedure with 10,000 subsamples. The analysis employed a two-tailed test with a significance level of 0.05. Standardized path coefficients (β), t-statistics, p-values, and 95% bias-corrected and accelerated (BCa) bootstrap confidence intervals were used to evaluate the structural relationships. A relationship was considered statistically significant when the corresponding two-tailed p-value was below 0.05 and its 95% confidence interval excluded zero.

Hypothesis decisions were based on both statistical significance and consistency between the observed coefficient direction and the direction specified in the original hypothesis. Consequently, a statistically significant coefficient in the opposite direction was not interpreted as support for the hypothesized relationship. The analysis examined six direct structural relationships: SEV → PIN, VUL → PIN, REF → PIN, SSE → PIN, RCO → PIN, and PIN → PTB. Their estimated coefficients, statistical significance, effect sizes, and collinearity diagnostics are presented in Table 5. The final structural estimates were also summarized visually in Figure 2, which presents the standardized path coefficients and $R^2$ values for the two endogenous constructs.

### 2.5.4 Indirect Effects Analysis

Specific indirect effects were examined to evaluate the relationships between the five PMT antecedents and Protective Transaction Behavior through Protection Intention. The analysis covered five indirect pathways: SEV → PIN → PTB, VUL → PIN → PTB, REF → PIN → PTB, SSE → PIN → PTB, and RCO → PIN → PTB. Statistical inference was based on the bootstrapped specific indirect effect estimates, associated t-statistics and p-values, and 95% BCa confidence intervals obtained from 10,000 bootstrap subsamples. An indirect effect was considered statistically significant when its confidence interval excluded zero. Because the structural model did not include direct paths from the five PMT antecedents to Protective Transaction Behavior, the indirect effect analysis was interpreted within the specified model structure. The absence of those direct paths prevented conclusions regarding full versus partial mediation.

## 3 RESULTS AND DISCUSSION

### 3.1 Measurement Model Assessment

The measurement model was evaluated to establish the reliability and validity of the constructs used to explain protective transaction behavior in Payment Point Online Bank (PPOB) services. The proposed model comprised seven constructs measured using 28 indicators, encompassing perceived severity, perceived vulnerability, response efficacy, security self-efficacy, response cost, protection intention, and protective transaction behavior. The assessment examined indicator reliability, internal consistency reliability, convergent validity, and discriminant validity under the specified reflective measurement model.

### 3.1.1 Indicator Reliability

Indicator reliability was evaluated using standardized outer loadings. As presented in Table 1, the loading values ranged from 0.713 to 0.899, with all 28 indicators exceeding the commonly recommended threshold of 0.708. The lowest loading was observed for VUL4 (0.713), which measures perceived exposure to digital transaction misuse, whereas SSE4 exhibited the highest loading (0.899), reflecting users' perceived ability to respond appropriately to suspicious PPOB-related messages or links. The four indicators within each construct demonstrated acceptable loading values, suggesting that the measurement items adequately represented their assigned constructs under the specified reflective measurement approach. Although VUL4 was relatively close to the minimum threshold, its loading remained acceptable. Accordingly, all indicators were retained in the measurement model.

These findings provide initial evidence of indicator reliability across the threat appraisal, coping appraisal, intention, and behavioral constructs. Nevertheless, satisfactory indicator loadings do not independently establish that conceptually related constructs are empirically distinguishable. This distinction was examined separately through discriminant validity assessment.

TABLE I. MEASUREMENT ITEMS AND OUTER LOADINGS

| Construct | Code | Measurement Items | Outer Loading |
|---|---|---|---|
| Perceived Severity (SEV) | SEV1 | Financial losses resulting from PPOB transaction fraud would have serious consequences for me. | 0.748 |
| | SEV2 | Unauthorized use of my PPOB account could have serious consequences for me. | 0.771 |
| | SEV3 | A personal data breach involving PPOB services could seriously affect me. | 0.858 |
| | SEV4 | Manipulation of PPOB payment information could cause serious problems for me. | 0.848 |
| Perceived Vulnerability (VUL) | VUL1 | I believe I could become a target of fraud when conducting PPOB transactions. | 0.816 |
| | VUL2 | My PPOB account authentication information could potentially be stolen or misused. | 0.844 |
| | VUL3 | I may encounter fraudulent messages or payment links when using PPOB services. | 0.853 |
| | VUL4 | I believe my PPOB transactions could be exposed to digital misuse. | 0.713 |
| Response Efficacy (REF) | REF1 | Verifying the authenticity of PPOB applications or websites effectively reduces transaction fraud risks. | 0.765 |
| | REF2 | Checking payment recipients and transaction amounts effectively reduces the risk of unauthorized transactions. | 0.866 |
| | REF3 | Keeping PINs and OTPs confidential effectively prevents unauthorized access to PPOB accounts. | 0.846 |

| | | | |
|---|---|---|---|
| | REF4 | Avoiding suspicious payment links effectively reduces the risk of PPOB-related fraud. | 0.734 |
| Security Self-Efficacy (SSE) | SSE1 | I am confident in my ability to distinguish legitimate PPOB applications or websites from suspicious ones. | 0.777 |
| | SSE2 | I can identify suspicious requests for PINs or OTPs during PPOB transactions. | 0.891 |
| | SSE3 | I am confident in my ability to verify the authenticity of payment recipient information before confirming PPOB transactions. | 0.891 |
| | SSE4 | I can determine appropriate actions when encountering suspicious PPOB-related messages or links. | 0.899 |
| Response Cost (RCO) | RCO1 | Verifying the authenticity of a PPOB service channel before making a transaction requires additional time. | 0.831 |
| | RCO2 | Rechecking PPOB payment information is inconvenient for me. | 0.872 |
| | RCO3 | Implementing security measures to protect my PPOB account requires considerable effort. | 0.868 |
| | RCO4 | Performing additional security verification makes PPOB transactions less convenient for me. | 0.823 |
| Protection Intention (PIN) | PIN1 | I intend to use verified and legitimate PPOB service channels for future transactions. | 0.871 |
| | PIN2 | I plan to recheck payment information before confirming future PPOB transactions. | 0.873 |
| | PIN3 | I intend to maintain the confidentiality of my PINs and OTPs whenever I use PPOB services. | 0.873 |
| | PIN4 | I plan to verify the authenticity of PPOB-related messages or links before responding to them. | 0.773 |
| Protective Transaction Behavior (PTB) | PTB1 | During the past three months, I have used official PPOB applications or websites when conducting transactions. | 0.871 |
| | PTB2 | During the past three months, I have checked payment recipients and transaction amounts before confirming PPOB transactions. | 0.867 |
| | PTB3 | During the past three months, I have kept my PINs and OTPs confidential when using PPOB services. | 0.893 |
| | PTB4 | During the past three months, I have reviewed my PPOB transaction history to identify unauthorized activities. | 0.769 |
| *Notes:* PPOB = Payment Point Online Bank; SEV = Perceived Severity; VUL = Perceived Vulnerability; REF = Response Efficacy; SSE = Security Self-Efficacy; RCO = Response Cost; PIN = Protection Intention; PTB = Protective Transaction Behavior. Outer loadings were obtained from the PLS-SEM measurement model. The measurement statements represent English adaptations of the Indonesian questionnaire indicators developed for this study. | | | |

### 3.1.2 Internal Consistency Reliability and Convergent Validity

Internal consistency reliability and convergent validity were examined using Cronbach's alpha, composite reliability (rho_a and rho_c), and average variance extracted (AVE). Table 2 presents the results for the seven constructs. Cronbach's alpha values ranged from 0.817 to 0.888, indicating satisfactory internal consistency across the measurement scales. The rho_a coefficients ranged from 0.828 to 0.895, while rho_c values ranged from 0.880 to 0.923. All coefficients exceeded the recommended minimum of 0.70, and none exceeded 0.95, indicating acceptable reliability without evidence of excessive indicator redundancy based on these coefficients.

Convergent validity was evaluated through AVE, which ranged from 0.647 to 0.750. Security Self-Efficacy recorded the highest AVE (0.750), indicating that its indicators shared a relatively high proportion of variance with the intended construct. Response Efficacy exhibited the lowest AVE (0.647), which nevertheless exceeded the minimum criterion of 0.50. The remaining constructs also satisfied this threshold, supporting convergent validity throughout the specified reflective measurement model. Taken together, the reliability and AVE results indicate that the seven constructs achieved satisfactory internal consistency and convergent validity. These findings support the adequacy of the measurement scales in capturing their intended dimensions, although their empirical distinctiveness requires separate consideration.

TABLE II. CONSTRUCT RELIABILITY AND CONVERGENT VALIDITY

| Construct | Cronbach's Alpha (α) | Composite Reliability (rho_a) | Composite Reliability (rho_c) | Average Variance Extracted (AVE) |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| Perceived Severity (SEV) | 0.825 | 0.855 | 0.882 | 0.651 |
| Perceived Vulnerability (VUL) | 0.823 | 0.837 | 0.883 | 0.654 |
| Response Efficacy (REF) | 0.817 | 0.828 | 0.880 | 0.647 |
| Security Self-Efficacy (SSE) | 0.888 | 0.895 | 0.923 | 0.750 |
| Response Cost (RCO) | 0.872 | 0.889 | 0.912 | 0.721 |
| Protection Intention (PIN) | 0.871 | 0.880 | 0.911 | 0.720 |
| Protective Transaction Behavior (PTB) | 0.872 | 0.881 | 0.913 | 0.725 |
| *Notes:* Cronbach's Alpha (α) = Internal consistency reliability; rho_a = Dijkstra–Henseler's reliability coefficient; rho_c = Composite reliability; AVE = Average Variance Extracted. Recommended thresholds: Cronbach's Alpha, rho_a, and rho_c ≥ 0.70; AVE ≥ 0.50. All seven constructs satisfied the specified internal consistency reliability and convergent validity criteria under the reflective measurement model. | | | | |

### 3.1.3 Discriminant Validity

Discriminant validity was assessed using the heterotrait–monotrait ratio (HTMT), which evaluates the extent to which theoretically distinct constructs can be differentiated empirically [24]. As shown in Table 3, HTMT values ranged from 0.472 to 0.939. Of the 21 construct pairs, 19 exhibited values below the conservative threshold of 0.85.

The HTMT value between Response Efficacy and Protective Transaction Behavior was 0.877, exceeding the conservative criterion of 0.85 but remaining below the more permissive threshold of 0.90. This relatively high association suggests that beliefs about the effectiveness of protective measures are closely related to respondents' reported security practices, although the two constructs represent conceptually different aspects of protective behavior. A more substantial concern was identified between Perceived Severity and Perceived Vulnerability, which produced an HTMT value of 0.939. This value exceeded the 0.90 threshold, indicating insufficient discriminant validity between these constructs. The corresponding 95% bias-corrected and accelerated bootstrap confidence interval ranged from 0.890 to 0.981, further indicating uncertainty around an already elevated HTMT estimate.

Despite this limitation, both constructs were retained because they represent theoretically distinct components of threat appraisal within Protection Motivation Theory. Perceived Severity captures the seriousness of potential adverse consequences, whereas Perceived Vulnerability reflects an individual's perceived likelihood of experiencing those consequences. Their theoretical differentiation, however, does not eliminate the empirical overlap detected in the measurement results. The complementary Fornell–Larcker assessment satisfied its conventional criterion, but this finding does not override the HTMT result. Inspection of the cross-loadings also identified two indicators requiring caution. PIN4 loaded slightly more strongly on Protective Transaction Behavior (0.777) than on its assigned construct, Protection Intention (0.773). Similarly, RCO1 exhibited a higher cross-loading on Protective Transaction Behavior (0.876) than its loading on Response Cost (0.831).

The original measurement specification was retained for the subsequent analysis. Nevertheless, the elevated HTMT value and the identified cross-loading patterns indicate that discriminant validity was not fully established across the model. Consequently, the structural relationships, particularly those involving Perceived Severity and Perceived Vulnerability, should be interpreted with this measurement limitation in mind.

TABLE III. DISCRIMINANT VALIDITY USING THE HTMT CRITERION

| **Construct** | **SEV** | **VUL** | **REF** | **SSE** | **RCO** | **PIN** | **PTB** |
|---|---|---|---|---|---|---|---|
| SEV | - | | | | | | |
| VUL | 0.939 | - | | | | | |
| REF | 0.757 | 0.795 | - | | | | |
| SSE | 0.486 | 0.479 | 0.772 | - | | | |
| RCO | 0.623 | 0.645 | 0.824 | 0.721 | - | | |
| PIN | 0.633 | 0.647 | 0.764 | 0.472 | 0.670 | - | |
| PTB | 0.638 | 0.658 | 0.877 | 0.673 | 0.833 | 0.821 | - |

*Notes:* SEV = Perceived Severity; VUL = Perceived Vulnerability; REF = Response Efficacy; SSE = Security Self-Efficacy; RCO = Response Cost; PIN = Protection Intention; PTB = Protective Transaction Behavior. Values below the diagonal represent HTMT estimates. The conservative threshold is 0.85, whereas 0.90 is commonly applied to theoretically related constructs. The bold value (0.939) exceeds the 0.90 criterion, indicating insufficient discriminant validity between SEV and VUL. The italicized value (0.877) exceeds the conservative threshold of 0.85 but remains below 0.90. All values are reported as obtained from SmartPLS.

### 3.2 Structural Model Assessment

Following the measurement model assessment, the structural model was evaluated to examine its explanatory power and the hypothesized relationships among the PMT constructs. The analysis included the coefficients of determination ($R^2$), adjusted $R^2$, cross-validated redundancy ($Q^2$), standardized path coefficients, effect sizes ($f^2$), and inner variance inflation factors (VIF). Statistical significance was evaluated using a bootstrapping procedure with 10,000 subsamples and a two-tailed significance level of 0.05.

#### 3.2.1 Explanatory Power and Predictive Relevance

The explanatory power of the structural model was assessed using $R^2$ and adjusted $R^2$. As reported in Table 4, Protection Intention achieved an $R^2$ of 0.520 and an adjusted $R^2$ of 0.515. These results indicate that Perceived Severity, Perceived Vulnerability, Response Efficacy, Security Self-Efficacy, and Response Cost collectively explained 52.0% of the observed variance in Protection Intention. Protective Transaction Behavior exhibited an $R^2$ of 0.549 and an adjusted $R^2$ of 0.549, indicating that Protection Intention accounted for 54.9% of the variance in respondents' self-reported protective transaction behavior. Both endogenous constructs therefore demonstrated moderate explanatory power within the proposed model.

Predictive relevance was examined using Stone–Geisser's cross-validated redundancy measure obtained through the blindfolding procedure. The $Q^2$ values were positive for both Protection Intention (0.345) and Protective Transaction Behavior (0.393), supporting predictive relevance under this criterion. The positive $Q^2$ values complement the $R^2$ results by indicating that the model demonstrated predictive relevance within the blindfolding assessment. However, they should not be interpreted as evidence of predictive performance on independent or genuinely out-of-sample observations. Such a claim would require additional procedures, including PLSpredict or comparable cross-validated predictive assessments.

Overall, the model explained a meaningful proportion of the variance in both endogenous constructs. Nevertheless, approximately 48.0% of the variance in Protection Intention and 45.1% of the variance in Protective Transaction Behavior remained unexplained, suggesting that additional individual, technological, or contextual factors may contribute to security-related behavior in PPOB services.

TABLE IV. EXPLANATORY POWER AND PREDICTIVE RELEVANCE

| Endogenous Construct | $R^2$ | Adjusted $R^2$ | $Q^2$ |
|---|---|---|---|
| Protection Intention (PIN) | 0.520 | 0.515 | 0.345 |
| Protective Transaction Behavior (PTB) | 0.549 | 0.549 | 0.393 |

*Notes:* $R^2$ = Coefficient of determination; Adjusted $R^2$ = Adjusted coefficient of determination; $Q^2$ = Stone–Geisser's cross-validated redundancy obtained through the blindfolding procedure. Positive $Q^2$ values indicate predictive relevance under the blindfolding criterion. $Q^2$ should not be confused with $Q^2$_predict, which evaluates out-of-sample predictive performance.

#### 3.2.2 Structural Path Relationships and Hypothesis Testing

Figure 2 presents the estimated structural relationships between the PMT constructs, together with the $R^2$ values for Protection Intention and Protective Transaction Behavior. The model specifies five antecedent relationships with Protection Intention and one relationship between Protection Intention and Protective Transaction Behavior. The structural results indicate differences in the magnitude, direction, and statistical significance of the proposed relationships. Response Efficacy emerged as the strongest positive predictor of Protection Intention, followed by Response Cost and Perceived Severity. In contrast, Perceived Vulnerability and Security Self-Efficacy did not demonstrate statistically significant relationships with Protection Intention.

The relationship between Protection Intention and Protective Transaction Behavior was substantially stronger than the other structural paths. This pattern is consistent with the explanatory role assigned to Protection Intention in the proposed model, although its interpretation remains conditional on the cross-sectional and self-reported nature of the data.

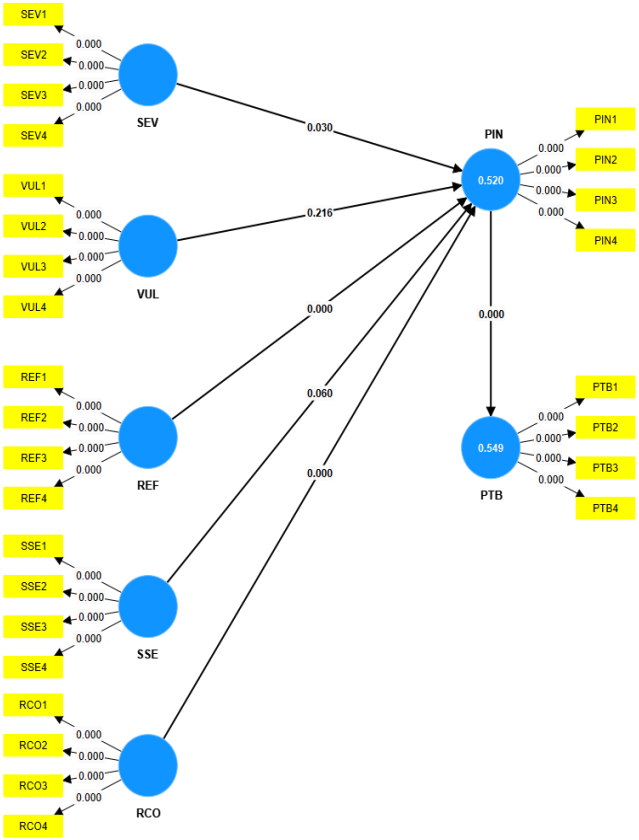



**Figure 2.** PLS-SEM Structural Model Results

The detailed hypothesis testing results are reported in Table 5. Of the six hypothesized relationships, three were supported, whereas three were not supported. Perceived Severity exhibited a positive and statistically significant relationship with Protection Intention (β = 0.133, t = 2.164, p = 0.030), supporting H1. However, the corresponding effect size was below the conventional threshold for a small effect ($f^2$ = 0.013), indicating that its incremental explanatory contribution was limited.

In contrast, Perceived Vulnerability was not significantly associated with Protection Intention (β = 0.082, t = 1.237, p = 0.216, $f^2$ = 0.005). Thus, H2 was not supported. This result suggests that perceived susceptibility to security threats did not provide a statistically distinguishable contribution to protection intention after accounting for the other predictors in the specified model. Response Efficacy demonstrated the strongest positive relationship with Protection Intention (β = 0.372, t = 5.665, p < 0.001). Its effect size was 0.098, indicating a small but meaningful incremental contribution relative to the remaining predictors. Accordingly, H3 was supported. This finding highlights the importance of users' beliefs concerning whether protective measures can effectively mitigate transaction-related security threats.

Security Self-Efficacy exhibited a negative but statistically insignificant relationship with Protection Intention (β = −0.080, t = 1.882, p = 0.060, $f^2$ = 0.007). The result did not support H4. Although the estimated coefficient was negative, its statistical insignificance prevents a conclusion that greater security self-efficacy is associated with lower protection intention in the population represented by the study. An unexpected result emerged for Response Cost. Contrary to the hypothesized negative relationship, Response Cost was positively and significantly associated with Protection Intention (β = 0.295, t = 5.129, p < 0.001, $f^2$ = 0.078). The corresponding 95% bootstrap confidence interval ranged from 0.181 to 0.407, remaining entirely above zero. Consequently, H5 was not supported because the observed direction contradicted the theoretical prediction, despite the relationship being statistically significant.

Finally, Protection Intention exhibited a strong positive relationship with Protective Transaction Behavior (β = 0.741, t = 28.219, p < 0.001). The effect size was substantial ($f^2$ = 1.220), indicating a large incremental contribution to explaining the endogenous behavioral construct. This result supported H6 and represented the strongest structural association in the model. The inner VIF values ranged from 1.000 to 3.034. All values remained below the conventional threshold of 5.0, suggesting no severe collinearity under this criterion. Nevertheless, Perceived Vulnerability exhibited a VIF of 3.034, slightly exceeding the more conservative threshold of 3.0. Together with the elevated HTMT between Perceived Severity and Perceived Vulnerability, this result reinforces the need for caution when interpreting their individual structural contributions.

TABLE V. STRUCTURAL PATH COEFFICIENTS AND HYPOTHESIS TESTING

| Hypothesis / Structural Path | β | t-value | p-value | $f^2$ | VIF | Decision |
|---|---|---|---|---|---|---|
| H1: SEV → PIN (+) | 0.133 | 2.164 | 0.030 | 0.013 | 2.874 | Supported |
| H2: VUL → PIN (+) | 0.082 | 1.237 | 0.216 | 0.005 | 3.034 | Not supported |
| H3: REF → PIN (+) | 0.372 | 5.665 | <0.001 | 0.098 | 2.960 | Supported |
| H4: SSE → PIN (+) | −0.080 | 1.882 | 0.060 | 0.007 | 1.933 | Not supported |
| H5: RCO → PIN (−) | 0.295 | 5.129 | <0.001 | 0.078 | 2.328 | Not supported* |
| H6: PIN → PTB (+) | 0.741 | 28.219 | <0.001 | 1.220 | 1.000 | Supported |

*Notes:* β = Standardized path coefficient; t-value = Bootstrapped t-statistic; p-value = Statistical significance; $f^2$ = Cohen's effect size; VIF = Variance inflation factor. SEV = Perceived Severity; VUL = Perceived Vulnerability; REF = Response Efficacy; SSE = Security Self-Efficacy; RCO = Response Cost; PIN = Protection Intention; PTB = Protective Transaction Behavior. The symbols (+) and (−) indicate the hypothesized directions. Hypotheses were evaluated at the 5% significance level. Conventional $f^2$ benchmarks are 0.02 (small), 0.15 (medium), and 0.35 (large).

### 3.3 Specific Indirect Effects Through Protection Intention

The indirect effects of the five PMT antecedents on Protective Transaction Behavior were examined through Protection Intention using 10,000 bootstrap subsamples and 95% bias-corrected and accelerated confidence intervals. The results, presented in Table 6, revealed three statistically significant indirect relationships. Response Efficacy exhibited the largest positive indirect effect on Protective Transaction Behavior through Protection Intention (β = 0.276, t = 5.277, p < 0.001, 95% BCa CI [0.171, 0.377]). This finding indicates that users' beliefs regarding the effectiveness of protective measures were positively associated with reported security behavior through their protection intention.

Response Cost also demonstrated a positive and statistically significant indirect effect (β = 0.219, t = 4.942, p < 0.001, 95% BCa CI [0.133, 0.309]). Although this relationship was statistically supported, its positive direction remained inconsistent with the negative association originally hypothesized between perceived protection costs and protection intention. Perceived Severity showed a smaller but statistically significant positive indirect effect on Protective Transaction Behavior (β = 0.099, t = 2.173, p = 0.030, 95% BCa CI [0.008, 0.187]). This result indicates that perceived seriousness of security threats was indirectly associated with protective transaction behavior through Protection Intention. In contrast, the indirect effect of Perceived Vulnerability was not statistically significant (β = 0.061, t = 1.239, p = 0.216, 95% BCa CI [−0.035, 0.155]). Similarly, Security Self-Efficacy did not exhibit a significant indirect effect (β = −0.059, t = 1.885, p = 0.059, 95% BCa CI [−0.118, 0.003]). Both confidence intervals included zero. These results identify Protection Intention as the specified indirect pathway connecting selected threat- and coping-appraisal constructs to Protective Transaction Behavior. However, because the model did not estimate direct paths between the five antecedent constructs and Protective Transaction Behavior, the findings do not establish full or partial mediation. Furthermore, the cross-sectional research design does not provide sufficient evidence to infer a causal mediation process.

TABLE VI. SPECIFIC INDIRECT EFFECTS THROUGH PROTECTION INTENTION

| Indirect Path | β | t-value | p-value | 95% BCa CI | Result |
|---|---|---|---|---|---|
| SEV → PIN → PTB | 0.099 | 2.173 | 0.030 | [0.008, 0.187] | Significant |
| VUL → PIN → PTB | 0.061 | 1.239 | 0.216 | [−0.035, 0.155] | Not significant |
| REF → PIN → PTB | 0.276 | 5.277 | <0.001 | [0.171, 0.377] | Significant |
| SSE → PIN → PTB | −0.059 | 1.885 | 0.059 | [−0.118, 0.003] | Not significant |
| RCO → PIN → PTB | 0.219 | 4.942 | <0.001 | [0.133, 0.309] | Significant* |

*Notes:* β = Standardized indirect effect; CI = Confidence interval; BCa = Bias-Corrected and Accelerated bootstrap confidence interval; SEV = Perceived Severity; VUL = Perceived Vulnerability; REF = Response Efficacy; SSE = Security Self-Efficacy; RCO = Response Cost; PIN = Protection Intention; PTB = Protective Transaction Behavior. Indirect effects were evaluated using 10,000 bootstrap subsamples. Statistical significance was established when the 95% BCa confidence interval excluded zero

### 3.4 Discussion of Key Findings

#### 3.4.1 The Role of Response Efficacy in Protective Transaction Behavior

One of the most important findings is the prominent role of Response Efficacy in explaining Protection Intention. Among the five PMT antecedents, Response Efficacy exhibited the strongest positive relationship with Protection Intention (β = 0.372), together with the largest positive indirect association with Protective Transaction Behavior (β = 0.276). This pattern is consistent with the central proposition of Protection Motivation Theory that protective responses depend partly on individuals' beliefs regarding the effectiveness of available countermeasures [4], [5]. Within the PPOB context, users who believe that verifying official payment channels, protecting authentication credentials, and checking transaction information are effective security measures tend to report stronger intentions to implement these practices.

The result is consistent with Johnston and Warkentin [6], who identified response efficacy as an important component of information security

behavioral intentions. More recent evidence from Kiran et al. [8] also supports the relevance of response efficacy in explaining cybersecurity behavior across computer and smartphone contexts. The present findings extend this discussion to PPOB-based digital transaction services, where security precautions involve financial transactions, authentication information, and payment verification. The results suggest that users' assessments of whether protective actions are effective represent a more salient positive correlate of protection intention than their perceived vulnerability or perceived ability to perform those actions.

From a practical perspective, the findings indicate the potential value of communicating not merely which protective actions users should perform, but also why those actions are expected to reduce specific transaction-related risks. For example, security guidance explaining how to verify official payment channels and identify suspicious requests for authentication credentials may be more informative than generic warnings about digital fraud. These remain practice-oriented implications rather than intervention effects demonstrated by the present study.

### 3.4.2 Divergent Roles of Perceived Severity and Perceived Vulnerability

The results reveal different patterns for the two threat appraisal constructs. Perceived Severity was positively associated with Protection Intention, whereas Perceived Vulnerability did not demonstrate a statistically significant relationship. This distinction suggests that, within the estimated model, judgments about the seriousness of potential security consequences were more closely associated with protection intention than subjective assessments of the likelihood of encountering those threats. Users may recognize the potential consequences of fraudulent transactions, account misuse, or personal data exposure without necessarily translating perceived susceptibility into stronger protective intentions.

The absence of a significant vulnerability relationship is not without precedent. Alrawhani et al. [10], in their investigation of information security policy compliance in the banking sector, similarly found that perceived vulnerability did not significantly explain behavioral intention. Nevertheless, their organizational setting differs from the customer-oriented PPOB context examined here, limiting the extent to which the findings can be treated as directly comparable. Importantly, the contrast between severity and vulnerability requires cautious interpretation because these constructs exhibited insufficient discriminant validity (HTMT = 0.939). The overlap suggests that respondents did not clearly distinguish the seriousness of potential consequences from their perceived likelihood of exposure. Accordingly, differences in the estimated structural coefficients cannot be interpreted as definitive evidence that severity is inherently more important than vulnerability.

The findings therefore point to a measurement challenge as well as a substantive research question. Future measurement refinement should distinguish perceived consequences from perceived exposure more explicitly, using transaction-specific situations and cognitively tested questionnaire items.

### 3.4.3 The Unexpected Relationship Between Response Cost and Protection Intention

The positive relationship between Response Cost and Protection Intention represents the most theoretically unexpected finding. Protection Motivation Theory generally assumes that greater perceived costs of adopting protective measures can reduce the motivation to perform them. However, the present study identified a significant positive coefficient ($\beta = 0.295$, $p < 0.001$), accompanied by a positive indirect effect on Protective Transaction Behavior through Protection Intention. This result differs from the originally hypothesized negative association and should not be interpreted as confirmation of the conventional response-cost proposition. Nor does it demonstrate that making security procedures more burdensome will increase users' protective intentions.

One possible interpretation is that users who are highly attentive to transaction security may simultaneously recognize protective procedures as demanding and express stronger intentions to perform them. Under this interpretation, the perceived effort associated with security verification does not necessarily prevent users from valuing protective practices. However, this explanation is exploratory and cannot be established from the available structural coefficients. An alternative possibility concerns the operationalization of Response Cost. The indicators capture perceived additional time, inconvenience, effort, and reduced practicality associated with security procedures. Their interpretation may depend on how respondents distinguish the burden of protective actions from the importance they attach to those actions. The relatively high cross-loading of RCO1 on Protective Transaction Behavior also warrants attention when evaluating the conceptual boundaries of this construct.

Before drawing stronger theoretical conclusions, the direction of the original item coding and the stability of the structural estimates should be verified. Subject to these checks, the positive coefficient can be reported as a context-specific deviation from the hypothesized relationship rather than as evidence requiring a post hoc revision of the original hypothesis.

### 3.4.4 Security Self-Efficacy and the Limits of Perceived Capability

Contrary to the hypothesized positive relationship, Security Self-Efficacy was not significantly associated with Protection Intention. Its estimated coefficient was negative but small (β = −0.080), and the corresponding confidence interval included zero.

This finding differs from cybersecurity research that has identified self-efficacy as a relevant predictor of security-related intentions or behaviors [6], [8]. Alrawhani et al. [10] similarly reported a significant role for self-efficacy in information security compliance intentions among banking employees. In the current PPOB model, respondents' confidence in their ability to identify suspicious links, verify payment information, and recognize unusual authentication requests did not provide a statistically significant unique contribution to Protection Intention after accounting for the other PMT constructs.

The result should not be interpreted as evidence that security competence is unimportant. Self-efficacy represents perceived capability rather than directly observed competence, and the current measurement does not establish whether respondents can correctly perform the corresponding security actions. Furthermore, its relationship with intention is estimated conditionally on the other included predictors, particularly Response Efficacy. The distinction between perceived capability and perceived effectiveness may therefore merit closer investigation in future PPOB research. Users may believe that a protective action is effective without necessarily evaluating their own ability to perform it in the same way. The present data, however, do not establish why these constructs differ in their estimated structural relationships.

### 3.4.5 Protection Intention and Self-Reported Protective Transaction Behavior

Protection Intention exhibited the strongest structural relationship in the model, with a standardized coefficient of 0.741 and an effect size of 1.220. The model explained 54.9% of the variance in Protective Transaction Behavior, indicating a substantial association between security-related intention and the protective practices reported by PPOB users. This result is consistent with the broader proposition that behavioral intentions are related to the adoption of recommended protective actions. In the PPOB context, these actions include accessing official transaction channels, verifying payment information, protecting authentication credentials, and reviewing transaction records.

Nevertheless, the magnitude of this association should be interpreted within the study's measurement design. Protection Intention and Protective Transaction Behavior were assessed using self-reported questionnaire responses. Moreover, the intention indicators referred to future protective actions, whereas the behavioral indicators asked respondents to report practices undertaken during the preceding three months. Consequently, the statistical association does not demonstrate that intention temporally preceded the reported behavior. The two constructs may also share response tendencies or conceptual similarities arising from their focus on comparable protective activities.

This limitation is particularly relevant in light of van 't Hoff-de Goede et al. [12], who demonstrated that self-reported protective online behavior may differ substantially from behavior observed through an experimental assessment. Accordingly, the present findings support a strong relationship between Protection Intention and self-reported protective transaction practices, but do not establish the effectiveness of those practices in preventing actual security incidents. Longitudinal investigations or studies incorporating observed security behavior would provide a stronger basis for examining the relationship between intention and subsequent protective action.

### 3.4.6 Theoretical and Practical Implications

The findings offer several implications for applying Protection Motivation Theory to PPOB-based digital transaction services. First, they indicate that the relative contributions of threat appraisal and coping appraisal are not uniform. Response Efficacy emerged as the strongest positive antecedent of Protection Intention, whereas Perceived Vulnerability and Security Self-Efficacy were not statistically significant in the specified model. Second, the unexpected positive association between Response Cost and Protection Intention highlights the importance of examining how security-related effort is perceived and operationalized in transaction environments. This finding does not invalidate PMT, but indicates that the hypothesized cost relationship was not supported in the present application. Further testing is necessary before proposing a context-specific modification of the theory.

Third, the strong association between Protection Intention and self-reported Protective Transaction Behavior demonstrates the relevance of distinguishing motivational judgments from reported security practices. This distinction contributes to the application of PMT in customer-facing digital payment services, while the cross-sectional design limits conclusions about behavioral change. From a practical standpoint, the findings suggest that PPOB service providers could prioritize clear and actionable security communication,

including guidance on official transaction channels, authentication protection, suspicious payment links, and payment verification. Such information may help users understand the protective purpose of recommended procedures.

The positive Response Cost coefficient should not be used to justify introducing additional security burdens. Instead, security procedures should remain understandable and proportionate to transaction risks, while their perceived inconvenience and protective value are assessed separately. Several methodological limitations qualify these implications. The elevated HTMT between Perceived Severity and Perceived Vulnerability, together with the identified cross-loading patterns, indicates that measurement distinctiveness was not fully established. The behavioral outcome was based on self-reports rather than independently verified transactions, and the model did not evaluate objective security outcomes or causal effects. In addition, the positive $Q^2$ values derived from blindfolding do not establish out-of-sample predictive performance.

These considerations indicate that the model offers a useful explanation of reported protective transaction behavior within the observed sample, while leaving opportunities for measurement refinement, longitudinal validation, and behavioral verification in future studies.

## 4 CONCLUSION

This study examined the factors associated with protective transaction behavior among Payment Point Online Bank (PPOB) users by applying Protection Motivation Theory (PMT) to a digital financial transaction context. Using survey data from 489 respondents and Partial Least Squares Structural Equation Modeling (PLS-SEM), the proposed model explained 52.0% of the variance in Protection Intention and 54.9% of the variance in self-reported Protective Transaction Behavior. Three of the six hypothesized structural relationships were supported, indicating that threat and coping appraisals differed in their associations with users' protective intentions. Response Efficacy emerged as the strongest positive antecedent of Protection Intention (β = 0.372), followed by Perceived Severity (β = 0.133). In contrast, Perceived Vulnerability and Security Self-Efficacy did not exhibit statistically significant relationships with Protection Intention. Notably, Response Cost demonstrated a significant positive association (β = 0.295), contradicting the hypothesized negative direction. This unexpected finding requires cautious interpretation and further examination of how users perceive the effort and inconvenience associated with security precautions. Protection Intention showed a strong positive association with self-reported Protective Transaction Behavior (β = 0.741). The indirect effects analysis further identified significant positive associations involving Response Efficacy, Response Cost, and Perceived Severity through Protection Intention, although these associations do not establish causal mediation. The findings contribute to the contextual application of PMT by demonstrating that the perceived effectiveness of protective measures is a particularly relevant correlate of security-related intentions in routine PPOB transactions. From a practical perspective, the results suggest that PPOB providers should emphasize clear security guidance, transaction verification procedures, and understandable explanations of how recommended precautions reduce transaction-related risks. Nevertheless, the study has several limitations, including insufficient discriminant validity between Perceived Severity and Perceived Vulnerability (HTMT = 0.939), reliance on cross-sectional self-reported data, and the absence of independently verified security behavior. Future research should refine the measurement of closely related PMT constructs, investigate the unexpected Response Cost relationship, and incorporate longitudinal designs or observed transaction security practices. Such extensions would strengthen understanding of how protective motivations relate to actual security behavior in digital financial services.

**Daftar Pustaka:**

[1] Bank Indonesia, "Monetary Policy Review : Desember 2025." Accessed: Juli. 15, 2026. https://www.bi.go.id/en/publikasi/laporan/Pages/TKM-Desember-2025.aspx

[2] OJK, "Satgas PASTI Imbau Masyarakat Waspadai Penipuan Menggunakan Artificial Intelligence." Accessed: Juli. 15, 2026. [Online]. Available: https://ojk.go.id/id/berita-dan-kegiatan/info-terkini/Pages/Satgas-PASTI-Imbau-Masyarakat-Waspadai-Penipuan-Menggunakan-AI.aspx

[3] A. D. Ansori and S. S. Nugroho, "The Role of Trust on the Continuance Usage Intention of Indonesian Mobile Payment Application," *Gadjah Mada International Journal of Business*, vol. 26, no. 2, pp. 231–257, 2024, doi: 10.22146/gamaijb.70452.

[4] R. W. Rogers, "A Protection Motivation Theory of Fear Appeals and Attitude Change1," *J. Psychol.*, vol. 91, no. 1, pp. 93–114, Sep. 1975, doi: 10.1080/00223980.1975.9915803.

[5] J. E. Maddux and R. W. Rogers, "Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change," *J. Exp. Soc.*

*Psychol.*, vol. 19, no. 5, pp. 469–479, Sep. 1983, doi: 10.1016/0022-1031(83)90023-9.

[6] A. C. Johnston and M. Warkentin, "Fear Appeals and Information Security Behaviors: An Empirical Study1," *MIS Quarterly*, vol. 34, no. 3, pp. 549–566, Sep. 2010, doi: 10.2307/25750691.

[7] P. Ifinedo, "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory," *Comput. Secur.*, vol. 31, no. 1, pp. 83–95, Feb. 2012, doi: 10.1016/j.cose.2011.10.007.

[8] U. Kiran, N. F. Khan, H. Murtaza, A. Farooq, and H. Pirkkalainen, "Explanatory and predictive modeling of cybersecurity behaviors using protection motivation theory," *Comput. Secur.*, vol. 149, p. 104204, Feb. 2025, doi: 10.1016/j.cose.2024.104204.

[9] T. Karayel and M. Saygılı, "Understanding smartphone security behavior through the core constructs of protection motivation theory: A comparative study of iOS and android users," *Comput. Secur.*, vol. 158, p. 104652, Nov. 2025, doi: 10.1016/j.cose.2025.104652.

[10] E. M. Alrawhani, A. Romli, and M. A. Al-Sharafi, "Evaluating the role of protection motivation theory in information security policy compliance: Insights from the banking sector using PLS-SEM approach," *Journal of Open Innovation: Technology, Market, and Complexity*, vol. 11, no. 1, p. 100463, Mar. 2025, doi: 10.1016/j.joitmc.2024.100463.

[11] A. B. Seini, I. O. Adam, and M. D. Alhassan, "Examining the effect of security behaviour on the continuance use of mobile money services in Ghana: a protection motivation perspective," *Inf. Technol. Dev.*, vol. 31, no. 4, pp. 1318–1335, Oct. 2025, doi: 10.1080/02681102.2025.2483695.

[12] M. S. van 't Hoff-de Goede, E. R. Leukfeldt, S. G. A. van de Weijer, and R. van der Kleij, "Does protection motivation predict self-protective online behaviour? Comparing self-reported and actual online behaviour using a population-based survey experiment," *Computers in Human Behavior Reports*, vol. 18, p. 100649, May 2025, doi: 10.1016/j.chbr.2025.100649.

[13] J. Hair and A. Alamer, "Partial Least Squares Structural Equation Modeling (PLS-SEM) in second language and education research: Guidelines using an applied example," *Research Methods in Applied Linguistics*, vol. 1, no. 3, p. 100027, 2022, doi: 10.1016/j.rmal.2022.100027.

[14] Sarstedt, Joseph F HairJr, Jun-Hwa Cheah, Jan-Michael Becker, and Christian M Ringle, "How to Specify, Estimate, and Validate Higher-Order Constructs in PLS-SEM," *Australasian Marketing Journal*, vol. 27, no. 3, pp. 197–211, Aug. 2019, doi: 10.1016/j.ausmj.2019.05.003.

[15] J. F. Hair, J. J. Risher, M. Sarstedt, and C. M. Ringle, "When to use and how to report the results of PLS-SEM," Jan. 14, 2019, *Emerald Group Publishing Ltd.* doi: 10.1108/EBR-11-2018-0203.

[16] J. F. Hair Jr, M. Sabol, M. S. Islam, and F. Murshed, "Conditional Mediation (CoMe) Models with PLS-SEM: An Update, Review, and Best-Practice Recommendations," *Australasian Marketing Journal*, 2024, doi: 10.1177/14413582261420459.

[17] R. Adyaputra, K. Imtihan, and M. Saleh, "Assessing User Satisfaction of Local Government Websites Through ISO 25010 and Technology Acceptance Model (TAM): A SmartPLS and IPMA-Based Study in Lombok Tengah," *Journal of Information and Organizational Sciences*, vol. 49, no. 2, pp. 291–312, 2025, doi: 10.31341/jios.49.2.8.

[18] K. Imtihan, Mardi, and M. Rodi, "The Impact of Visual Quality and User Interface Responsiveness on Student Satisfaction in Academic Information Systems (AIS)," *Pak. J. Life Soc. Sci.*, vol. 22, no. 2024, pp. 19896–19906, 2024.

[19] A. Vance, M. Siponen, and S. Pahnila, "Motivating IS security compliance: Insights from Habit and Protection Motivation Theory," *Information & Management*, vol. 49, no. 3–4, pp. 190–198, May 2012, doi: 10.1016/j.im.2012.04.002.

[20] K. Imtihan, A. Tantoni, and M. Mardi, "A Modified TAM-ECT Model for Evaluating User Satisfaction and Behavioral Intention in Community-Based Internet Services," *Edu Komputika Journal*, vol. 12, no. 1, pp. 61–74, 2025.

[21] A. Aman, K. Imtihan, and M. Rodi, "Evaluating User Satisfaction and Public Engagement in Local Government Social Media," *International Journal of Engineering, Science and Information Technology*, vol. 5, no. 3, pp. 235–248, 2025, doi: 10.52088/ijesty.v5i3.905.

[22] J. Hair, G. Tomas M. Hult, Christian M. Ringle, and Marko Sarstedt, "A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)," 21AD.

[23] J. F. Hair Jr *et al.*, "An introduction to structural equation modeling," *Partial least squares structural equation modeling (PLS-SEM) using R:*

*a workbook*, pp. 1–29, 2021, doi: 10.1007/978-3-030-80519-7_1.

[24] J. Henseler, C. M. Ringle, and M. Sarstedt, "A new criterion for assessing discriminant validity in variance-based structural equation modeling," *J. Acad. Mark. Sci.*, vol. 43, no. 1, pp. 115–135, Jan. 2015, doi: 10.1007/s11747-014-0403-8.