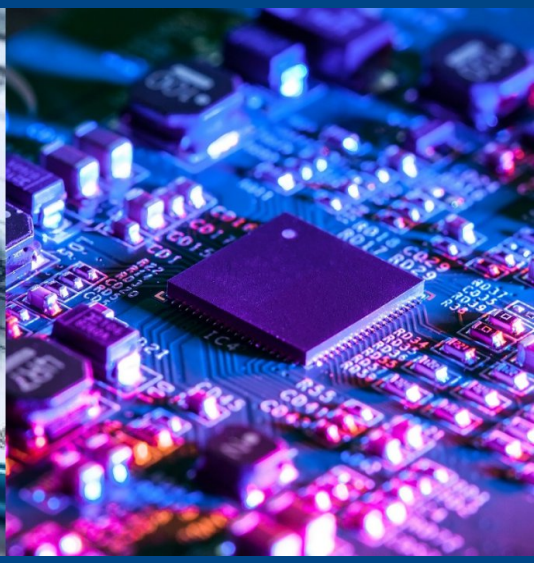
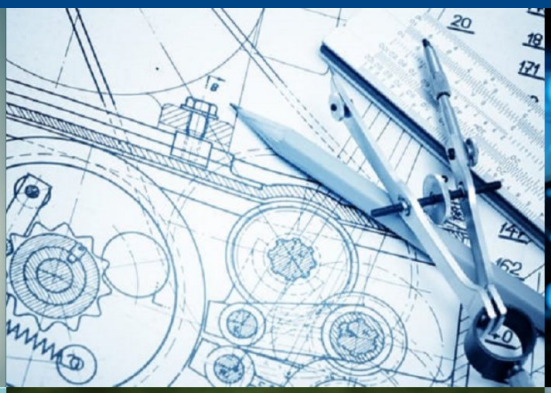
ISSN: 2582-7219

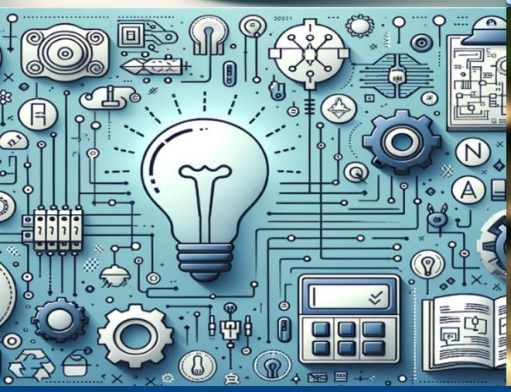




International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206 **Volume 9, Issue 4, April 2026**

© 2026 IJMRSET | Volume 9, Issue 4, April 2026| DOI:10.15680/IJMRSET.2026.0904095

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

How Security Nudges Work in Fintech: The Role of Risk Perception and Message Processing Route in Authentication Behavior

Winona Neha Noronha, Dr. Avinash Rana

MBA Student, CMS Business School, Jain Deemed-to-be University, Bengaluru, India

Assistant Professor, Faculty of Management Studies, CMS Business School, Jain Deemed-to-be University, Bengaluru, India

ABSTRACT: The rapid adoption of fintech platforms has significantly transformed financial interactions, offering convenience and accessibility to users worldwide. However, this digital transformation has also increased vulnerability to security threats, particularly due to weak authentication practices among users. Despite the availability of secure mechanisms such as multi-factor authentication and strong password policies, user compliance remains inconsistent. This highlights the importance of understanding behavioral factors influencing security decisions.

This study examines the effectiveness of different security nudges in influencing authentication behavior within fintech environments. It also investigates the roles of elaboration, representing cognitive processing, and psychological reactance, representing resistance to influence. A structured questionnaire was administered to 154 respondents, and the collected data was analyzed using Exploratory Factor Analysis (EFA), Confirmatory Factor Analysis (CFA), and Structural Equation Modeling (SEM).

The findings reveal that security nudges significantly influence authentication behavior, but their effectiveness varies across types. Fear appeal and social proof nudges show a strong direct impact on authentication strength, while informative nudges primarily influence cognitive engagement through elaboration. Elaboration partially mediates the relationship between nudges and authentication behavior, indicating that both cognitive and direct pathways are involved. Interestingly, psychological reactance does not negatively moderate the relationship, but instead shows a positive association with both elaboration and authentication strength.

The study contributes to the literature on behavioral cybersecurity by integrating nudge theory, the Elaboration Likelihood Model, and psychological reactance. It also provides practical insights for fintech platforms to design more effective, user-centered security interventions.

KEYWORDS: Security Nudges, Authentication Behavior, Fintech Security, Elaboration Likelihood Model, Psychological Reactance, Behavioral Cybersecurity, Structural Equation Modeling

I. INTRODUCTION

The proliferation of digital financial technologies has fundamentally altered how individuals manage financial transactions. Fintech platforms, including mobile banking applications, digital wallets, and online payment systems, have enabled users to perform financial activities with unprecedented ease. However, this increased accessibility has also introduced significant security risks, particularly related to user behavior.

Despite widespread awareness of cybersecurity threats, users often fail to adopt secure authentication practices. Weak passwords, reuse of credentials, and reluctance to enable additional security features remain common issues. Traditional security approaches primarily focus on technological solutions, often overlooking the behavioral dimension of cybersecurity. This gap highlights the need for interventions that can influence user behavior effectively.

Security nudges have emerged as a promising approach in this context. Nudges are subtle modifications in the decision-making environment designed to guide users toward desirable behaviors without restricting their choices. In fintech

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

applications, nudges can take various forms, including informative messages, social comparisons, fear-based warnings, and default settings.

This study aims to examine how different types of security nudges influence authentication behavior. It further explores the role of elaboration, which reflects the extent of cognitive processing, and psychological reactance, which represents resistance to perceived influence.

The study contributes to existing literature in three ways. First, it compares multiple nudge types within a unified framework. Second, it integrates behavioral theories such as the Elaboration Likelihood Model and psychological reactance theory. Third, it applies advanced statistical techniques to analyze both direct and indirect relationships.

II. LITERATURE REVIEW

Nudge theory, proposed by Thaler and Sunstein, suggests that individuals' decisions can be influenced through subtle changes in the choice environment. In the context of cybersecurity, nudges have been used to promote behaviors such as password updates and secure browsing practices. However, the effectiveness of nudges depends on how users perceive and process the information presented.

The Elaboration Likelihood Model provides a theoretical framework for understanding message processing. According to ELM, individuals process information through either the central route, involving deep cognitive engagement, or the peripheral route, relying on simple cues. Informative nudges are likely to activate the central route, encouraging users to evaluate risks and make informed decisions. In contrast, social proof and default nudges rely on heuristics and may not require extensive cognitive effort.

Psychological reactance theory explains how individuals respond to perceived threats to their autonomy. When users feel that their freedom is restricted, they may resist persuasive attempts. In cybersecurity contexts, reactance is often assumed to reduce compliance with security recommendations. However, recent studies suggest that reactance may not always have a negative impact and may instead lead to increased awareness and proactive behavior.

Existing research has primarily focused on individual nudges, with limited studies comparing multiple nudge types within a single model. Furthermore, the interplay between elaboration, reactance, and authentication behavior remains underexplored. This study addresses these gaps by integrating multiple constructs and examining their relationships using Structural Equation Modeling.

III. RESEARCH MODEL AND HYPOTHESES

The conceptual model of this study is designed to examine how different types of security nudges influence authentication behavior in fintech environments. The model proposes both direct and indirect relationships between the variables, providing a comprehensive framework to understand user decision-making in digital security contexts.

Specifically, different nudge types (informative, social proof, fear appeal, and default) are expected to influence authentication strength directly, as well as indirectly through elaboration. Elaboration represents the degree to which users engage in deeper cognitive processing when exposed to security messages. In addition, psychological reactance is included in the model to assess whether users' resistance to perceived influence alters the effectiveness of nudges.

The inclusion of both mediation and moderation effects allows for a more nuanced understanding of how behavioral interventions operate, moving beyond simple cause-and-effect relationships.

Hypotheses

- **H1:** Security nudges positively influence authentication strength
- **H2:** Elaboration mediates the relationship between security nudges and authentication strength
- **H3:** Psychological reactance moderates the relationship between security nudges and authentication strength
- **H5:** Fear appeal nudges are more effective than other nudge types

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

IV. METHODOLOGY

This study adopts a quantitative research design to empirically test the proposed relationships. Data was collected through a structured online questionnaire distributed among fintech users, resulting in a total of 154 valid responses. The sample consists primarily of digitally active individuals, making it appropriate for studying behavior in fintech environments.

The questionnaire was divided into multiple sections to measure key constructs, including psychological reactance, elaboration, different nudge types, and authentication strength. All items were measured using a five-point Likert scale ranging from strongly disagree to strongly agree. The use of standardized scales ensures consistency and comparability across responses.

Data analysis was conducted using Python, enabling systematic and reproducible analysis. Reliability of the constructs was assessed using Cronbach's alpha to ensure internal consistency. Exploratory Factor Analysis (EFA) was performed to identify the underlying factor structure of the variables, followed by Confirmatory Factor Analysis (CFA) to validate the measurement model.

Structural Equation Modeling (SEM) was employed to test the hypothesized relationships among variables. SEM is particularly suitable for this study as it allows simultaneous analysis of multiple relationships, including direct, indirect, and interaction effects. This provides a comprehensive understanding of how different factors influence authentication behavior.

V. RESULTS AND ANALYSIS

The analysis begins with descriptive statistics, which indicate moderate agreement across all constructs. This suggests that respondents exhibit balanced perceptions and behaviors, providing a realistic representation of user attitudes in fintech contexts. Reliability analysis further confirms that most constructs demonstrate acceptable to strong internal consistency, supporting the reliability of the measurement scales.

The Kaiser-Meyer-Olkin (KMO) value of 0.844 and a statistically significant Bartlett's test confirm that the data is suitable for factor analysis. The results of Exploratory Factor Analysis identify six distinct factors that align with the theoretical constructs of the study, indicating a clear and interpretable factor structure.

Confirmatory Factor Analysis further validates the measurement model. The model demonstrates excellent fit, with high values for Comparative Fit Index (CFI) and Tucker-Lewis Index (TLI), and a negligible Root Mean Square Error of Approximation (RMSEA). All factor loadings are statistically confirming the convergent validity of the constructs.

The Structural Equation Modeling results provide key insights into the relationships between variables. Informative and fear appeal nudges are found to significantly influence elaboration, indicating that these nudges encourage deeper cognitive processing. This suggests that users engage more actively with messages that provide information or highlight risks.In terms of direct effects, social proof and fear appeal nudges have a significant positive impact on authentication strength. This highlights the importance of social influence and emotional triggers in shaping user behavior. Informative and default nudges, however, do not show a strong direct effect, indicating that their influence may be more indirect.

Elaboration is found to significantly influence authentication behavior, confirming its role as a mediating variable. However, the mediation is partial, suggesting that nudges affect behavior both directly and through cognitive processing.

Psychological reactance does not moderate the relationship between nudges and authentication behavior, as initially hypothesized. Instead, it shows a positive direct effect on authentication strength. This indicates that users who value autonomy may be more engaged and proactive in adopting secure practices.

Overall, the results demonstrate that security nudges influence authentication behavior through a combination of cognitive, emotional, and social mechanisms.

© 2026 IJMRSET | Volume 9, Issue 4, April 2026| DOI:10.15680/IJMRSET.2026.0904095

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

VI. DISCUSSION

The findings of this study indicate that security nudges influence authentication behavior through multiple pathways rather than a single mechanism. Informative nudges primarily affect users through cognitive engagement by providing logical and factual information, encouraging deeper processing of security-related decisions. This aligns with the central route of the Elaboration Likelihood Model, where individuals who think more critically about information are more likely to adopt stable behavioral changes (Petty & Cacioppo, 1986).

In contrast, social proof nudges operate through peripheral processing by leveraging social influence. Users tend to follow the behavior of others, especially in situations involving uncertainty. This is consistent with prior research highlighting the role of social norms in shaping decision-making (Cialdini, 2009). Fear appeal nudges, however, combine both emotional and cognitive elements, making them particularly effective. By emphasizing potential risks, they create urgency and motivate users to adopt secure behaviors.

Elaboration plays a significant role in influencing authentication strength, suggesting that users who process information more deeply are more likely to engage in secure practices. However, the mediation is partial, indicating that nudges can also directly influence behavior without requiring deep cognitive processing.
An important finding relates to psychological reactance. Contrary to traditional assumptions, reactance does not weaken the effectiveness of nudges. Instead, it shows a positive relationship with both elaboration and authentication behavior. This suggests that users who value autonomy may be more proactive in managing their security, challenging the conventional view of reactance as purely negative (Brehm, 1966).

Overall, the results highlight that effective security interventions must consider cognitive, emotional, and social dimensions of user behavior.

VII. CONCLUSION

This study examined the impact of different types of security nudges on authentication behavior in fintech environments, while also analyzing the roles of elaboration and psychological reactance. The findings confirm that security nudges are effective in influencing user behavior, but their effectiveness varies across types and underlying mechanisms.

Informative nudges primarily promote cognitive engagement, encouraging users to process security information more deeply. Social proof nudges influence behavior through social conformity, while fear appeal nudges combine emotional and cognitive elements to drive action. These findings highlight that different nudges operate through distinct psychological pathways.

Elaboration emerged as an important factor influencing authentication behavior, indicating that deeper cognitive processing leads to stronger security practices. However, the mediation effect was partial, suggesting that nudges can influence behavior both directly and indirectly.

A key contribution of this study is the finding that psychological reactance does not reduce the effectiveness of nudges. Instead, it positively influences both elaboration and authentication strength. This challenges traditional assumptions and suggests that autonomy-oriented users may take greater responsibility for their security.

Overall, the study provides a comprehensive understanding of how behavioral interventions function in digital security contexts. The findings contribute to both theory and practice by offering insights into designing effective and user-centered security systems in fintech environments.

VIII. IMPLICATIONS

Theoretical Implications

This study extends the application of the Elaboration Likelihood Model to the context of fintech security behavior, demonstrating that different nudges activate different processing routes. Informative nudges align with central processing, while social proof nudges rely on peripheral cues (Petty & Cacioppo, 1986).

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

The study also highlights the role of elaboration as a partial mediator, showing that behavioral outcomes are influenced by both cognitive engagement and direct effects. Additionally, the findings challenge traditional views on psychological reactance, suggesting that it can have a positive influence in certain contexts rather than acting as a barrier (Brehm, 1966).

Overall, the study contributes to nudge theory by emphasizing that different nudges operate through distinct mechanisms and should not be treated as a single category.

Managerial Implications

The findings provide practical insights for fintech companies and digital security designers. Organizations should adopt a combination of nudges rather than relying on a single approach. Informative nudges can be used to educate users, while social proof nudges can leverage peer influence to encourage adoption of security practices (Cialdini, 2009).
Fear appeal nudges can be effective in highlighting risks and prompting immediate action, but should be used carefully to avoid overwhelming users. Default nudges can simplify decision-making by making secure options the standard choice.

Another key implication is that maintaining user autonomy is important. Since psychological reactance does not negatively impact nudge effectiveness, organizations can focus on transparent and user-friendly security design rather than restrictive measures.

Overall, fintech platforms should adopt a user-centered approach that combines cognitive, emotional, and social elements to improve security behavior.

REFERENCES

1. Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science, 347*(6221), 509–514. https://doi.org/10.1126/science.aaa1465
2. Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly, 34*(3), 613–643.
3. Brehm, J. W. (1966). *A theory of psychological reactance*. Academic Press.
4. Cialdini, R. B. (2009). *Influence: Science and practice* (5th ed.). Pearson Education.
5. Cortina, J. M. (1993). What is coefficient alpha? An examination of theory and applications. *Journal of Applied Psychology, 78*(1), 98–104.
6. Fabrigar, L. R., Wegener, D. T., MacCallum, R. C., & Strahan, E. J. (1999). Evaluating the use of exploratory factor analysis in psychological research. *Psychological Methods, 4*(3), 272–299.
7. Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2019). *Multivariate data analysis* (8th ed.). Cengage Learning.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com