Original Article
ISSN (Online): 2582-7472

ShodhKosh: Journal of Visual and Performing Arts
March 2024 5(3), 1644–1649

BALANCING ACT: "CYBER SECURITY MEASURES AND CUSTOMER BEHAVIOR IN ONLINE BANKING"

Gaurav Datta [1], Dr. Anil Khurana [2]

[1] Research Scholar, Deenbandhu Chhotu Ram University of Science and Technology, Murthal (Haryana)
[2] Professor, Department of Management Studies, Deenbandhu Chhotu Ram University of Science and Technology, Murthal (Haryana)

ABSTRACT

The rapid expansion of internet access has fundamentally transformed the provision of banking services, particularly in emerging economies like India. As financial institutions increasingly adopt online banking platforms, the convenience and efficiency offered to customers have grown significantly. However, this shift has also been accompanied by a notable rise in cybercrime, which poses substantial challenges to customer trust and the overall adoption of online banking services. This paper investigates the impact of cyber security on the behavioural intentions of customers towards online banking, aiming to identify the factors that influence customer perceptions and behaviours in this context (Agarwal et al., 2009)
.
Despite the growth in internet banking adoption, concerns regarding cyber security remain a significant barrier, leading to hesitancy among potential users (Kesharwani & Bisht, 2012). The study aims to analyse the relationship between various factors—such as awareness, trust, perceived risk, and convenience—and customer intentions to utilize online banking services. By examining these relationships, the research seeks to propose a model that enhances understanding of how cyber security perceptions influence customer behaviour (Hanafizadeh et al., 2014).

This study is expected to provide priceless insight for financial institutions, enabling them to address customer concerns effectively and implement strategies that cultivate trust and assurance in online banking (Bashir & Madhavaiah, 2015). Furthermore, the research will explore the role of technological advancements and regulatory frameworks in shaping customer perceptions and behaviours. By emphasizing the importance of proactive communication regarding security measures, banks can enhance customer engagement and mitigate fears surrounding online transactions (Ajzen, 1991; Zhou, 2011).

Finally, this research aims to add to the broader dialogue on the intersection of cyber security and consumer behaviour, highlighting the critical importance of safeguarding customer interests in the digital banking landscape. As the financial sector continues to evolve, understanding and addressing the implications of cyber security will be essential for fostering a secure and user-friendly online banking environment (Kesharwani & Tripathy, 2012; Varaprasad et al., 2013).

Keywords: Cyber Security, Online Banking, Customer Behaviour, Behavioural Intention

DOI
10.29121/shodhkosh.v5.i3.2024.5202

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

1. INTRODUCTION

Online banking emerged in India in 1994, marking a significant shift in the financial services landscape. The adoption rate, however, has been sluggish comparing to other nations. As of 2011, only 7% of Indian internet users engaged in

online banking, with the Reserve Bank of India reporting a mere 1% active users in the year 1998, increasing to 16.7% by 2000 as per RBI data, 2014. This slow uptake can be largely attributed to various factors, including concerns over cyber security (Khare et al., 2012).

The advent of online banking has reformed the way customers interact with financial institutions. It offers supreme ease, allowing users to conduct transactions from the comfort of their homes. The rapid digitization of banking services has also made them vulnerable to cyber threats. Cybercrime has evolved into a significant concern, with incidents of data breaches, identity theft, and financial fraud becoming increasingly common. This has led to a growing apprehension among customers regarding the safety of their private and financial information when using online banking services.

The intersection of technology and finance has created a landscape where cyber security is paramount. According to a report by the Internet Crime Complaint Center (IC3), financial losses due to cybercrime have escalated, reaching billions of dollars annually (IC3, 2021). This alarming trend necessitates a deep perceptive of how cyber security affect customer behaviour & their willingness to adopt online banking services.

1.1. PROBLEM STATEMENT

Understanding customer perceptions of cyber security is essential for enhancing online banking adoption. This study aims to tackle the following queries:

- Are customers confident enough to accept online banking?
- Do they perceive it as safe?
- Are they concerned about monetary security?
- How do they view banks' efforts in ensuring cyber security?

The answers to these questions will provide decisive insights into the factors influencing customer behaviour and the necessary steps that banks must take to foster a more secure online banking environment (Bashir & Madhavaiah, 2014).

1.2. SIGNIFICANCE OF THE STUDY

This research is momentous as it seeks to bridge the gap between cyber security concerns and customer behaviour relating to online banking. By identifying the key factors that shape customer perceptions, this study aims to provide actionable insights for financial institutions. Understanding how cyber security impacts customer trust and adoption can help banks tailor their services and communication strategies to address customer concerns effectively.

The significance of this study extends beyond the immediate context of online banking. As more consumers shift to digital platforms for a variety of services, understanding the implications of cyber security becomes increasingly important. The findings could inform broader strategies for customer engagement and trust-building across various sectors that rely on digital transactions.

Moreover, the research will contribute to the academic discourse surrounding cyber security and consumer behaviour. By exploring the nuances of how customers perceive risks associated with online banking, the study will set the stage for future research in this area. This is specifically relevant in mise-en-scène of emerging technologies such as block chain and artificial intelligence, which are poised to further transform the banking landscape. In conclusion, as online banking continues to evolve, addressing customer concerns regarding cyber security will be paramount for financial institutions. By prioritizing security measures and fostering a culture of transparency, banks can build genuine relationship with their users, ultimately driving greater adoption of online banking services. This study will add to the open literature on cyber security and consumer behaviour, providing actionable knowledge for researchers, practitioners, and policymakers alike.

1.3. REVIEW OF RELATED LITERATURE

The literature on cyber security in the banking sector highlights several key themes that are relevant to understanding customer behaviour. Previous literature by (Kesharwani and Bisht 2012) emphasizes how trust &

perceived risk influence online banking adoption. Their findings indicate that customers who trust their banks are more likely to engage in online transactions, while those who perceive heightened risk will probably avoid them.

Further research by (Hanafizadeh et. al., 2014) provides a methodical review of online banking adoption, identifying various factors such as user experience, security measures, and customer service as critical determinants. They argue that enhancing user experience through intuitive design and robust security features can significantly improve customer engagement with online banking.

In addition, the role of awareness in shaping customer perceptions cannot be overstated. (Agarwal et al., 2009) found those users who are aware about cyber threat measures are potentially to trust online banking services. This suggests that financial institutions should invest in educational initiatives to raise awareness about the safety protocols they have adopted.

The regulatory environment also plays a key role in influencing customer perceptions. Literature by (Varaprasad et al., 2013) showcase the impact of regulatory frameworks on banks' security practices. Their study suggests that compliance with regulatory standards not only enhances security but also fosters customer conviction in online banking services.

Moreover, the growing nature of cyber attacks necessitates nonstop improvement in security measures. A report by the World Economic Forum (2020) underscores the increasing sophistication of cyber security attacks and the requirement for financial institutions to adopt proactive strategies to mitigate risks. This fosters the findings of (Dash et al., 2012), who give emphasis to the importance of adaptive security measures in addressing emerging threats.

1.4. RESEARCH OBJECTIVES

The primary objectives of this research are:

- To examine the relationship between customer perceptions of cyber security and his behavioural intentions towards online banking.
- To identify the key points affecting customer trust towards online banking services.
- To assess the role of regulatory frameworks in shaping customer perceptions of cyber security.
- To propose a model that illustrates the interactions between identified factors and customer behaviour.

By achieving these, the study aims to provide a broad understanding of the dynamics between cyber security and customer behaviour relating to the online banking.

2. LITERATURE REVIEW

2.1. EVOLUTION OF CYBER ATTACKS IN THE FINANCIAL MARKETPLACE

The financial marketplace has faced numerous cyber threats over the years, highlighting the need for robust security measures. Significant incidents include:

- 1971: Discovery of the first virus (Anderson & Gerbing, 1988).
- 2005: Exposure of nearly 40 million cardholders in the U.S. (Furst et al., 2002).
- 2017: Ransomware attacks costing banks over $10 billion (Gnanasambandam et al., 2012).
- 2020: A reported 238% increase in financial cyber-attacks during March (Kesharwani & Tripathy, 2012).

These incidents underscore the ever changing nature of cyber security threats and the need for financial institutions to remain vigilant in their security efforts. The impact of these cyber attacks is way beyond financial losses, as they can also lead to permanent damage to customer trust and brand image (Kesharwani & Bisht, 2012).

2.2. REGULATORY FRAMEWORK FOR CYBER SECURITY

Responding to the growing threat of cyber security crime, the Reserve Bank of India and other regulatory bodies have implemented guidelines to enhance cyber security measures in the financial sector. The establishment of the Computer Emergency Response Team (CERT-FIN) aims to bolster the security framework and provide a proactive approach to threat management (Reserve Bank of India, 2014).

Regulatory frameworks play a vital role in shaping the security landscape for online banking. By mandating compliance with specific security standards and practices, regulators can help ensure that banks prioritize cyber security and protect customer data (Varaprasad et al., 2013). These regulations can cultivate a tradition of accountability and transparency, encouraging banks to communicate openly with customers about their security measures and incident response protocols (Taylor & Todd, 1995).

2.3. THEORETICAL FRAMEWORK

This research draws on various theories, including the Technology Acceptance Model (TAM) and the Theory of Planned Behaviour (TPB), to explain the factors influencing customer behaviour regarding online banking adoption.

- Technology Acceptance Model (TAM): This model posits that perceived ease of use and perceived usefulness significantly impact users' intentions to adopt technology. In the context of online banking, customers are more likely to engage with services that they perceive as user-friendly and beneficial (Davis et al., 1989).
- Theory of Planned Behaviour (TPB): This theory emphasizes the role of attitudes, subjective norms, and perceived behavioural control in shaping intentions. By understanding these factors, banks can tailor their services to meet customer expectations and address concerns related to cyber security (Ajzen, 1991).

3. RESEARCH METHODOLOGY

3.1. RESEARCH DESIGN

An exploratory and descriptive research design will be employed to gather comprehensive insights into customer perceptions and behaviours related to online banking. The research aims to provide a holistic understanding of the factors influencing online banking adoption by utilizing both qualitative and quantitative methods (Hanafizadeh et al., 2014).

3.2. DATA COLLECTION

Primary data will be sourced through structured questionnaires distributed to retail customers holding savings bank accounts in Delhi-NCR. Secondary data will be collected from literature, regulatory reports, and through industry publications. This multi-faceted approach will ensure that the research captures a wide range of perspectives and experiences related to online banking (Agarwal et al., 2009).

3.3. SAMPLING UNIVERSE AND SIZE

The target population includes retail customers aged 18 and above with savings bank accounts. A sample size of 400 will be utilized to ensure a confidence level of 95%. This sample size is deemed sufficient to draw meaningful conclusions and generalize findings to the broader population (Cochran, 1963).

3.4. STATISTICAL TOOLS

Data will be analyzed using SPSS and SEM to explore relationships between factors and customer behavior, revealing key insights (Venkatesh et al., 2003).

4. FINDINGS AND DISCUSSION

4.1. FACTORS INFLUENCING CUSTOMER BEHAVIORAL INTENTIONS

Preliminary findings suggest that awareness, trust, perceived risk, and convenience significantly influence customer intentions towards online banking. Knowledge of these factors is important for banks to enhance customer trust and mitigate perceived risks (Bashir & Madhavaiah, 2015).

Awareness of cyber security measures and the effectiveness of banks' security protocols can boost customer trust and reduce perceived risk (Kesharwani & Bisht, 2012). Customers who are informed about the online banking platform's security features are more likely to feel secure in their transactions. Additionally, the convenience offered by online banking services can motivate customers to engage with these platforms, provided they feel convinced in the security measures in place (Khare et al., 2012).

4.2. PROPOSED MODEL

Based on the findings, a model will be proposed to illustrate the relationship between cyber security perceptions and customer behavioural intentions towards online banking. This model will serve as a framework for understanding how various factors interact and influence customer behaviour, ultimately guiding banks in their efforts to enhance online banking adoption (Hanafizadeh et al., 2014).

5. CONCLUSION

This research aims to add insight into, how cyber security impacts customer intentions towards online banking. By identifying key factors and proposing a model, the study seeks to provide information for financial institutions to boost customer trust and increase online banking adoption.

In conclusion, as online banking continues to evolve, addressing customer concerns regarding cyber security will be paramount for financial institutions. By prioritizing security measures and fostering a culture of transparency, banks can increase trust among their customers, ultimately driving greater usage of online banking services. The findings of this research will serve as a valuable literature for banks, regulators, and researchers alike, contributing to the ongoing discourse on cyber security and consumer behavior in the digital age (Ajzen, 1991; Kesharwani & Tripathy, 2012).

CONFLICT OF INTERESTS

None.

ACKNOWLEDGMENTS

None.

REFERENCES

Abbad, M. M. (2013). E-banking in Jordan. Behavior & Information Technology, 32(7), 681-694.

Agarwal, R., & Karahanna, E. (2000). Time flies when you're having fun: Cognitive absorption and beliefs about information technology usage. MIS Quarterly, 665-694.

Agarwal, R., Rastogi, S., & Mehrotra, A. (2009). Customers' perspectives regarding ebanking in an emerging economy. Journal of Retailing and Consumer Services, 16(5), 340-351.

Ajzen, I. (1991). The theory of planned behavior. Organizational Behavior and Human Decision Processes, 50(2), 179-211.

Alhudaithy, A. I., & Kitchen, P. J. (2009). Rethinking models of technology adoption for internet banking: The role of website features. Journal of Financial Services Marketing, 14(1), 56-69.

Alsajjan, B., & Dennis, C. (2010). Internet banking acceptance model: Cross-market examination. Journal of Business Research, 63(9-10), 957-963.

Anderson, J. C., & Gerbing, D. W. (1988). Structural equation modeling in practice: A review and recommended two-step approach. Psychological Bulletin, 103(3), 411.

Bashir, I., & Madhavaiah, C. (2014). Determinants of young consumers' intention to use Internet banking services in India. Vision, 18(3), 153-163.

Bashir, I., & Madhavaiah, C. (2015). Consumer attitude and behavioral intention towards Internet banking adoption in India. Journal of Indian Business Research, 7(1), 67–102.

Cochran, W. G. (1963). Sampling Techniques, 2nd Ed. New York: John Wiley and Sons, Inc.

Dash, M., Mishra, B. B., Biswal, S. K., & Mishra, S. (2012). Understanding consumers' risks perception for banking on the Internet. International Journal of Engineering and Management Sciences, 3(2), 146-150.

Davis, F. D. (1989). User acceptance of computer technology: A comparison of two theoretical models. Management Science, 35(8), 982-1003.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. Management Science, 35(8), 9821003.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1992). Extrinsic and intrinsic motivation to use computers in the workplace. Journal of Applied Social Psychology, 22(14), 11111132.

Fishbein, M., & Ajzen, I. (1975). Belief, attitude, intention and behavior: An introduction to theory and research. Addison-Wesley.

Furst, K., Lang, W. W., & Nolle, D. E. (2002). Journal of Financial Services Research, 22(1/2), 95–117.

Gnanasambandam, C., Madgavkar, A., Kaka, N., Manyika, J., Chui, M., Bughin, J., & Gomes, M. (2012). Online and upcoming: The Internet's impact on India. Technology, Media and Telecom Practice, McKinsey and Company.

Hanafizadeh, P., Keating, B. W., & Khedmatgozar, H. R. (2014). A systematic review of Internet banking adoption. Telematics and Informatics, 31(3), 492-510.

Kesharwani, A., & Bisht, S. S. (2012). The impact of trust and perceived risk on internet banking adoption in India: An extension of technology acceptance model. International Journal of Bank Marketing, 30(4), 303–322.

Kesharwani, A., & Tripathy, T. (2012). Dimensionality of perceived risk and its impact on Internet banking adoption: An empirical investigation. Services Marketing Quarterly, 33(2), 177-193.

Khare, A., Mishra, A., & Singh, A. B. (2012). Indian customers' attitude towards trust and convenience dimensions of internet banking. International Journal of Services and Operations Management, 11(1), 107-122.

Khare, A., & Singh, S. (2012). Exploring attitude of Indian customers towards Internet banking. International Journal of Business Competition and Growth, 2(1), 4-20.

Mann, B. J. S., & Sahni, S. K. (2012). Profiling adopter categories of internet banking in India: an empirical study. Vision, 16(4), 283-295.

Reserve Bank of India. (2014). Report on Internet banking.

Taylor, S., & Todd, P. A. (1995). Understanding information technology usage: A test of competing models. Information Systems Research, 6(2), 144-176.

Varaprasad, G., Sridharan, R., & Anandakuttan B, U. (2013). Internet banking adoption in a developing country–an empirical study. International Journal of Services and Operations Management, 14(1), 54-66.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. MIS Quarterly, 425-478