Research Paper
Impact Factor: 7.184
Peer Reviewed & Indexed Journal
www.iibarr.com

IJBARR
E- ISSN -2347-856X
ISSN -2348-0653

CUSTOMERS LEVEL OF UNDERSTANDING OF BANKING SECURITY MEASURES: A STUDY WITH SPECIAL REFERENCE TO MADURAI CITY

S. Suba* Dr.A. Mayilmurugan**
**Research Scholar (Part Time),Head &Associate Professor,*
PG and Research Department of Commerce, Madurai KamarajUniversity,The Madura College, Madurai.
***PG and Research Department of Commerce Madurai KamarajUniversity, The Madura College, Madurai.*

Abstract *security features are becoming a crucial part of contemporary banking systems due to the growing usage of digital and technologically advanced banking services. Safe banking transactions and the prevention of financial fraud depend heavily on customers' awareness of these security procedures. This study looks at how well-informed consumers are about banking security procedures, specifically in Madurai City. Customers' knowledge of security procedures pertaining to ATM use, online and mobile banking, debit and credit cards, and fraud protection techniques is the main emphasis of the study. The study uses a descriptive research design and is predicated on primary data gathered from Madurai City bank customers using a structured questionnaire. Books, journals, papers, and bank publications provided secondary data. The respondents were chosen by convenience sampling. Statistical procedures such chi-square testing, mean score analysis, and percentage analysis were used to examine the gathered data.*

Key Words: Customer Awareness, Digital Banking, Cyber - Security, Fraud Prevention.

Introduction

The banking industry has seen significant change in the current digital era due to the quick uptake of ATMs, mobile banking, internet banking, and other electronic payment methods. Customers can now execute financial transactions at any time and from any location thanks to these advances that have improved banking's accessibility, speed, and convenience. The rules, procedures, and technological tools that banks use to protect consumer accounts and financial data are collectively referred to as banking security measures. These safeguards include biometric verification, encryption, two-factor authentication, PINs, passwords, and OTPs, as well as real-time fraud alerts. Even though banks make significant investments to fortify these security procedures, their performance ultimately depends on consumers comprehending and appropriately adhering to these measures.Customer knowledge and comprehension of banking security protocols are vital in combating financial fraud and cyber threats. This study intends to assess the level of customer understanding regarding banking security measures, focusing specifically on Madurai City. The research aims to analyse awareness of digital banking security, cyber threats, and fraud prevention strategies, offering valuable insights for banks to enhance customer education and encourage safe banking practices.

Review of literature

1. Research by **Telo (2023)** found that multiple factors such as age, education, trust in the bank, and user experience significantly influence security awareness among bank customers. The study emphasizes that banks must consider these variables when designing strategies to increase customer security awareness, as a lack of understanding can undermine technological security defences.

2. **Datta&Khurana (2024)** examined online banking security and customer behaviour, noting that as digital banking services grow, customers' perceptions of security protocols and ease of use play a crucial role in their adoption of secure banking services. This research highlights that customer awareness affects not only security behaviour but also trust and willingness to use digital platforms.
3. **Shukla et al. (2025)** reported that many banking customers remain unaware or indifferent toward fundamental cybersecurity practices such as secure password behaviour and fraud reporting. This study demonstrates that, despite confidence in banks' cybersecurity measures, a significant portion of users lack understanding of crucial security practices that reduce risk.
4. **Furqon (2024)**The role of communication and customer education in shaping security behaviour has been stressed in literature highlighted that although digital financial services have expanded, there remains a gap between communication efforts by financial institutions and actual customer behaviour.
5. **Hasan et al. (2025**) financial literacy alone did not significantly change online banking adoption, concerns about data protection and cyber security strongly affected customer trust and satisfaction with online banking services.

Objectives

1. To assess customers' knowledge of banking security technologies used to protect their financial information.
2. To analyse the role of bank staff in communicating security practicesand ensuring customers understand how to keep their accounts safe.
3. To measure customers' perception of safety while using digital banking platforms, including websites and mobile applications.

Theoretical Framework : This study is grounded in two primary theories
Technology Acceptance Model (TAM) – **Davis (1989**This model explains how users come to accept and use technology based on perceived usefulness and perceived ease of use.In the context of banking security, if customers perceive digital banking platforms as secure and easy to use, they are more likely to follow security measures and adopt safe practices.

Protection **Motivation Theory (PMT)** – **Rogers (1975)**PMT suggests that individuals are motivated to protect themselves when they perceive a threat and believe that preventive measures are effective and manageable. Applied here, customers' adherence to security measures (like using OTPs or following ATM safety guidelines) depends on their understanding of threats (fraud, cybercrime) and the perceived effectiveness of security protocols.

Conceptual Framework-A conceptual framework visually represents the relationships between variables in your study.

Variables -Independent Variables (Factors influencing customer understanding):
Customer Knowledge of Security Measures – Awareness of banking security technologies

1. Familiarity with ATM safety guidelines.
2. Awareness of physical safety measures (emergency exits, signage).

Bank Role Communication by bank staff

1. Education on cyber threats.
2. Customer support and guidance.

Dependent Variable

Customers' Level of Understanding of Banking Security Measures

1. Knowledge and application of safe banking practices.
2. Perception of safety while using digital platforms.

Explanation: Customer knowledge and bank role are key determinants of how well customers understand and follow banking security measures. A higher level of understanding leads to better adoption of safe banking practices, reducing the risk of financial fraud and enhancing trust in the banking system.

Research methodology The study adopts a descriptive research design. Descriptive research helps to describe the current status of customers' understanding of banking security measures and examine the influence of demographic factors on awareness and behaviour. The research focuses on measuring awareness, knowledge, and perception among bank customers in Madurai City.Convenience sampling is used to select the respondents. Customers who are available and willing to participate from different banks and branches across Madurai City were included to ensure diversity. while remaining feasible for 100 respondents in Madurai City.

Data analysis and results

Rank 1 : customers perceive bank staff communication about account security as the most effective measure.

Rank 2-5 : Moderate understanding was observed in areas including familiarity with emergency exits, ATM safety guidelines, awareness of bank security technologies, and education about cyber threats**.**

Rank 6: the lowest-ranked area was customers' confidence in using digital banking platforms**,** indicating a need for enhanced education and support in online banking security.

Overall, the results suggest that while banks are effective in direct communication, there are gaps in customers' practical knowledge and digital security confidence.

Q.NO	Understanding Level	Weighted Average					Total	Overall Rank	Category
		5	4	3	2	1			
1	Customer aware that bank uses security technologies.	40	212	87	20	0	359	4	MEDIUM
2	ATM safety guidelines (e.g., covering PIN)	135	220	54	0	0	409	3	MEDIUM
3	familiar with emergency exits	155	244	24	0	0	423	2	MEDIUM
4	Bank staff clearly communicates	200	240	0	0	0	440	1	HIGH
5	Bank educates about cyber threats	0	240	99	14	0	353	5	MEDIUM
6	Feels safe using digitalplatforms website, mobile app).	0	192	135	14	0	341	6	LOW

Chi square test

Null Hypothesis (H_0) There is no significant association between customers' awareness of the bank's use of security technology and the bank's efforts to educate customers about cyber threats.

Alternative Hypothesis (H_1) There is a **significant association** between customers' awareness of the bank's use of security technology and the bank's efforts to educate customers about cyber threats.

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	13.353[a]	6	.038

Since $.038 < .05$, we reject the null hypothesis. This suggests that the distribution of one variable is dependent on the other; they are not occurring together by pure chance.

Findings

The study reveals that customers in Madurai City have a good level of understanding of banking security measures mainly through direct communication from bank staff, which they perceive as the most effective method. However, customers show only a moderate level of awareness regarding ATM safety guidelines, emergency exits, bank security technologies, and cyber threats. The lowest level of understanding is found in customers' confidence in using digital banking platforms, indicating fear and lack of adequate knowledge about online security. Overall, while banks are successful in creating basic awareness, gaps exist in practical knowledge and digital security confidence among customers.

Suggestions

Banks should strengthen customer education on digital banking security by providing simple training sessions, demonstrations, and awareness programs, especially focusing on cyber threats and safe online practices. Since staff communication is effective, bank employees should be encouraged to guide customers regularly about security measures. Information should be shared in simple language and local language to improve understanding. Improving digital support services and continuously educating customers will help enhance their confidence and ensure safer banking practices.

Conclusion

The study reveals that while banks excel in direct communication regarding security, significant gaps exist in customers' digital security confidence. Addressing these gaps through targeted education, improved digital support, and enhanced cybersecurity awareness will strengthen customer trust and promote safer banking practices.Focused awareness initiatives and enhanced customer engagement can significantly improve customers' understanding and confidence in banking security measures.

References

1. Telo (2023)https://journals.sagescience.org/index.php/ssret/article/view/54?utm.
2. Datta&Khurana (2024) From Passwords To Perceptions: A Comprehensive Analysis Of Online Banking Security And Customer Behavior.https://www.granthaalayahpublication.org/Arts-Journal/ShodhKosh/issue/view/20.
3. Kshitij Shukla Research scholar, Department of Commerce, Integral University, Lucknow.
4. Furqon (2024) IJSOC | ISSN : 2715-8780 DOI : https://doi.org/10.54783/ijsoc.v4i1.
5. Hasan et al. (2025) Journal for Social Science Archives 10.59075/JSSA ISSN Online: 3006-3310.