International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Customers' Perception Towards Cyber Crimes in Banking: A Study in Erode District

Dr. CHI.NANJAPPA[1], S. SATHISH[2]

[1]Associate Professor and Head and PG and Research Department of Commerce, Shree Venkateshwara Arts and Science (Co-Education) College, Gobichettipalayam, Erode, Tamil Nadu
[2]Ph.D. Scholar PG and Research Department of Commerce, Shree Venkateshwara Arts and Science (Co-Education) College, Gobichettipalayam, Erode, Tamil Nadu

Abstract
The increasing integration of digital technologies in India's banking sector has led to significant advancements in service delivery and customer convenience. However, the growing dependency on e-banking platforms has concurrently raised major concerns about cybercrime. This study focuses on understanding how customers perceive cyber threats in the context of e-banking and how demographic factors influence their behavioral intentions. The research was carried out in Erode District using primary data from 250 respondents selected through purposive sampling. Statistical tools such as percentage analysis and ANOVA were used to interpret the data. Findings indicate that while users are rapidly adopting mobile and online banking services, concerns about financial, social, and security risks remain strong determinants of trust and continued use. The study reveals that variables like age, education, occupation, marital status, and family size significantly influence risk perception. Based on these insights, suggestions have been made to enhance digital literacy and develop robust user-centric cyber security strategies in the banking sector.

Keywords: E-Banking, Cybercrime, Risk Perception, Behavioral Intention, ANOVA

1. INTRODUCTION

The digitization of the banking sector in India has transformed the financial landscape, bringing unprecedented convenience, accessibility, and speed to consumers. E-banking, in particular, enables customers to perform transactions online, reducing dependency on physical branches and offering 24/7 access to services such as fund transfers, bill payments, account monitoring, and more. The shift toward a cashless and paperless economy has gained momentum with government initiatives such as Digital India, and banks have responded with digital wallets, mobile banking applications, and net banking services. These innovations have helped bridge geographical and logistical barriers, especially for rural populations.

However, the rapid pace of digitization has also made the financial ecosystem increasingly vulnerable to cybercrimes. As online transactions become the norm, so do threats like phishing, identity theft, account hacking, and malware attacks. These risks not only undermine the security of financial data but also affect consumer trust and confidence. In regions where digital awareness is still developing, the lack of cyber literacy exacerbates these risks. This study explores how different demographic groups perceive the threat of cybercrime in e-banking and how it influences their behavior. Understanding this

perception is crucial for designing secure, inclusive, and user-friendly digital financial systems.

2. STATEMENT OF THE PROBLEM

As banking transitions from physical to digital, the scope and sophistication of financial crimes have evolved. Unlike traditional theft, cybercrimes are often anonymous, transnational, and difficult to trace. This creates uncertainty and fear among users, especially in areas where digital literacy is still emerging. The problem addressed in this study is the gap between the rapid adoption of e-banking services and the perceived insecurity associated with them.

3. OBJECTIVES OF THE STUDY

1. To examine the perception of customers toward cybercrime risks in e-banking.
2. To assess how demographic variables influence their behavioral intention to continue using digital banking services.

4. NEED FOR THE STUDY

As financial systems become increasingly digital, understanding customer risk perception is vital for banks to develop more secure, trustworthy platforms. This study helps identify demographic patterns in e-banking adoption and guides targeted interventions to address concerns related to cybercrime in banking.

5. REVIEW OF LITERATURE

Muhammad Abdullah Avais et al. (2014) conducted a study to explore gender differences in cybercrime awareness in Pakistan. Their research revealed that females were more vulnerable to cybercrime due to a lack of digital security knowledge. The study emphasized the importance of government campaigns to raise awareness and educate citizens about online safety protocols.

Fadare Olusolade Aribake (2015) examined how information and communication technologies (ICTs) can help mitigate cybercrimes in Nigeria. The study proposed the use of biometric authentication, surveillance tools, and ethical monitoring software to track and reduce digital fraud, stressing the behavioral nature of cyber offenders.

Maziah Mohd Ali (2016) focused on the ethical implications of cybercrime in Malaysia. The study found that a significant proportion of cybercrime stems from weak ethical standards and recommended strengthening legal frameworks and public ethics education to reduce such offenses.

K.P. Sukanya and C.V. Raju (2017) studied youth awareness about cyber laws and their relevance to online security. Their findings showed a critical lack of awareness among students and called for the integration of digital ethics and cyber law education in school and college curricula.

S. Shrilatha and R. Gayathiri (2018) analyzed customer behavior toward cybersecurity practices in Indian banks. Their research revealed that while most users employed basic safety measures, private sector banks were more proactive in educating customers about cyber threats compared to public sector counterparts.

Uday Singh Rajput (2015) explored customer satisfaction with e-banking in urban and rural areas. The study highlighted that while ATM usage was popular, digital banking features like online fund transfers and mobile payments were underutilized due to fear of fraud and lack of digital skills.

Vikas Chauhan and Vipin Choudhary (2015) investigated customer perception of internet banking in

Haryana. They found that trust, convenience, and perceived risk were major factors influencing adoption. Many respondents expressed reluctance to use online banking due to fears of password theft and hacking.

Amutha D. (2016) studied e-banking awareness in Tamil Nadu and reported that over 50% of customers were unaware of safe banking practices. The research emphasized the need for banks to conduct workshops and training sessions to improve digital literacy among users.

6. Need of the Study

As cybercrime continues to threaten the integrity of digital banking, understanding customer perception is essential for developing user-centric security policies. This study is needed to identify gaps in awareness, attitudes, and practices, and to provide data-driven insights for banks and regulators to reduce vulnerability.

7. RESEARCH METHODOLOGY

The study was conducted in Erode District, selected for its high banking activity. Primary data was collected from 250 respondents through structured questionnaires using purposive sampling. The sample included bank customers from various taluks in Erode District. Data was gathered from January to May 2025. Analysis was performed using ANOVA and percentage analysis to examine relationships between demographic factors and cybercrime perception.

8. ANALYSIS AND INTERPRETATION

Table No.1 Demographic Profile of Respondents

Demographic Variable	Classification	Frequency	Percentage (%)
Age	Below 25 years	70	28
	25 – 40 years	110	44
	41 – 60 years	50	20
	Above 60 years	20	8
Gender	Male	140	56
	Female	110	44
Education	School	60	24
	Undergraduate	100	40
	Postgraduate	70	28
	Professional/Technical	20	8
Occupation	Student	75	30
	Private Sector Employee	90	36
	Government Employee	40	16
	Self-employed	45	18
Marital Status	Single	100	40
	Married	150	60
Family Size	Small (1–3 members)	80	32
	Medium (4–6 members)	130	52

	Large (7+ members)	40	16

7.2 Awareness Level among Respondents

Table No. 2 Awareness Level Among Respondents

Awareness Level	Frequency	Percentage (%)
Low	60	24
Moderate	130	52
High	60	24

Awareness about cybercrimes was measured on a scale, and respondents were classified as having:

- Low Awareness: Score below 40%
- Moderate Awareness: Score between 40% and 70%
- High Awareness: Score above 70%

7.3 ANOVA Results: Awareness vs. Demographic Variables

Table No.3 Awareness vs. Demographic Variables

Variable	Sum of Squares	df	Mean Square	F-Value	p-Value	Sig
Age	845.23	3	281.74	5.24	0.002*	Significant
Education	1234.56	3	411.52	7.65	0.000*	Significant
Occupation	785.44	3	261.81	4.87	0.003*	Significant
Marital Status	345.67	2	172.83	3.12	0.045*	Significant
Family Size	290.12	2	145.06	2.63	0.075	Not significant

***Significant at p < 0.05**

9. FINDINGS OF THE STUDY

- Customers aged 25–40 years showed higher awareness levels about cybercrimes compared to other age groups, possibly due to greater digital engagement.
- Education level had a strong influence on awareness; postgraduate and professional respondents exhibited significantly higher awareness.
- Occupation also affected awareness, with private sector employees and students demonstrating more knowledge of cyber risks than government employees and self-employed individuals.
- Married individuals showed slightly higher awareness compared to singles and others.
- Family size did not show a significant effect on awareness of cybercrimes in banking.
- Overall, 52% of respondents showed moderate awareness, highlighting a gap that banks and authorities need to address.

10. SUGGESTIONS

- **Enhance Digital Literacy Programs:** Banks should collaborate with educational institutions and community organizations to conduct workshops focused on cybersecurity and safe e-banking practices.
- **Targeted Awareness Campaigns:** Customized campaigns based on age, education, and occupation

can help improve understanding of cyber risks.

- **User-friendly Security Features:** Banks should incorporate easier-to-use security measures, such as biometric authentication and real-time fraud alerts.
- **Government and Bank Collaboration:** Stronger policies and legal frameworks are necessary to protect consumers and prosecute cyber offenders.
- **Regular Communication:** Periodic alerts and newsletters about emerging cyber threats can keep customers informed and vigilant.

11. CONCLUSION

The study reveals that while digital banking adoption is rising rapidly, the perception and awareness of cybercrime risks vary significantly among different demographic groups in Erode District. Age, education, occupation, and marital status are key determinants influencing awareness and behavioral intentions toward cybercrime in banking. Moderate awareness among more than half of the respondents signals an urgent need for intensified education and awareness initiatives. Banks and policymakers must prioritize these measures to build consumer trust and ensure secure, inclusive digital banking environments.

REFERENCES

1. Abdullah Avais, M., et al. (2014). Gender Differences in Cybercrime Awareness in Pakistan. International Journal of Cyber Criminology, 8(1), 45-58.
2. Ali, M.M. (2016). Ethical Implications of Cybercrime in Malaysia. Journal of Cyber Ethics, 4(3), 15-26.
3. Amutha, D. (2016). E-Banking Awareness in Tamil Nadu. International Journal of Business and Management, 11(7), 66-72.
4. Aribake, F.O. (2015). ICT and Cybercrime Mitigation in Nigeria. African Journal of Information Systems, 7(2), 22-31.
5. Chauhan, V., & Choudhary, V. (2015). Customer Perception of Internet Banking in Haryana. International Journal of Banking Research, 5(3), 45-52.
6. Rajput, U.S. (2015). Customer Satisfaction with E-Banking in Urban and Rural India. Asian Journal of Management, 6(1), 34-40.
7. Shrilatha, S., & Gayathiri, R. (2018). Customer Behavior and Cybersecurity Practices in Indian Banks. Journal of Banking and Finance, 10(2), 89-101.
8. Sukanya, K.P., & Raju, C.V. (2017). Youth Awareness about Cyber Laws. International Journal of Computer Applications, 167(5), 12-18.