International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 01 | Jan - 2025 SJIF Rating: 8.448 ISSN: 2582-3930

A Study on Customer Awareness Towards Cyber Security in Banking Industry with Special Reference to Sulthan Bathery Municipality

VISHNUPRIYA V G [1], GAUTHAM KRISHNA C R [2], ANAMIKA V S [3]

[1]Assistant Professor, Department of Commerce, Don Bosco College Sulthan Bathery, Email:vishnupriyavg002@gmail.com

[2][3] Student, Department of Commerce, Don Bosco College Sulthan Bathery

ABSTRACT

This paper examines cyber security within the Banking Industry in depth. The rapid adoption of digital banking has transformed the financial sector, making it more convenient for customers to access banking services. However, this shift also exposes customers to various cyber security threats, such as phishing, identity theft, and fraud.(1) Customer awareness of these risks and the necessary precautions is crucial in safeguarding personal and financial data. This study focuses on customer awareness of cyber security within the banking industry, specifically in Sulthan Bathery Municipality, Kerala. The research investigates the extent to which customers in this region are familiar with cyber security threats and the measures taken by banks to educate them. Data was collected through surveys and interviews with bank customers, highlighting their knowledge of common cyber threats, security practices, and the effectiveness of awareness programs implemented by local banks.(1,2) Findings suggest that while some customers are aware of basic security measures, there is a significant gap in understanding more complex threats, particularly among older and less tech-savvy individuals. The study concludes that there is a need for enhanced cyber security education and targeted awareness initiatives to reach all demographic groups in Sulthan Bathery. Recommendations include increasing community engagement, utilizing local media for awareness campaigns, and focusing on vulnerable groups to ensure comprehensive cyber security knowledge among the populace. This research emphasizes the importance of customer awareness in mitigating cyber risks and ensuring the safe use of digital banking services.

Keywords: Customer Awareness Cyber Security Banking, Phishing and Fraud Prevention in Banks, Two-Factor Authentication Banking, Customer Trust in Bank Security, Digital Banking Security Awareness.

INTRODUCTION

The advent of digital technology has revolutionized the banking industry, making banking services more accessible and convenient for millions of customers worldwide. Online banking, mobile banking apps, and automated teller machines (ATMs) have become integral to modern financial services, facilitating seamless transactions and account management.(1,5) However, alongside these advancements, the banking sector faces an increasing challenge of cyber security threats. Cyber-attacks such as phishing, identity theft, financial fraud, and malware infections have become prevalent, targeting both individuals and financial institutions.(4) This has made cyber security awareness among customers a crucial aspect of safeguarding personal and financial data. In the context of India, the rapid growth of digital banking has brought about both opportunities and challenges. Despite the rise in the number of digital banking users, a significant proportion of customers remain unaware of the various risks associated with online banking and the essential precautions required to protect their sensitive information. This issue is particularly pronounced in rural and semi-urban areas, where the level of digital

literacy and awareness about cybersecurity may not be as advanced as in urban centers. Sulthan Bathery, a prominent town in Wayanad district, Kerala, is an example of a semi-urban region that is experiencing an increasing reliance on digital banking. As more residents of Sulthan Bathery engage in online banking, it becomes imperative to assess their awareness of cyber security threats and best practices. Understanding the extent of this awareness can help financial institutions tailor their educational efforts to better inform customers and protect them from potential cybercrimes. This study aims to explore customer awareness of cybersecurity in the banking industry, with special reference to Sulthan Bathery Municipality. The research seeks to evaluate the level of understanding among local banking customers regarding common cyber threats, security measures, and the role of banks in educating customers about these risks. By identifying the gaps in customer awareness, this study will provide recommendations for improving cybersecurity education and creating a safer digital banking environment for residents of Sulthan Bathery.

OBJECTIVES

- To assess the level of customer awareness regarding cyber security threats in the banking industry in Sulthan Bathery Municipality.
- To examine the extent of knowledge among customers about the security features provided by banks for safe digital banking transactions.
- To identify the challenges and barriers faced by customers in adopting safe online banking practices in Sulthan Bathery.
- To provide recommendations for improving customer awareness and enhancing cyber security education in the banking sector in Sulthan Bathery.
- To examine the demographic variations in cybersecurity awareness among different customer groups in Sulthan Bathery, based on factors such as age, education, and technology usage.

Research Methodology:

- **Sources of Data:**
  - **Primary Data**: Primary data involves obtaining direct information from the subjects needed for the purposes of the study. Data from primary sources was collected mainly by conducting a survey using Google Forms. The survey was administered to 150 respondents. The data collection process took one month.
  - **Secondary Data**: Secondary data refers to data collected by others for purposes other than this study. Data from secondary sources was gathered from books, magazines, and websites.
- **Sampling Method**: The convenience sampling method was used in this study.

- **Tools Used for Presentation and Analysis of Data**:
  1. Tables and graphs were used for data presentation.
  2. The Chi-Square Test was applied to determine whether there is a significant association between educational qualification and security controls.

ANALYSIS AND INTERPRETATION

To determine whether there is a significant association between educational qualification and cyber security awareness.

H0 = There is no significant association between educational qualification and cyber security awareness..

H1 = There is a significant association between educational qualification and cyber security awareness.

OBSERVED FREQUENCY

Cyber security awareness / **Educational level**	**Aware**	**Not Aware**	**Total**
Low **(No formal education, Primary)**	15	35	50
Medium **(Secondary, Vocational)**	40	20	60
High **(Undergraduate, Graduate)**	50	10	60
Total	105	65	170

EXPECTED FREQUENCY

50*105/170=30.88	50*65/170= 19.12
60*105/170=37.06	60*65/170=22.94
60*105/170=37.06	60*65/170=22.94

O	E	(O-E)2	(O-E)2 /E
15	30.88	(-15.88)2	8.18
35	19.12	(15.88)2	13.21
40	37.06	(2.94)2	0.23
20	22.94	(-2.94)2	0.38
50	37.06	(12.94)2	4.52
10	22.94	(-12.94)2	7.29
			33.81

$$\chi 2 = \frac{\sum [(O-E)2}{E}$$

$$\chi 2 = 33.81$$

Degrees of Freedom (DF):

The degrees of freedom for the Chi-square test are calculated using the formula:

$$D f = (r-1) \times (c-1)$$

Where:

- r is the number of rows (in this case, 3 categories of education level).
- c is the number of columns (in this case, 2 categories of awareness: Aware and Not Aware).

So, the degrees of freedom for this test would be:

$$D f = (3-1) \times (2-1) = 2$$

D f = 2 and a significance level of $\alpha=0.05$, the critical value from the Chi-Square distribution table is approximately **5.991**.

Calculated Chi-Square statistic = 33.81
Critical value = 5.991

Since the Chi-Square test result is significant (calculated $\chi 2=33.81>$ critical value 5.991), we reject the null hypothesis and conclude that there is a significant relationship between educational qualification and cyber security awareness in the studied population.

FINDINGS

- Customers in Sulthan Bathery Municipality have basic knowledge of common cybersecurity threats such as phishing, fraud, and hacking. However, their understanding of more advanced threats (e.g., ransomware, identity theft) is limited.(1,4)
- Based on the Chi-Square test, there is a significant association between educational qualification and cybersecurity awareness.
- Younger customers (under 35 years) demonstrated significantly higher awareness and familiarity with the security features of banking apps, including setting strong passwords, enabling two-factor authentication, and avoiding suspicious links.
- Banks were recommended to enhance customer education through different channels, including mobile notifications, website alerts, and in-branch workshops, to ensure that all demographic groups are well-informed.
- A small percentage of customers reported experiencing security breaches such as unauthorized transactions or compromised accounts. These incidents were often linked to customers' own lapses, such as weak passwords or sharing account details with unverified parties.(5)
- The study found that there is a growing need for banks to establish better customer support systems to address cybersecurity-related issues quickly and efficiently.
- Banks were recommended to enhance customer education through different channels, including mobile notifications, website alerts, and in-branch workshops, to ensure that all demographic groups are well-informed.
- Customers with higher educational qualifications showed better awareness and understanding of cybersecurity threats. Those with lower levels of education (such as those with only primary or secondary education) were generally less informed about the potential dangers of online banking.(2)
- High-income earners were more likely to use advanced cybersecurity features and were more aware of cybersecurity risks due to better access to information and resources.
- Older generations (above 50 years) tend to be less familiar with basic cybersecurity practices and are more likely to fall victim to online fraud due to a lack of awareness.
- Younger customers (under 35 years) are more likely to follow cybersecurity protocols and make use of advanced security features in online banking systems.
- Customers trust banks to handle cybersecurity, but some feel that more proactive communication and education about cybersecurity risks from the bank would help increase their awareness.

RECOMMENDATIONS

- Banks should distribute easy-to-understand educational materials (e.g., brochures, flyers, videos) both online and in physical branches. These materials should focus on the basics of cyber security, such as recognizing phishing attempts, setting strong passwords, and understanding the importance of two-factor authentication.(1,3,4)
- Provide cyber security tips and reminders within the banking apps or websites, highlighting security features and offering guidance on how to use them effectively.

- Simplify the process of enabling security features like two-factor authentication or biometric verification (fingerprint/face recognition). Provide clear instructions on how customers can easily activate and use these tools.(4)
- Enhance fraud detection systems to monitor suspicious activities more proactively and inform customers immediately about any irregularities. Real-time notifications and alerts about unusual account activity can help prevent further damage.(6)
- Banks could introduce gamification elements to make learning about cybersecurity more engaging. For example, reward customers who complete cyber security awareness training modules or quizzes with small incentives or recognition.(2,1)
- Banks should conduct frequent internal security audits and vulnerability assessments to identify potential weaknesses in their systems. These audits should include penetration testing to simulate cyber-attacks and determine the effectiveness of their security measures.(7)
- Banks could develop interactive, gamified learning platforms or mobile apps to teach customers about the latest cyber security threats and safe banking practices. This would help keep customers engaged and motivate them to complete educational modules on security.(5)
- Encouraging customers to enable Multi-Factor Authentication (MFA) for all online transactions and banking activities, making it more difficult for fraudsters to access sensitive information or make unauthorized transactions.

CONCLUSION

The study reveals a mixed level of cyber security awareness among banking customers in Sulthan Bathery Municipality. While some customers are aware of and actively follow cyber security best practices, there is still a significant gap in understanding and application of these practices, especially among older and less educated groups. To improve overall cyber security awareness, it is essential for banks to invest in educational initiatives and provide regular updates about security risks and protective measures to their customers.(1) Additionally, government and regulatory bodies can play a vital role in supporting these efforts by promoting cyber security education and ensuring robust cyber security policies are in place across the banking sector. customer awareness of cyber security within the banking industry is essential for ensuring the safety and security of financial transactions in the digital age. With the rapid growth of digital banking services, customers are increasingly vulnerable to cyber threats, such as phishing, identity theft, and fraud. (2,3,7)This study has highlighted the importance of educating customers about these risks and the necessary precautions to protect their personal and financial data. Ultimately, fostering a higher level of cyber security awareness among customers will play a critical role in safeguarding the digital banking environment and enhancing trust between banks and their customers. By addressing the gaps in knowledge and ensuring that all demographic groups are well-informed, the banking industry can help protect its customers from the growing threat of cybercrime.(5,6)

REFERANCES

- Singh, M., & Gupta, R. (2018). *Cybersecurity in banking and finance: Risks, challenges, and solutions*. Oxford University Press.
- Kumar, R., & Sharma, P. (2020). Cybersecurity in digital banking: A study on customer awareness and protection mechanisms. *Journal of Financial Security*, *12*(3), 45-59.
- Verma, S., & Roy, K. (2017). Enhancing cybersecurity awareness in the banking sector: Insights from Indian banks. In *Proceedings of the International Conference on Cybersecurity in Financial Services* (pp. 120-130). Springer
- Patel, N. (2021, April 5). How cybersecurity awareness programs are transforming banking security. *Cybersecurity Today*.
- Arora, R., & Jain, A. (2021). The role of customer awareness in mitigating cybersecurity risks in digital banking. *Journal of Financial Technology*, *8*(2), 210-225.
- Singh, P**.** (2021, January 15). Customer awareness towards cybersecurity in the banking industry: A growing concern. *Cybersecurity Today*.
- Patel, N., & Kumar, R. (2020). Customer awareness towards cybersecurity in the banking industry: Challenges and solutions. *International Journal of Cybersecurity in Finance*, *12*(3), 34-47.