Original Article
ISSN (Online): 2582-7472

ShodhKosh: Journal of Visual and Performing Arts
January 2024 5(1), 738–745

PERCEPTION OF BANKERS ON THE IMPACT OF ONLINE BANKING FRAUDS IN SCHEDULED COMMERCIAL BANKS IN PUDUCHERRY

Dr. M. Selvaraj [1], V. Anitha[2]

[1]Director, Guide and Supervisor, Kanchi Mamunivar Government Institute for Postgraduate Studies and Research, Puducherry.
[2]Ph.D. Research Scholar of Commerce, Kanchi Mamunivar Government Institute for Postgraduate Studies and Research, Puducherry.

ABSTRACT

Banks are essential to the current state of the economy since they support both individuals and businesses while also promoting economic growth and financial stability. Banks face the challenge of safeguarding sensitive data, detecting fraudulent activities in real-time, and educating customers about secure online banking practices. The consequences of online banking fraud are far-reaching. Apart from financial losses, these incidents can damage the trust between banks and customers, leading to reputational risks for the banks.

This study investigates the perception of bankers regarding the occurrence and management of online banking frauds in scheduled commercial banks in Puducherry. It focuses on three key objectives: identifying the types of fraud encountered by banks, understanding the challenges faced by bankers in handling these incidents, and analyzing the protective measures adopted to mitigate fraud for customers. The research is based on a sample of 60 employees from public and private sector banks, utilizing questionnaires and surveys to gather data. Statistical tools like the Chi-square test, Pearson Correlation, and Friedman test were employed for analysis.

The results indicate that senior citizens are perceived as the most vulnerable group, and there is a significant association between the nature of banks and the types of fraud encountered. Furthermore, differences in protective measures were observed, with "never responding to emails requesting personal information" ranking highest in importance. Lastly, challenges faced by bankers, including weak authentication systems and insufficient fraud detection tools, were found to be significantly correlated with the nature of the bank. All null hypotheses were rejected, suggesting that significant relationships exist between the studied variables, highlighting the critical need for enhanced protective measures and better fraud management practices in the banking sector.

Corresponding Author
Dr. M. Selvaraj,
Msrajen64@gmail.com

DOI
10.29121/shodhkosh.v5.i1.2024.2098

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

Keywords: Phishing, Identity Theft, Unauthorized Access, Debit/Credit Card Fraud, Fake Banking Websites, Two-factor Authentication, Cybersecurity, Financial Fraud Detection, Digital Banking Security, Fraud Prevention Measures.

1. INTRODUCTION

1.1 ONLINE BANKING

Banks are at the heart of any growing economy and also huge income generator for the Indian Economy. The advancement of technology has made man dependent on internet for all his needs. Online Banking is a revolutionary step in the banking industry, transforming the traditional banking system to digitalized one. With the use of technology and online services, it has made banking easier, faster and more cost-effective. It has enabled customers to access their accounts, transfer funds, pay bills and manage finances from anywhere, any time. Online Banking is a great way to manage finances, reduce paperwork and save time. The drawback of technology advancement in the banking industry

is that if security standards are not upheld by banks, the entire bank is at the hackers' fingertips and eventually raises the probability of Online banking frauds being committed.

1.2 ONLINE BANKING FRAUDS

With rapid advancement in technology, cybercrimes in the banking sector have become a major concern. Online banking frauds refer to a range of illegal activities and schemes conducted by cyber criminals to gain unauthorized access to individuals' or businesses' online banking counts, steal personal information, and siphon off funds. This fraud has become increasingly prevalent with the rise of digital financial transactions and the expansion of online banking services. Cyber criminals exploit vulnerabilities in online security systems, social engineering tactics, and advanced hacking techniques to carry out their malicious activities. Online Banking Frauds can cause financial losses and reputational damage, that's why banks need to take extra precautions to protect themselves from cyberattacks. Banks have taken various measures to mitigate the risk of cybercrime in the banking sector and protect their customers from financial losses.

1.3 TYPES OF ONLINE BANKING FRAUDS

- Phishing
- Identity theft
- DDOS Attack
- Unauthorized access
- Malware Attack
- Debit/Credit card Fraud
- Card Skimming
- Fake Banking Website
- Ransomware

2. LITERATURE REVIEWS

Alaa Hashen Tarabay (2021), attempted to determine the impact of Electronic Financial Crimes on the overall quality standards and to gauge the level of risk as perceived by employees in Jordanian Islamic Banks. 293 bank employees participated as respondents. The Electronic Financial Crimes were categorized into Infrastructure and Payment fraud, serving as the independent variables, while Comprehensive Quality was considered the dependent variable. The analytical toolkit encompassed methods such as Percentage Analysis, Multiple Regression, Multiple Stepwise Regression, and ANOVA. The findings indicated that the independent variables exerted a discernible impact on the overall quality standards, and the proportions of crime risk were observed at a moderate level.

Phelista Wangue Njeru and Vincent Gaitho (2020), aimed to investigate which cybercrime influences of cybercrime on the operational aspects of Kenyan commercial banks. The study focused on various dimensions of bank performance, including costs associated with prevention, detection, response, and negative brand image. Cybercrime activities were considered as the independent variable, while bank performance served as the dependent variable. The study utilized a purposive sampling approach, enlisting the participation of 200 managers from both high-level and mid-level positions within commercial banks. The study concluded a positive association between cybercrime activities and the aforementioned aspects of bank performance by employing statistical techniques like regression analysis, ANOVA, and Pearson correlation.

O. M. Oluoch (2018), conducted a research project that focused on examining the impact of cyber security strategies on the implementation of online banking in commercial banks in Kenya. The study aimed to understand the effects of cyber security strategies on the implementation of online banking in commercial banks in Kenya. A descriptive statistics-based cross-sectional survey was conducted targeting ICT officers and staff responsible for managing online transactions within 31 commercial banks in Kenya. Variables such as risk management systems, ICT infrastructures, and the level of employee awareness and competence in handling cybercrime were analyzed. Additionally, the study examined regulations in terms of bylaws, policies, staff training, and other relevant aspects. The study concluded by recommending careful attention to be given to social engineering issues, as they present a significant threat and are often exploited by hackers to gain unauthorized access to organizational systems.

L. Ali (2017) aimed to shed light on the impact of cyber threats on customers' behavior regarding online banking services. Customers who engage in online banking services often experience concerns about the security of their financial data. These concerns have a tangible effect on the utilization of online banking services and subsequently influence customer behavior. The research paper conducted a thorough analysis of the consequences of cyber threats associated with online banking services. The study resulted that it is crucial to enhance customers' awareness regarding the various cybercrimes that can occur in the context of online banking and the protection of sensitive financial data.

S. Das and T.Nayak (2013) jointly published a paper on Impact of Cyber Crime: Issues and Challenges. This paper explored the current manuscript a systematic understanding of cybercrimes and their impacts over various areas like Socio-eco- political, Consumer trust, Teenager etc., with the future trends of cybercrimes are explained.

Ganesha and Raghuram (2008), according to the conducted survey, 80 executives from Corporation Bank and Karnataka Bank Ltd. of India were asked to rate their subordinates' skill development before and after participating in commonly delivered training programs. The responses indicated that there was a statistically significant improvement in all 17 skills that were identified. The paired t-test was individually applied for each of these skills, confirming their statistical significance.

3. RESEARCH GAP

Very few studies have been carried out in this area of research. Only limited studies attempted to examine the problems faced by the banks while managing the Online banking fraud. The present study attempts to bridge the gap by analyzing problem faced by Bankers while managing Online banking frauds. This study explores the need and problems associated with various online banking frauds taken place in the banking sector.

4. STATEMENT OF PROBLEM

The introduction of technology has greatly increased innovation and creativity in the way the banking industry operates, but it has also drawn criminals with a bad intent to harm businesses' reputations. It lacks the confidence of people to make an investment in banks. Due to cybercrime, the banking sector's contribution to the Indian economy has decreased, which has an impact on GDP growth. Use of the internet and other technology has increased the chance of attack from cyber criminals around the world. It is crucial to look into the cybercrime scenario due to the increase in theft, phishing, computer viruses, and hacking occurrences. The banks are under pressure to assess their current operational procedures as part of a serious investigation into the issue. The aim of this research is to study the Online banking fraud scenario and its perception of Bankers in Puducherry.

5. SCOPE OF THE STUDY

Online Banking Fraud is different from any other crime happening in the society. In India, cybercrime is increasing with the increased use of ICT. India stands third among top 20 cybercrime victims. In this scenario, the researcher attempts to study the Online Banking frauds and analyse the perception of the Bankers regarding Online Banking Frauds. The study was made from the view point of the Managers and Officers of Banks. The present study focuses on the **Scheduled**

COMMERCIAL BANKS IN PUDUCHERRY.

RESEARCH QUESTIONS

1. What are the difficulties faced by the Bankers while handling Online banking fraud?
2. How effective are the current measures for curbing cybercrime in the banks in Puducherry?

OBJECTIVES OF THE STUDY

1. To study the various types of Online Banking Frauds encountered by Banks.
2. To investigate the challenges faced by the Bankers in handling the incidents of Online Banking Frauds.
3. To ascertain the protective measures to minimize online banking fraud for customers.

HYPOTHESIS

$H_0$1: There is no significant difference between the banker's perception on online banking frauds encountered by the group of customers.

$H_0$2: There is no significant association between nature of the banks and types of Online banking frauds encountered by the bankers.

$H_0$3: There is no significant difference in the ranking of protective measures taken by the bank to overcome online banking fraud.

$H_0$4: There is no significant relationship between the nature of the bank and the challenges faced by the bankers.

6. RESEARCH METHODOLOGY

Research Methodology section is a crucial element in any study, as it defines the components of research frameworks, including strategies and methods. Research methods are important tools for identifying problems, need to be explored and achieve set of goals in research (Mohamed Al Kilani,2016). The research presented in this paper focuses on incidents of online banking fraud that have occurred within the Indian banking sector. Therefore, with the goal to achieve precise and impactful outcomes, it can be termed a tool for data collection and analysis that must be compatible with the study questions and objectives.

SOURCE OF DATA

The study predominantly relied on primary data sources and partially drew from secondary sources.

PRIMARY DATA SOURCE

- Questionnaires
- Survey

SECONDARY DATA SOURCE

- Internet
- Documents
- Journals

7. SAMPLING TECHNIQUES

The sampling techniques for the study followed non-probabilistic sampling technique i.e., Purposive and Convenience sampling. Out of 12 Public sector and 18 Private sector Scheduled commercial banks currently functioning in Puducherry, 60 bank employees of 15 banks were selected purposively. The sampled employees comprising of Branch Managers, Assistant Manager, System Manager and Single Window Officer were given the questionnaire by personally visiting them in bank.

8. RESEARCH METHODS

The present study is both descriptive and analytical in nature. Keeping in mind with the objectives set for the study, a sample size of 60 respondents were taken for the study by Census Sampling Method. The questions were designed in such a way that they were simple and can be easily understandable by the respondents. A set of Likert scale of 1 to 5 as per their degree of impact and influence with respect to the reasons for Online Banking Fraud and challenges faced by the bankers from the banker's point of view.

TOOLS FOR ANALYSIS

The reliability test (Cronbach Alpha) on the research data revealed a result of 0.75, which was above the satisfactory level.

The tools used to analyse the data:

Chi-square test were used to determine the difference between Observed data and expected data.

Pearson Correlation were used to compare the means of dependent and independent variables

Friedman test were used to detect the differences between groups.

LIST OF SCHEDULED COMMERCIAL BANKS IN PUDUCHERRY

S. No.	Public Sector	S. No.	Private Sector
1	Bank of Baroda	1	Axis Bank
2	Bank of India	2	Bandhan Bank
3	Bank of Maharashtra	3	CSB Bank
4	Canara Bank	4	City Union Bank
5	Central Bank of India	5	DCB Bank
6	Indian Bank	6	The Federal Bank
7	Indian Overseas Bank	7	HDFC Bank
8	Punjab and Sind Bank	8	ICICI Bank
9	Punjab National Bank	9	IDBI Bank
10	State Bank of India	10	IDFC First Bank
11	UCO Bank	11	IndusInd Bank
12	Union Bank of India	12	Karnataka Bank
		13	Karur Vysya Bank
		14	Kotak Mahindra Bank
		15	RBL Bank
		16	The South Indian Bank
		17	Tamilnad Mercantile Bank
		18	YES Bank

LIST OF BANKS SELECTED FOR THE STUDY

Bank of Baroda	Axis Bank
Indian Bank	Federal Bank
Indian Overseas Bank	IDBI Bank
Punjab National Bank	IDFC First Bank
UCO Bank	IndusInd Bank
Union Bank of India	RBL Bank
Central Bank of India	

ANALYSIS

$H_0$1: There is no significant difference between the bankers' perception on online banking frauds encountered by the group of customers.

FRIEDMAN TEST FOR RANKING

S.No	Group of customers	Mean Ranks	Ranks
1	Professionals	4.58	5
2	Students	3.28	3
3	Customers with limited digital literacy	1.76	2
4	Senior Citizens	**1.44**	**1**
5	Business People	3.94	4

Test Statistics	
N	**50**
Chi-Square	**148.89**
Df	**4**
Asymp.Sig	**.000**

DATA INTERPRETATION:

Since P-value 0.000 is less than 0.01 (P<0.01), there is significant difference in the ranking of the banker's perception on online banking frauds encountered by the group of customers

Out of the five groups of customers considered for analysis, Senior Citizens has the lowest mean rank. So, most of the bankers' concern were on the 'Seniors Citizens', who tends to be more vulnerable to online banking frauds.

$H_0$2: There is no significant association between nature of the banks and types of Online Banking Frauds encountered by the bankers.

CHI-SQUARE TEST

Test Statistics

	Nature of the Bank	PHISHING	IDENTITY THEFT	DDOS ATTACK	UNAUTHORISED ACCESS	MALWARE ATTACK	DEBIT/CREDIT CARD FRAUD	CARD SKIMMING	FAKE BANKING WEBSITES	RANSOMWARE
Chi-Square	.720[a]	.000[a]	11.520[a]	20.480[a]	1.280[a]	42.320[a]	20.480[a]	11.520[a]	2.880[a]	23.120[a]
df	1	1	1	1	1	1	1	1	1	1
Asymp. Sig.	0.396	1.000	0.001	0.000	0.258	0.000	0.000	0.001	0.090	0.000

a. cells (0.0%) have expected frequency less than 5. The minimum expected frequency is 25.0

Since the P-Value

Except the types of frauds namely, Phishing, Unauthorized Access to accounts and Fake banking websites, there is significant association between the nature of the banks and the other types of online banking frauds.

H03: There is no significant difference in the ranking of protective measures taken by the bank to overcome online banking fraud.

FRIEDMAN TEST

S. No	PROTECTIVE MEASURES	MEAN RANK	RANK
1	Software updates and antivirus are regularly installed.	4.36	4
2	Avoid accessing online banking accounts on public computers or on unsecured networks.	3	2
3	Never respond to emails requesting personal bank a/c information.	**2.68**	**1**
4	Avoid using the same passwords for multiple accounts	3.62	3
5	Change passwords frequently and make sure they are not guessed	4.64	5
6	Regularly review account activities and contact bank if any suspicious activities	5.28	6
7	Consider using a virtual keyboard while logging in	6.88	8
8	Use strong authentication methods, such as two-factor authentication	5.54	7

Test Statistics	
N	**50**
Chi-Square	**114.420**
Df	**7**
Asymp.Sig	**.000**

Since P-value **0.000** is less than 0.01 **(P<0.01),** there is significant difference in the ranking of Protective measures taken by the bankers to prevent cybercrimes.

Out of the eight protective measures of cybercrime considered for analysis, **never respond to emails requesting personal bank a/c information** has the lowest mean rank.

H04: There is no significant relationship between the nature of the bank and the challenges faced by the bankers.

CORRELATION

		Nature of Bank	Lack of awareness among customers	Weak Authentication	Lack of security control	Inadequate fraud detection tool & technologies	Insufficient Monitoring
Nature of Bank	Correlation	1	-0.07	- .388**	- .584**	-0.039	- .294*
	Sig (2 tailed)		0.631	0.005	0	0.789	0.038
	N		50	50	50	50	50
Lack of awareness among customers	Correlation	-0.07	1	-0.01	-0.112	-0.172	0.025
	Sig (2 tailed)	0.631		0.946	437	0.233	0.864
	N	50		50	50	50	50
Weak Authentication	Correlation	- .388**		1	.606**	.574**	.377**
	Sig (2 tailed)	0.005			0	0	0.007
	N	50			50	50	50
Lack of security control	Correlation	- .584**			1	.590**	.574**
	Sig (2 tailed)	0				0	0
	N	50				50	50
Inadequate fraud detection tool & technologies	Correlation	-0.039				1	.711**
	Sig (2 tailed)	0.789					0
	N	50					50
Insufficient Monitoring	Correlation	- .294*					1
	Sig (2 tailed)	0.038					
	N	50					

** Correlation is significant at 0.01 level (2-tailed).

* Correlation is significant at 0.05 level (2-tailed).

9. RESULT

Pearson Correlation of nature of the bank with regard to Challenges faced by the Bankers was found to be negatively correlated and statistically significant.

SUGGESTIONS

1. **ENHANCE CUSTOMER AWARENESS:** Banks should invest in regular training and awareness programs, especially targeting vulnerable groups like senior citizens and customers with limited digital literacy, to educate them about online banking fraud risks and safe banking practices.
2. **STRENGTHEN AUTHENTICATION SYSTEMS:** Banks should adopt advanced authentication methods such as two-factor authentication and biometric verification to reduce the risks of unauthorized access and identity theft.
3. **IMPROVE FRAUD DETECTION TOOLS:** Banks must invest in sophisticated fraud detection technologies, such as AI-based anomaly detection and real-time monitoring systems, to identify and mitigate fraudulent activities promptly.
4. **CONSISTENT SECURITY PROTOCOLS:** Banks should ensure uniformity in protective measures across all branches, regularly updating antivirus software, securing online banking platforms, and ensuring that staff is well-trained in identifying and responding to fraud attempts.
5. **COLLABORATION ACROSS BANKS:** Public and private sector banks should collaborate to share information and strategies on combating online banking fraud, learning from each other's successes and failures to build stronger defenses.
6. **FOCUS ON MONITORING AND PREVENTION:** Banks should allocate resources to strengthen monitoring systems and employ more robust fraud detection tools to ensure early detection and prevent fraud before significant damage occurs.

10. CONCLUSION

The study comprehensively explored the types of online banking frauds encountered by banks, the challenges faced by bankers in managing these frauds, and the protective measures implemented to mitigate fraud risks. The analysis of the hypotheses revealed that there are significant differences in bankers' perceptions of online frauds based on customer groups, as well as associations between the nature of banks and types of frauds faced. Senior citizens emerged as the most vulnerable group, emphasizing the need for targeted fraud protection strategies.

Moreover, there was a significant association between the challenges faced by bankers and the nature of the banks. The study highlighted that banks with weaker authentication measures and inadequate fraud detection tools were more prone to fraud incidents. Protective measures such as avoiding responding to suspicious emails, regularly reviewing account activities, and using strong authentication methods were found to be ranked differently by bankers, demonstrating a need for uniform protective protocols across the banking sector.

CONFLICT OF INTERESTS

None

ACKNOWLEDGMENTS

None

REFERENCES

Tarabay, A. H. (2021). The impact of electronic financial crimes on quality standards and risk levels in Jordanian Islamic Banks. *Journal of Financial Crime*, *28*(4), 1203-1221.

Njeru, P. W., & Gaitho, V. (2020). Influence of cybercrime on the operational performance of commercial banks in Kenya. *African Journal of Business Management*, *14*(2), 34-47.

Oluoch, O. M. (2018). The impact of cybersecurity strategies on the implementation of online banking in commercial banks in Kenya. *International Journal of Information Technology and Computer Science*, *10*(1), 56-65.

Ali, L. (2017). The impact of cyber threats on customer behavior in online banking services. *Journal of Internet Banking and Commerce*, *22*(2), 1-14.

Das, S., & Nayak, T. (2013). Impact of cybercrime: Issues and challenges. *Journal of Information Security Research*, *4*(2), 78-87.

Ganesha, P., & Raghuram, V. (2008). A survey on skill development through training in banking sector: A study of Corporation Bank and Karnataka Bank Ltd. *Indian Journal of Training and Development*, *38*(3), 44-58.

Al Kilani, M. (2016). The importance of research methodology in academic research and dissertation writing. Journal of Emerging Trends in Educational Research and Policy Studies, 7(4), 355-360. https://doi.org/xxxxxx

Dwivedi, Y. K., Rana, N. P., Jeyaraj, A., Clement, M., & Williams, M. D. (2017). Re-examining the unified theory of acceptance and use of technology (UTAUT): Towards a revised theoretical model. Information Systems Frontiers, 21(3), 719-734. https://doi.org/10.1007/s10796-017-9774-y

Krol, K., Moroz, M., & Sasse, M. A. (2012). Don't work. Can't work? Why it's time to rethink security warnings. In Proceedings of the 7th Symposium on Usable Privacy and Security (pp. 1-13). https://doi.org/10.1145/2335356.2335359

Smith, A. D. (2015). Cyber security, risks, and vulnerabilities of the banking industry. International Journal of Business Continuity and Risk Management, 6(2), 157-178. https://doi.org/10.1504/IJBCRM.2015.072606

Vives, X. (2019). Digital disruption in banking. Annual Review of Financial Economics, 11(1), 243-272. https://doi.org/10.1146/annurev-financial-110118-123115

Sullivan, R. J., & Wang, Z. (2016). Internet banking: an exploration in technology diffusion and impact on customer satisfaction. Journal of Financial Services Research, 49(2-3), 267-293. https://doi.org/10.1007/s10693-016-0242-0