iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** II **Month of publication:** February 2025

DOI: https://doi.org/10.22214/ijraset.2025.67033

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue II Feb 2025- Available at www.ijraset.com

Digital Banking Frauds and Safety Awareness in Rural Areas of Sonipat: A Customers Perspective Study

Dr. Ramesh Kumar
Associate Professor, Department of Commerce, PGDAV College Eve, New Delhi -110085

Abstract: ***Research Aims: The present study examines the awareness and perception of digital banking frauds among bank customers in the rural areas of Sonipat, aiming to reduce fraud incidents and promote a secure, cashless economy. Design/Methodology/Approach: This study descriptive nature. A sample size of 150 participants was selected. Data were collected via surveys and structured interviews, followed by statistical analysis including ANOVA and correlation analysis. Research Findings: The findings indicated significant demographic variations in awareness levels with gender wise, younger individuals and those with higher education and employment status exhibiting greater awareness of digital banking. Theoretical Contribution/Originality: The study will useful to improve and promote secure and frauds free digital banking services in rural area. The Managerial Implication: This study provides critical insights for banks and policymakers to implement targeted educational campaigns and robust security measures tailored to specific demographic needs, enhancing overall customer safety. Research Limitation & Implications: this study related specific rural area of Sonipat Haryana and sample size is limited to 150 customers. The assessment highlights the need for customized strategies to improve e-banking security and awareness, suggesting that future research should include larger sample sizes and other regions for broader applicability.***
Keywords: Digital frauds, Digital banking, Customer awareness, Security measures, demographic analysis, financial frauds

I. INTRODUCTION

The banking sector has gone through a colossal change with the coming of computerized innovations (Bhasin, 2006). This shift has introduced remarkable comfort and productivity, permitting customers to get to banking administrations whenever and anyplace (Mangala and Lalitha, 2023). Be that as it may, it has additionally increased the weakness to various kinds of misrepresentation (Ololade and Salawu, 2020).

The ascent of e-banking frauds is a developing concern, making it fundamental to understand customer awareness and perception to moderate these perils successfully (Reurink, 2018). This study focus on the awareness of e-banking frauds among bank customers in rural area of Sonipat, Haryana, with a definitive target of reducing misrepresentation incidents and propelling a protected, credit only economy (S and I, 2011).

Advanced banking has changed the financial sector, enabling consistent exchanges and enhancing client experience (Sanjeev, 2006). Regardless of these benefits, the computerized landscape has turned into a breeding ground for modern extortion strategies (V and Choudhary, 2015). E-banking frauds, including phishing, vishing, smishing, and malware assaults, have become increasingly common (Ololade and Salawu, 2020).

Understanding customer perceptions and awareness is basic in developing methodologies to fight these frauds and guarantee the security of computerized exchanges (Pani and Sweetheart, 2014).

This exploration intends to survey the awareness levels of e-banking frauds among customers in Mewat district, a locale portrayed by different financial foundations (Reurink, 2018). By examining different segment factors like age, orientation, training, and work status, this study looks to recognize openings in awareness and give encounters into the viability of current safety measures (S and I, 2011). The revelations will assist banks in Mewat with districting to tailor their instructive missions and improve security shows, eventually fostering a more secure banking climate (Mangala and Lalitha, 2023).

Addressing the particular requirements of various segment gatherings is basic in propelling a protected, credit only economy (V and Choudhary, 2015). This study includes the significance of customer training and the execution of good safety efforts (Sanjeev, 2006).

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue II Feb 2025- Available at www.ijraset.com

II. LITERATURE REVIEW

1) The evolution of e-banking frauds

The evolution of e-banking frauds has seen a significant shift away from conventional real-world strategies and toward sophisticated digital ones. In general, fake banking robberies included direct real-life robberies, impersonations, and false documentation. However, the rapid development of digital technologies has unquestionably altered the nature of these frauds. A significant turning point in this development occurred in the middle of the 2000s, when web banking became widespread and introduced a new class of misrepresentation wagers. Bhasin (2006) gives an intensive certain layout of this change, including how the shift from physical to mechanized stages has expanded the degree and multifaceted nature of bogus activities.

The methods used by con artists have evolved along with computerized financial innovations. Current e-banking fakes are portrayed by their rising unpredictability and refinement. Methods like phishing, in which fraudsters stunt individuals into giving secret information, and smishing, in which they use SMS to achieve comparative fake objectives, have become more normal. In addition, the number of malware attacks that target banking systems to steal data or resources has also increased. These cutting edge systems are ordinarily overall around formed and use advanced creative gadgets, making them harder to recognize and thwart. Mangala and Lalitha (2023) investigate this growing complexity by demonstrating the various modern methods that cybercriminals use to exploit weaknesses in electronic banking systems.

The two banks and their clients keep on confronting new challenges because of mechanical headways. As fraudsters innovate and adapt, the banking industry must constantly improve its security measures and educate customers about the most recent threats and preventative measures. The change from standard to electronic monetary fakes features the requirement for a dynamic and proactive strategy for overseeing deception balance, using both inventive types of progress and client care drives to safeguard against these creating risks.

2) Kinds of E-Banking Cheats

E-banking cheats incorporate numerous noxious activities highlighted exploiting the shortcomings of cutting edge monetary structures. Among the most well-known forms of fraud are phishing, vishing, smishing, and malware attacks. The practice of sending deceptive emails that appear to be coming from legitimate sources and trick recipients into providing private information such as credit card numbers, usernames, and passwords is referred to as phishing. Vishing, also known as voice phishing, is a type of fraud that uses phone calls to achieve similar objectives. Commonly, the guests claim to be bank delegates to take private client information from clients who know nothing about the trick. Smishing is a type of phishing that uses SMS messages to trick people into giving personal information or clicking on suspicious links. The use of harmful software with the intention of infiltrating and causing damage to computer systems, stealing data, or facilitating unapproved transactions is examples of malware attacks (Ololade and Salawu, 2020).

These blackmail types are changed as well as dominating across different monetary regions. Pani and Lover (2014) compared the prevalence of fraud at public and private banks in a comparative study. Public sector banks, which typically deal with a larger customer base and may have a less advanced digital infrastructure, are more susceptible to traditional frauds like phishing and smishing. Then again, private region banks, which normally put more in state of the art security progresses, face more convoluted malware and computerized attacks. The study emphasizes the significance of individualized security strategies that take into account the specific customer profiles and vulnerabilities of various banking sectors.

For successful methods of avoidance and moderation, it is crucial to comprehend the types of e-banking fraud and their prevalence in various financial contexts. Banks can, on a fundamental level, reduce the risk of misrepresentation and enhance the general security of computerized financial services by educating customers about these types of fraud and implementing robust safety measures.

3) In the fight against e-banking frauds, customer education and awareness regarding digital security are of the utmost importance.

Measures for Customer Awareness and Prevention As indicated by Sanjeev (2006), instructed clients are bound to perceive and keep away from fake endeavors, accordingly bringing down the general gamble of misrepresentation. According to Sanjeev (2006), educational initiatives can consist of studios, enlightening brochures, and regular updates regarding brand-new threats and strategies for dealing with them. Clients can be more mindful and less inclined to succumb to stunts on the off chance that they know about the different strategies utilized by rascals (Sanjeev, 2006).

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Despite customer education, banks play a critical role in the implementation of robust security measures and ensure that their customers are well-informed about these measures (V and Choudhary, 2015). Banks can use advanced technologies like multi-factor authentication, encryption, and real-time fraud detection systems to protect their digital platforms (V and Choudhary, 2015). According to V and Choudhary (2015), they should also be able to effectively communicate with their customers about these security features and offer guidance on how to use digital banking safely.

A comprehensive strategy for preventing e-banking frauds is developed through the incorporation of client education and high-level security measures. Banks can give assets that engage clients to safeguard their own monetary information, send cautions and alerts about dubious exercises, and direct ordinary instructive courses (V and Choudhary, 2015; (2006), Sanjeev According to Sanjeev (2006), banks and their respective customers must work together to create a secure banking environment. As digital banking develops, education advancement and the application of cutting-edge security technologies will continue to be crucial safeguards against e-banking fraud (V and Choudhary, 2015; (2006)

4) Points of view from both a worldwide and a territorial point of view

The worldwide financial industry is significantly impacted by the monetary misrepresentation peculiarity. A comprehensive composing review by Reurink (2018) examines the different kinds of money related cheats, their turn of events, and the goliath influence they have on monetary foundations all over the planet. As a result of these scams, customers lose faith in banking systems and incur significant financial losses. Various high-profile misrepresentation episodes have shaken the worldwide financial industry, inciting the reception of more modern extortion identification and anticipation advancements and more tight administrative systems (Reurink, 2018)

In the Indian setting, the monetary region faces unequivocal challenges and entryways with respect to overseeing money related swindles. S and I (2011) say that the rapid growth of digital banking services in India has brought both benefits and risks. Weaknesses are clear a result of the extraordinary monetary scene and clients' changing degrees of computerized proficiency. In India, public area banks serve a bigger populace that is regularly less mechanically wise, making them especially defenseless against normal types of extortion like phishing and smishing. Despite being more technologically advanced, private sector banks nonetheless face sophisticated cyber threats like malware and advanced persistent threats (S and I, 2011).

India's administrative environment has been evolving to address these issues. The Save Bank of India (RBI) and other government agencies are organizing efforts with the goals of improving the security foundation of banks and expanding client education on computerized security exercises. In any case, the ampleness of these activities shifts across different areas and banking affiliations. S and I (2011) assert that a more unified and comprehensive methodology that incorporates cutting-edge technological solutions, robust regulatory frameworks, and extensive customer awareness programs is required.

The two banks and administrative specialists should cooperate to resolve these issues. By using in general endorsed techniques and fitting them to the Indian setting, the monetary region can redesign its flexibility against deception. According to S and I (2011), improvements can be made by utilizing cutting-edge technologies, collaborating across institutions, and increasing investments in customer education initiatives. Understanding the perspectives on financial fraud from both a global and a regional perspective makes it easier to develop more effective strategies to protect the banking sector in India and elsewhere.

A. Objectives Of The Study

To study the awareness and customers perception towards digital banking frauds and safety in rural area of Sonipat

B. Hypotheses

H1: There is a significant difference in awareness levels of digital banking frauds between men and women in rural area of sonipat
H2: Age has a significant impact on the perception of digital banking fraud risks.
H3: Educational level influences the effectiveness of safety awareness measures.
H4: Employment status affects the frequency of encountering digital banking frauds

III. METHODOLOGY

A. Research Design

An analytical research design was employed to assess the awareness of digital banking frauds among customers in rural areas of Sonipat, Haryana.

B. Sample Selection

A total of 150 participants were selected through personal meet-ups, including 70 women and 80 men.

C. Data Collection

- Surveys and structured interviews were conducted to gather data on customer awareness and experiences with digital frauds.
- Questions focused on the types of fraud encountered awareness levels, and the perceived effectiveness of safety measures.

D. Data Analysis

Demographic Analysis

- Gender Distribution: 70 women (46.67%) and 80 men (53.33%).
- Age groups: 18-25, 26-35, 36-45, 46-60.
- Educational levels: Below high school, high school, undergraduate and postgraduate.
- Employment status: Employed, unemployed, students, retired.

Table 1: Demographic Analysis

Demographic Variable	Frequency	Percentage (%)
Gender (Women)	70	46.67
Gender (Men)	80	53.33
Age 18-25	40	26.67
Age 26-35	50	33.33
Age 36-45	30	20.00
Age 46-60	30	20.00
Education Below HS	20	13.33
Education HS	50	33.33
Education UG	50	33.33
Education PG	30	20.00
Employed	60	40.00
Unemployed	40	26.67
Students	30	20.00
Retired	20	13.33

(Sources: Primary data)

E. Hypothesis Testing

Table 2: Awareness Levels by Gender: ANOVA Analysis

Source	Sum of Squares	df	Mean Square	F	p-value
Between Groups	156.25	1	156.25	4.56	0.034
Within Groups	5025.75	148	33.94		
Total	5182.00	149			

(Sources: Primary Data)

The ANOVA examination of awareness levels by gender indicates a tremendous difference between men and women. How much squares between bunches is 156.25 with a degree of freedom (df) of 1, resulting in a mean square of 156.25. How much a square inside bunches is 5025.75 with 148 degrees of freedom, leading to a mean square of 33.94. The calculated F-value is 4.56 with a p-value of 0.034. This p-value is less than the standard significance level of 0.05, suggesting that there is a measurably tremendous difference in the awareness levels of digital banking frauds between men and women in rural area of sonipat. Men appear to be more aware of e-banking frauds compared to women, featuring a need for targeted awareness projects to bridge this hole.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Table 3: Perception by Age Group: ANOVA Analysis

Source	Sum of Squares	df	Mean Square	F	p-value
Between Groups	295.60	3	98.53	5.78	0.001
Within Groups	2517.40	146	17.25		
Total	2813.00	149			

(Sources: Primary Data)

The ANOVA investigation examining the perception of digital banking fraud gambles across different age bunches shows basic variety. How much squares between bunches is 295.60 with 3 degrees of freedom, resulting in a mean square of 98.53. How much squares inside bunches is 2517.40 with 146 degrees of freedom, leading to a mean square of 17.25. The F-value is calculated to be 5.78 with a p-value of 0.001. Given that this p-value is fundamentally less than 0.05, it indicates that age altogether influences the perception of e-banking fraud gambles. Younger age gatherings (18-25 and 26-35) tend to have a higher perception of fraud gambles compared to older age gatherings (36-45 and 46-60), suggesting that younger people may be more attuned to digital dangers or conceivably more frequent users of digital banking services.

Table 4: Education Level and Awareness: Correlation Analysis

Variable	Correlation Coefficient (r)	p-value
Education Level	0.65	0.0001

(Sources: Primary Data)

The correlation investigation between education level and awareness of digital banking frauds reveals areas of strength for a relationship. The correlation coefficient (r) is 0.65, showing a critical positive correlation. The p-value for this correlation is 0.0001, which is exceptionally basic. This result suggests that higher education levels are associated with greater awareness of digital banking frauds. People with undergraduate and postgraduate education are more likely to be aware of different types of digital banking frauds and the measures to prevent them, compared to those with simply secondary school education or below. This emphasizes the importance of educational initiatives in enhancing fraud awareness.

Table 5: Employment Status and Frequency of Fraud Encounter: Correlation Analysis

Variable	Correlation Coefficient (r)	p-value
Employment Status	0.58	0.0003

The correlation investigation between education level and awareness of e-banking frauds reveals areas of strength for a relationship. The correlation coefficient (r) is 0.65, showing a critical positive correlation. The p-value for this correlation is 0.0001, which is exceptionally basic. This result suggests that higher education levels are associated with greater awareness of e-banking frauds. People with undergraduate and postgraduate education are more likely to be aware of different types of e-banking frauds and the measures to prevent them, compared to those with simply secondary school education or below. This emphasizes the importance of educational initiatives in enhancing fraud awareness.

IV. DISCUSSION

A. Demographic Varieties in Awareness

The results of this study show that customers in rural area of Sonipat district have very different perceptions and levels of awareness of digital banking frauds. According to earlier research (Sanjeev, 2006), gender differences can influence digital literacy and engagement with online security practices. Men showed higher levels of awareness than women did. This uniqueness highlights the need for orientation explicit instructive ventures to guarantee that all clients are similarly educated about potential computerized financial dangers.

B. Age and Awareness Levels

Age also emerged as significant influences on digital banking fraud awareness. When compared to their elders, younger members, particularly those between the ages of 18 and 25, and those between the ages of 26 and 35, displayed higher levels of awareness.

Younger people's increased knowledge of digital technologies and use of online banking services may be to blame for this trend (Mangala and Lalitha, 2023). Subsequently, mindfulness missions should consider age-explicit procedures, utilizing stages and concentrated strategies that actually reach and connect with various age social affairs.

C. Job of Training

Training level was found to have solid areas for a relationship with consciousness of e-banking fakes. Individuals with advanced education levels, similar to undergrad and postgraduate certifications, were bound to know about various misrepresentation types and preventive measures (V and Choudhary, 2015). This finding highlights the fundamental role that education plays in providing individuals with the knowledge they require to safely navigate the digital banking landscape. Banks and monetary establishments should consequently focus on instructive drives that improve computerized education among all client sections.

D. Business Status and Extortion Experience

Business status moreover out and out affected the recurrence of experiencing e-banking cheats. According to Ololade and Salawu (2020), employed people reported having more frequent encounters with e-banking frauds. This may be because they use digital banking services more frequently for business-related transactions. This recommends that utilized individuals could profit from designated planning and assets given by their bosses in a joint exertion with monetary establishments, pointed toward improving their ability to perceive and answer extortion endeavors.

E. Ideas for Banks and Technique Producers

These encounters highlight the requirement for banks and policymakers to execute designated instructive missions and good safety efforts customized to the particular necessities of various segment social affairs (Pani and Sweetheart, 2014). By tending to the novel weaknesses and prerequisites of each social affair, banks can upgrade in general client security and trust in advanced banking. For example, more seasoned clients and ladies could profit from more escalated and regular extortion mindfulness planning, while more youthful and utilized individuals could be designated through computerized channels and working environment getting ready projects.

Generally, the review highlights the significance of a complex method for managing misrepresentation counteraction, uniting progressed innovative arrangements with complete client training drives to relieve the dangers related with e-banking cheats (Reurink, 2018). In the rural areas of Sonipat banks can effectively reduce fraud and promote a secure, cashless economy by cultivating an informed and cautious customer base.

V. CONCLUSION

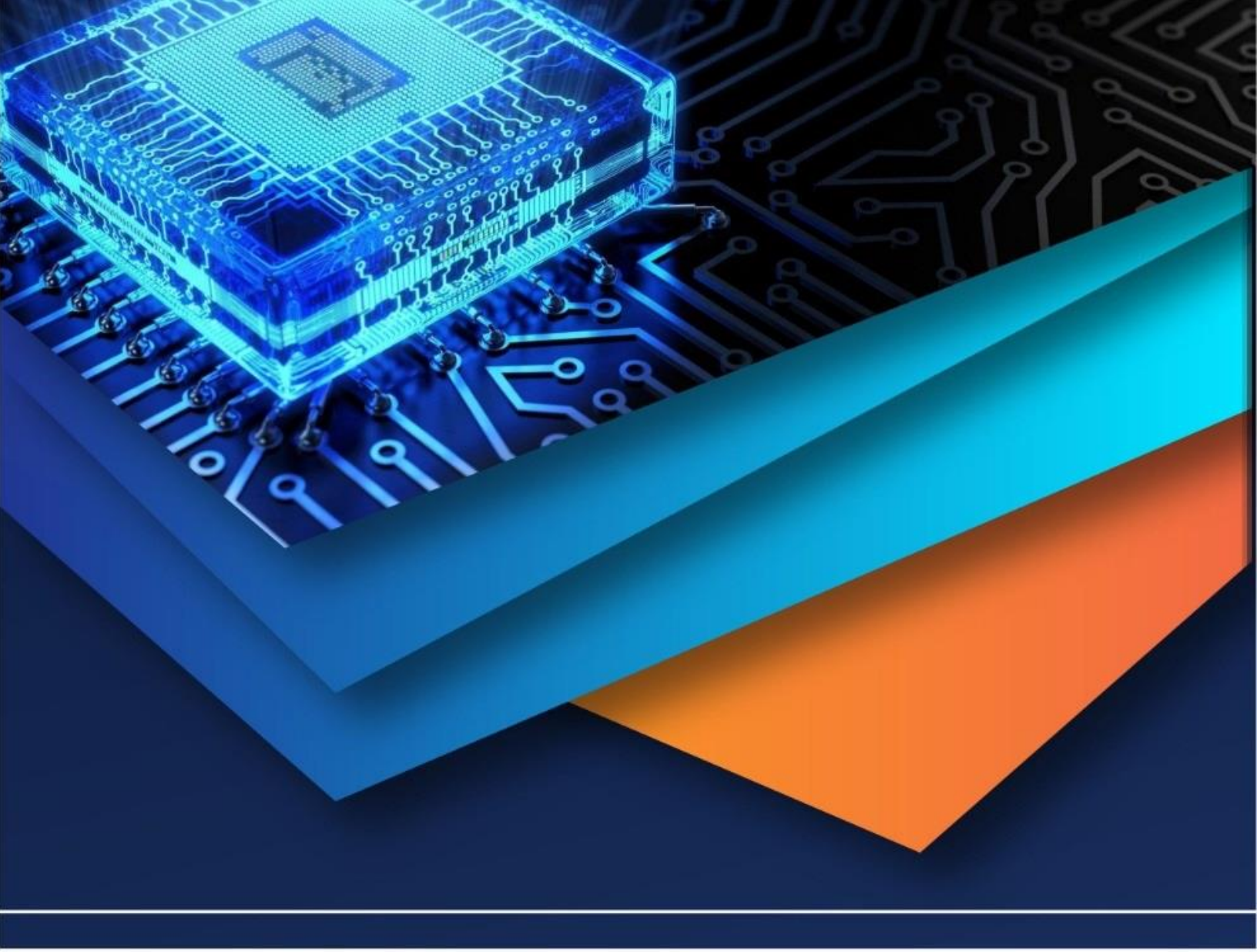
This study underscores the fundamental importance of understanding customer awareness and perception to effectively battle digital banking frauds. The discoveries feature basic demographic varieties in awareness levels, with men, younger people, and those with higher education and employment status exhibiting greater awareness. By addressing the specific needs of these different demographic gatherings, banks can accommodate their security measures and educational missions to enhance customer safety and confidence in digital banking. This targeted approach is essential for propelling a secure, cashless economy. Future research should mean to expand the scope of this study to other regions and include larger sample sizes for a more comprehensive investigation, ensuring that the pieces of knowledge gained are extensively applicable and can illuminate strategies to mitigate digital banking frauds on a wider scale.

REFERENCES

[1] Bhasin, L. M. (2006). Guarding Privacy on the Internet. 7(1). Conference of State Bank Supervisors (CSBS). (2024). Research and policy conference. Retrieved from https://www.csbs.org/sites/default/files/2024-06/CBRC%20pubs/CB21pub_2018_Final.pdf
[2] DashDevs. (2024). 5 challenges of digital transformation in banking. Retrieved from https://dashdevs.com/blog/5-challenges-of-digital-transformation-in-banking/
[3] DashDevs. (2024). Managing bank fraud and high-risk customers: A-Z guide. Retrieved from https://dashdevs.com/blog/bank-fraud-and-money-laundering-prevention/
[4] Electric AI. (2024). High-profile company data breaches. Retrieved from https://www.electric.ai/blog/recent-big-company-data-breaches
[5] InbuiltData. (2024). Future of finance: The growing use of AI in banking. Retrieved from https://www.linkedin.com/pulse/future-finance-growing-use-ai-banking-inbuiltdata-revolutionizing-gxvwc

[6] International Journal of Research Publication and Reviews (IJRPR). (2024). Cybersecurity in banking. Retrieved from https://ijrpr.com/uploads/V5ISSUE6/IJRPR30421.pdf
[7] Mangala, D., & Lalitha, S. (2023). A Systematic Literature Review on Frauds in Banking Sector. Journal of Financial Crime, 30, 285-301(17).
[8] Ololade, M. B., & Salawu, K. M. (2020). E-Frauds in Nigerian Banks: Why and How? Journal of Financial Risk Management, 9(3).
[9] Pani, L. K., & Swain, S. (2014). Comparative Analysis of Retail Banking Between Private and Public Sector Banks in Odisha. Indian Journal of Applied Research 4(3).
[10] Coleman, B.,Campbell,P.C., Mclaughlin,T.J.Walker,V.,& Bourne,P.A. (2024). E-banking fraud in Jamaica: A cross-sectional quantitative study. Retrieved from https://www.researchgate.net/publication/381524381_Ebanking_Fraud_in_Jamaica_A_Cross-sectional_Quantitative_Study
[11] Abdulrazaq,S., Yinusa A,O.& Ajadi,I.A. (2024). Effect of e-banking services on customers' satisfaction in University of Ilorin, Ilorin, Kwara State. Retrieved from https://www.researchgate.net/publication/381505534_Effect_of_EBanking_Services_on_Customers'_Satisfaction_in_University_of_Ilorin_Ilorin_Kwara_State
[12] Reurink, A. (2018). Financial Fraud: A Literature Review. Journal Of Economic Surveys, 32(5), 1292-1325.
[13] S, R., & I, S. M. (2011). Impact of Electronic Crime in Indian Banking Sector. The International Journal of Business and Information.
[14] Sanjeev, G. M. (2006). Data Envelopment Analysis for Measuring Technical Efficiency of Banks. The Journal of Business Perspective, 10(1).
[15] TechMagic. (2024). Core banking modernization: Navigating through challenges. Retrieved from https://www.techmagic.co/blog/core-banking-modernization/
[16] The Digital Banker. (2024). Exploring the future of AI in retail banking. Retrieved from https://thedigitalbanker.com/exploring-the-future-of-ai-in-retail-banking/
[17] V, C., & Choudhary, V. (2015). Internet Banking: Challenges and Opportunities in Indian Context.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)