A STUDY ON AWARENESS OF E-BANKING FRAUDS WITH REFERENCE TO BANKCUSTOMERS IN KERALA

Aravind T Sajeev[1], Archana R Nair[2], Dr. Prasanth A P[3]

[1&2] *Final Year M. Com Students, Department of Commerce and Management, School of Arts, Humanities and Commerce,Amrita Vishwa Vidyapeetham, Kochi*

[3] *Assistant Professor, Department of Commerce and Management, School of Arts, Humanities and Commerce, Amrita Vishwa Vidyapeetham, Kochi*

archanarajeev173@gmail.com, prasanthap@kh.amrita.edu

8075832664, 9539609489

Corresponding Authors: Archana R Nair, Dr. Prasanth A P

Abstract: Electronic banking frauds refer to any type of fraudulent activity that involves the use of electronic banking systems or online banking services in order to steal money, personal information or other financial assets from customers. The objective of the study is to create anawareness about various factors of banking frauds among customers, to measure how well thebanking customers are aware about banking frauds. Questionnaires are used to collect the information from the bank customers in Kerala. The study was conducted on 65 respondents which include 43 female 22 male. The participants ranged in age from 18 to 55. The customersare suggested to use only authenticate, safe, secure and trusted websites of banks to eliminate the online banking frauds and avoid use of public or open Wi-Fi network for online banking transactions.

Keywords: Awareness, Detection, Scam, Banking frauds

1. Introduction

Today’s world is enormously changing now and then more with the predominance of modern technologies. In these days, Digital device convergence makes bank customer to spends their time on “Virtual platforms” and thereby, preference towards digital conservations of cashless E-transaction emerge. As Banking industry being a service based one, it is necessary for the banks to figure out the customer requirements, their awareness, contentedness, security issues, challenges faced by customers in usage of Online banking and preventive measures to alleviate online banking frauds.

The practice of E-banking had become so widespread, boom of online banking throughout the worldwide had quadrupled in stealing sensitive login credentials of valuable customer information causing havoc in the banking sector threats rising at alarming rate, almost had doubled in Online banking frauds. The significance of online banking frauds has been so jeopardized that they are frequently viewed as wrathful trickster instruments. The reputation of the banks will be harmed by the frequent occurrence of online banking frauds. In addition to being illegal and punishable offences, bank frauds are regarded as white-collar crimes. Because of many loopholes in the banking industry, unscrupulous elements indulge in a large number of modus operandi for committing fraudulent activities on online banking.

The report on the advances and patterns in Indian banking for the nine-month period ending in March 2022 is being made accessible by the Government of India's Reserve Bank of India (RBI). The report highlighted that fraud cases involving ₹ 87 crore were reportedby banking entities during this period, as compared to ₹ 60 crore reported during the same period last year. Additionally, cash frauds have also seen an increase, with 589 frauds involving ₹ 81 crore reported in the 6-month period. The report also mentioned that the number of fraud cases reported by private banks were higher than those reported by PSU banks, however, the share of PSBs in terms of the amount involved was 66.7%. The RBI report also noted that the modus operandi of frauds has shifted to card or internet-based transactions.

Online Banking

Internet banking and electronic banking are alternative titles for it. Users is able to financial transactions online combined with the help of online banking. Because online banking became available, customers may now fulfil the vast majority of their key banking needs without physically going to a bank location. Anywhere they choose-at home, at work, or while traveling—anyone is able to conduct all the key financial operations at their own convenience.

Definition of fraud

Fraud is defined as "any behavior by which one person intends to gain a disadvantage over another" by Chakrabarty in 2013. In a nutshell, fraud is any act or omission which has the goal of helping one party at the cost of another, whether by falsifying the fact or in any other manner. The Indian Penal Code's Section 421 defines “Fraud as whoever dishonestly orfraudulently removes, conceals or delivers to any person, or transfers or causes to be transferredto any person, without any consideration, any property, intending thereby to prevent, or knowing it to be likely that he will thereby prevent, the distribution of that property accordingto the law among his creditors or any other person, shall be punished with imprisonment of either description for a term which may extended to two years or with fine or with both”.

Bank Frauds

The Indian economy rely largely on banks. Section 17 of the Indian Contract Act of 1872 states fraud as "Any act by which one person intends to achieve a disproportionate advantage over another." Any unauthorized acquisition or acceptance of money from a financial institution, such as a bank, can be referred to as bank fraud and is considered as a fraudulent and/or unlawful conduct by a person or organization. It is a professional crime, an unlawful act and a criminal offence also. When someone makes use of illegal procedures for obtaining cash, assets, or other kinds of property through financial institutions, it is said that they have engaged in bank fraud. False information and fraudulent promises tend to be used in an effort to increase profits. The two primary causes for the increasing incidence of bank frauds are the complexities of financial transactions and the inability to strictly adhere to branch operation procedures. The number of bank frauds is rising yearly as a result of the banking system's many shortcomings.

Frauds in Online Banking

It's vital to be aware of the potential risks and take measures to protect your information as a way to safeguard against online banking fraud. Use an encrypted web browser, and make sure the security secures on the device are updated. Use safe login credentials at all times, and never share them with anyone. Never click on any links or attachments acquired by someone you don't know, and be suspicious of unsolicited emails or calls asking for personal or financial information. In conclusion, get in contact with your bank immediately if you suspect that your online banking account might have been hijacked. Nowadays, a lot of individuals utilize online banking services to check their balances, make purchases, bill payments, transfer cash, print statements, etc. In most instances, to prevent fraudulent transactions, the user identity usually includes the customer identity number and password. But you could easily fall into the control of cybercriminals due to simple ignorance or negligent actions.

2. Review of literature

Fernandes, L. (2013). He emphasizes how the internet needs to expand business opportunities and how fraudsters are coming up with innovative, sophisticated scams. The cost of the trading company trying to manage fraudulent activities has been significant and rising. The overview of e-payment fraudulent activities in this paper. It gives information on actual payment frauds as well as revenue losses as a result of fraud. The concept of fraud detection and prevention is explained in more detail. The purpose of this research is to take investigative and preventive steps, as well as countermeasures to lessen their effects, in order to reduce fraud in e-payment transactions and the associated revenue loss. This paper's main objective was to examine the current state of fraud in the economy, including the distinct types of fraud and the resulting revenue losses. The scope of the study is decided upon to use secondary sources, with a focus on fraud prevention and detection. The article's primary objective is to decrease both of the as well as the possibility which will be fraud occur in e-payment transactions cash of lost due of fraud.

Reurink, A. (2019). He analyses the different the types context of the financial fraud in the economy, its prevalence and impacts as identified by previous research, as well as the organizational functions that analysts believe encourage it. It performs as a jumping-off point for more research into the causes and consequences of financial fraud. Moreover, it facilitates in pointing out areas which require further study. The paper provides evidence the that additional analysis is necessary on the economic and market structures that support financial fraud, as well as the role of financial intermediaries by so doing. The paper draws the conclusion that in understanding essential to consider the implications of financial fraud, it is the greater social and economic context in which it occurs.

Siddique, M. I., & Rehman, S. (2011). He highlights that the impact of e-retailing practices on consumer–an overview. This study explores how the rise of information and communication technology has created more opportunities for electronic crimes, such as denial of service attacks, identity theft, phishing, money laundering, credit card fraud, spamming, viruses, unauthorized entry, information tampering, cyber stalking, phone napping and click jacking. They provide a few suggestions for how banks can ensure secure online banking, such as appointing reliable officers, creating customer awareness of their rights and duties, and using updated technology.

Sheikh, B. A., & Rajmohan, P. (2017). He acknowledges India's adoption of digital banking. An electronic advancement in the financial sector has been prompted by the implementation of electronic banking. Leveraging a range of banking operations has been made possible by the dynamic and adaptable nature of these communication channels as well as their based-on geography reach. Digital banking, also referred to as electronic fund transfer (EFT), is simply the process of transmitting money directly from one account to another using electronic means. This study emphasizes how social engineering, the use of unauthorized digital certificates, the decryption of sensitive data, and the impersonation of OCR (Optical Character Recognition) paved the way for fraudsters in internet banking in an otherwise weak security environment.

Bhasin, M. L. (2015). He conducted qualitative research based on cluster analysis. The author found that many bank frauds cases have been piling up in courts for many years. He identified that overburden of bank staff makes them to indulge in bank frauds and the policy of "Zero-tolerance" is not followed in Indian banks. The author suggested that staff working in sensitive services should have periodical rotation of bank services, multi-level scrutiny to be adopted for transactions and adoption latest technologies will enable banks and customers to minimize the banking frauds

Pooja, M. He highlights that unreported figures of Indian banking frauds are in rising trend, fraud arises in all sectors, advancement in technology is one of the key factors in massive fraud. Authors classified bank frauds into three main categories such as KYC related frauds, advances related frauds and technology related frauds. Internet banking frauds, ATM frauds, and other payment options like prepaid cards, credit cards, and debit cards have all enhanced due to cyber risk. Hackers are much more fruitful as web, mobile, cloud, and social media usage starts to rise to rise. The findings indicate that 10 fraudsters used to have a field day with their happy hunting thanks to electronic transactions. Building cyber risk management initiatives should be a prime consideration for government entities like that of the CBI, CBDT, CBEC, CVC, andRBI if they want to guarantee secure, and vigilant online banking transactions.

M. A. J. Sakti, N. A. Achsani, and F. Syarifuddin (2018). He highlights the fact that financial scandals and fraudulent activities are widespread and have occurred in all eras and countries. Due to the significant rising trend in financial fraud, forensic accounting has attracted prominence. Forensic accounting is a field that integrates accounting, auditing, and investigative knowledge and experience and experience. Forensic accountants (FAs) have more opportunities than it has ever been. They employ a large number of organizations, which include insurance firms, banks, police departments, and the government, or engage in public practice. By actually putting a scenario, rebuilding financial records, and trying to follow a trail of evidence, FAs typically put together a puzzle. In this article, numerous forensic accounting perspectives and prospects for the future are examined.

(2015). Lokhande, P. S., and Meshram, B.B. Data theft analysis using digital forensics. He highlights that up-gradation in the usage of technology made populace unaware of felonious transactions in net banking. The methods used by fraudsters such as phishing mails, key loggers, spoofed page, redirecting the users link and SIM card cloning are not familiar to customers. Authors made out in the case study that one victim, the customer of Union Bank of

India received a SMS regarding the name change in the beneficiary account for transfer of payment. The victim ignored the SMS considering that as a usual SMS. Later, after 24 8 hours the victim received another SMS that Rs.4.60 lakhs has been transferred to Standard Chartered Bank. The victim realized that his account had been hacked and he filed a complaint under various sections of IPC and ITA 2008. Police investigated and tracked that hackers used five different locations to access the Internet server of IP address from Hong Kong city location of TV media Company; Police found out that the fraudsters purchased jewellery worth Rs. 1.90 lakh from Allahabad. Authors concluded that sophisticated and advanced tools are used for hacking the account of unwary customers and stealing money from their account. Authors suggested that banking sector must take steps to make aware of the banking customer regarding threats in transactions in net banking transactions.

3. Objective of the study

In particular, the key objective is to find out if there's awareness of internet banking and

what chapter objectives are follows:

To study about awareness about various factors of banking frauds among customers.

To measure how well the banking customers are aware about banking frauds

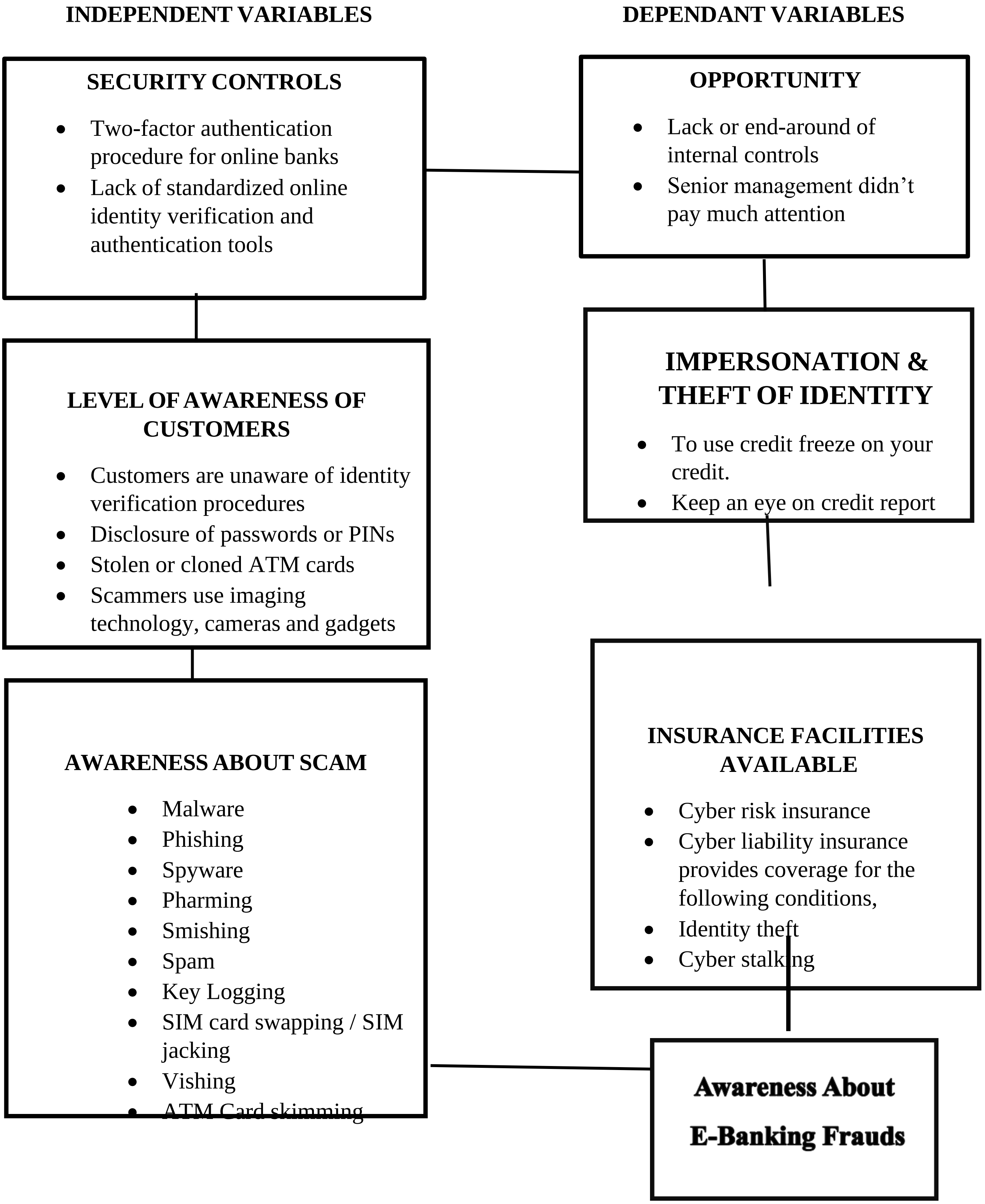
To identify the tools and measures to prevent and mitigate the chances of frauds in Banking Sector.

3. Research methodology

Descriptive Research has been used to conduct the study. The samples were collected using Purposive Sampling technique. Questionnaires are used to collect the information from the bank customers in Kerala. For this purpose, literature and previous studies are studied from reliable journals, studies, reports, websites. Likert scale is used for the survey as it provides a structured way of measuring participants opinion. The study was conducted on 65 respondents which include 43 female 22 male. The participants ranged in age from 18 to 55.

6. Conceptual framework

The study will be based on the awareness of the banking customers about the online banking frauds. The conceptual framework shows the relationship between the dependent and independent variables.



INDEPENDENT VARIABLES

DEPENDANT VARIABLES

SECURITY CONTROLS

- Two-factor authentication procedure for online banks
- Lack of standardized online identity verification and authentication tools

OPPORTUNITY

- Lack or end-around of internal controls
- Senior management didn't pay much attention

LEVEL OF AWARENESS OF CUSTOMERS

- Customers are unaware of identity verification procedures
- Disclosure of passwords or PINs
- Stolen or cloned ATM cards
- Scammers use imaging technology, cameras and gadgets

IMPERSONATION & THEFT OF IDENTITY

- To use credit freeze on your credit.
- Keep an eye on credit report

AWARENESS ABOUT SCAM

- Malware
- Phishing
- Spyware
- Pharming
- Smishing
- Spam
- Key Logging
- SIM card swapping / SIM jacking
- Vishing
- ATM Card skimming

INSURANCE FACILITIES AVAILABLE

- Cyber risk insurance
- Cyber liability insurance provides coverage for the following conditions,
- Identity theft
- Cyber stalking

Awareness About E-Banking Frauds

Analysis and Interpretation

Table 1: Demographic Profile of the Respondents.

Variables	Classification	No of respondents (n=65)	Percentage (%)
Gender	Male	22	33.84
	Female	43	66.15
Age (in years)	18-25	51	78.46
	25-30	8	12.30
	35-50	3	4.61
	Above 50	2	3.07
Educational qualification	12th grade or less	6	9.23
	Diploma	1	1.53
	Bachelor’s degree	32	49.23
	Post graduate degree	26	40
Occupation details	Private sector	15	23.07
	Government sector	2	3.07
	Corporate sector	6	9.23
	Banking sector	1	1.53
	Student	41	63.07

The awareness about E-banking frauds of the respondents is analyzed and the results shows that majority (66.15%) of the respondents are Female and 78.46% of them belong to the age of 18-25 years. 49.23% of the respondents are undergraduates. Most of the respondents (63.07%) are students

Independent t-test about the awareness of e-banking frauds

Table 1. shows no significant relationship between males and females regarding to awareness about e-banking frauds and banking services. p-values are greater than 0.05. The low awareness about e-banking frauds and banking services provided by banks, because variables mean value is less than these.

Variables	**Gender**				**Values**	
	Male (22)		**Female (43)**		**T value**	**P value**
	MEAN	**SD**	**MEAN**	**SD**		
Identify Theft and Fraud (ITF) (Mean)	**2.55**	**0.74**	**2.74**	**0.66**	**-1.105**	**0.273**
Awareness about Scam (Mean)	**2.77**	**1.02**	**2.60**	**0.82**	**0.719**	**0.475**
Insurance Facilities Available (Mean)	**2.95**	**0.84**	**2.77**	**0.68**	**0.963**	**0.339**
Banking Governance (Mean)	**2.50**	**0.96**	**2.33**	**0.84**	**0.755**	**0.453**
Poor Monitoring (Mean)	**2.23**	**0.92**	**2.23**	**0.81**	**-0.024**	**0.981**
Scam Through QR code (Mean)	**2.68**	**0.78**	**2.47**	**0.67**	**1.170**	**0.247**
Fraud By Compromising Credentials on Results Through Search Engine (Mean)	**2.32**	**0.95**	**2.56**	**0.88**	**-1.014**	**0.315**
Fraud Using Screen Sharing Apps (Mean)	**2.23**	**0.97**	**2.07**	**0.70**	**0.748**	**0.457**
Awareness about E banking threats	**10.18**	**2.41**	**9.83**	**1.99**	**0.633**	**0.529**

Source: Comprehended from primary data.

Ho1.

Table 1: Comparison of the variables with gender and the distribution of respondents by gender.

According to Table 1, there were 66.1% male respondents and 33.9% female respondents among the study's participants. The null hypothesis is accepted at 0.05 because the p-value is greater than at significance level 0.05. This means that there is no significant difference between male and female awareness of E-banking scams and risks, according to an independent t-test.

(Analysis of variance) ANOVA

Factors affecting E-Banking Frauds	**MEAN**				**f value**	**p value**
	18-25	**25-30**	**30-35**	**40-55**		
Identify Theft and Fraud (ITF) (Mean)	2.68	2.62	2.00	3.50	1.568	0.194
Awareness about Scam (Mean)	2.66	2.62	2.00	3.50	.895	0.473
Insurance Facilities Available (Mean)	2.92	2.50	2.00	3.00	1.634	0.177
Banking Governance (Mean)	2.43	2.00	2.66	2.00	0.702	0.594
Poor Monitoring (Mean)	2.27	2.12	1.66	2.00	0.632	0.642
Scam Through QR code (Mean)	2.56	2.37	2.33	2.50	0.286	0.886
Fraud By Compromising Credentials on Results Through Search Engine (Mean)	2.49	2.50	2.66	2.00	0.234	0.918
Fraud Using Screen Sharing Apps (Mean)	2.11	2.25	2.6667	1.00	1.423	0.237
Awareness about E banking threats	10.06	9.51	8.3333	11.0625	0.684	0.605

<u>(Analysis of variance) ANOVA</u>

The analysis of variance (ANOVA) test has been conducted to evaluate the statistical significance of the outcome. Since the p-value is higher than 0.05, Table 2 is utilized. As a result, there are not significant variations among the variables influencing people's awareness of threats and frauds in online banking. In accordance with the table (Hair, Joseph, JW, and BJ), the analysis of variance (ANOVA) gives a static evaluation for overall model fit in terms of F statistics. This table (Hair Jr et al., 2010) [6] gives a representation of the ANOVA analysis, which provides a test of statistical significance for the overall model fit with respect to the F-statistic. As observed in the table, the F-statistic value is highly significant, with a p-value of a value of 0.05. This shows that there exists a linear relationship between the variables that are independent, such as, and the dependent variable, awareness of E-banking frauds and threats.

- Awareness about scam,
- Insurance Facilities Available,
- Banking Governance,
- Poor Monitoring,
- Scam Through QR Code,
- Fraud By Compromising Credentials on Result Through Search Engine,
- Fraud Using Screen Sharing Apps.

In other words, any given change in one of the independent variables will always produce a corresponding change in the dependent variable (awareness about E- banking frauds and threats.), Thus, all independent variables were confirmed by the analysis to have strong impact on dependent variable.

Multiple Regression Analysis

The Coefficient of determination with standard error of estimates

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics					Durbin-Watson
					R Square Change	F Change	df1	df2	Sig. F Change	
1	0.993[a]	0.986	0.984	0.26856	0.986	499.695	8	56	.000	1.937

a. Predictors: (Constant), Awareness about Scam, Fraud Using Screen Sharing Apps, Identify Theft and Fraud (ITF), Fraud by Compromising Credentials on Results Through Search Engine, Poor Monitoring, Insurance Facilities Available, Banking Governance, Scam Through QR code, Fraud by Compromising Credentials on Result Through Search Engine, Fraud Using Screen Sharing Apps.

b. Dependent Variable: awareness about E- banking frauds and threats.

A value of.984 for the adapted R Square is shown in the table. Independent variables such as those mentioned above are indicated., Awareness about Scam, Fraud Using Screen Sharing Apps, Identify Theft and Fraud, Fraud by Compromising Credentials on Results Through Search Engine, Poor Monitoring, Insurance Facilities Available , Banking Governance , Scam Through QR code, Fraud by Compromising Credentials on Result Through Search Engine, Fraud Using Screen

Sharing Apps, this model explained that other factors, which are not considered in the study, explain nearly 98.4 per cent of the total variation between dependent variable awareness levels regarding awareness about E- banking frauds and threats as well as remaining 1.6 percent. The adjusted R square corresponds to a significantly greater benchmark of 0.5 that should be sufficiently explained for the regression model.

Anova

An analysis of variance using ANOVA was applied for the purpose of assessing Statistical Relevance of the results. From the table, we can see that there is a significant difference between the awareness of awareness about E- banking frauds and threats, given that the p value is less than 5% of the relevant level. As a result, the table found that statistical test for model fit in F statistics was provided by an analysis of variance ANOVA. Since there is a linear relationship between the dependent variable (awareness of E-banking frauds and threats), and the independent variables will always result in an equivalent change in the dependent variable, as can be seen in the table, all independent variables were confirmed by the analysis to have a strong impact on the dependent variable. The value of F statistic, which is 499.695, is highly significant with a 5% level of significance.

ANOVA

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	288.326	8	36.041	499.695	.000[b]
	Residual	4.039	56	.072		
	Total	292.365	64			

a. Dependent Variable: awareness about e-banking frauds
b. Predictors: (Constant), Awareness about Scam, Fraud Using Screen Sharing Apps MEAN, Identify Theft and Fraud (ITF) MEAN, Fraud by Compromising Credentials on Results Through Search Engine, Poor Monitoring MEAN, Insurance Facilities Available Mean, Banking Governance mean, Scam Through QR code mean.

Coefficients

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	0.393	0.188		2.08	0.04

	Identify Theft and Fraud (ITF) MEAN	0.617	0.054	0.198	11.327	0.00
	Insurance Facilities Available Mean	0.440	0.070	0.153	6.24	0.00
	Banking Governance mean	0.227	0.064	0.093	3.54	0.00
	Poor Monitoring MEAN	0.329	0.067	0.130	4.91	0.00
	Scam Through QR code mean	0.413	0.090	0.137	4.57	0.00
	Fraud By Compromising Credentials on Results Through Search Engine Mean	0.204	0.054	0.086	3.79	0.00
	Fraud Using Screen Sharing Apps MEAN	0.145	0.052	0.054	2.77	0.00
	Awareness about Scam	0.146	0.007	0.490	21.91	0.00

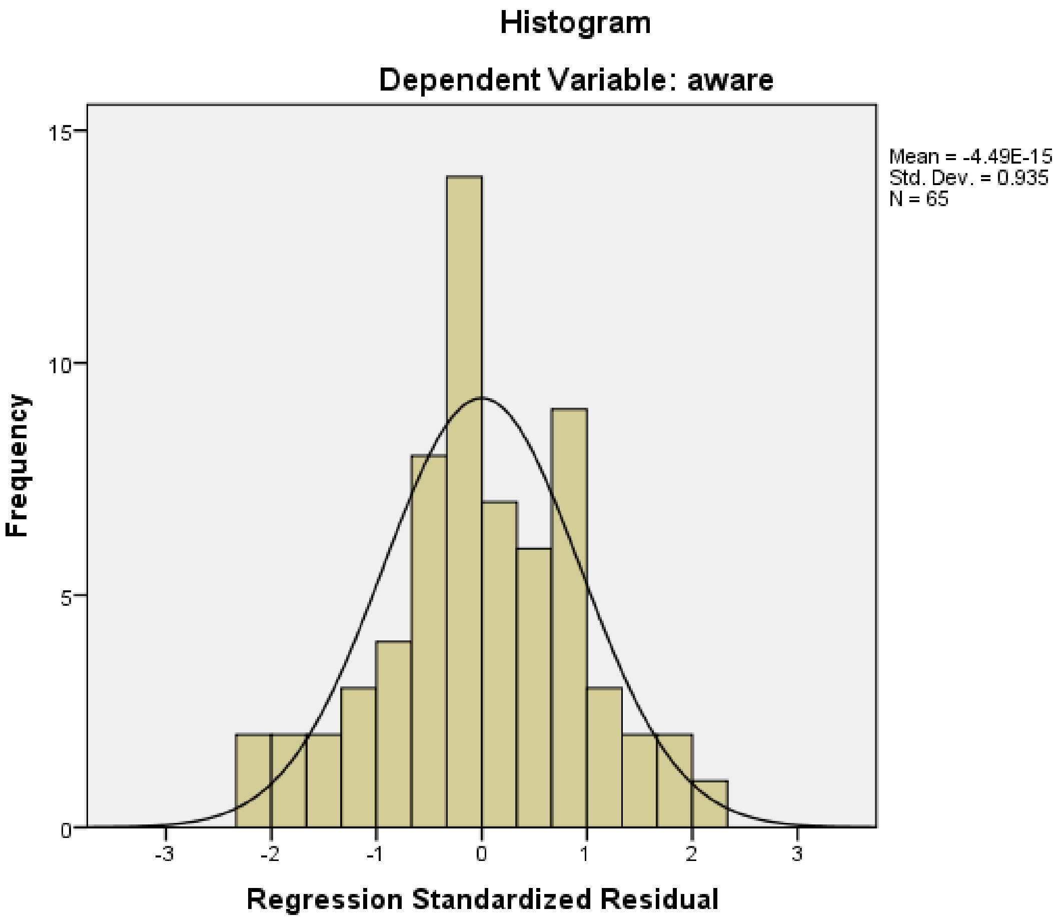
a. Dependent Variable: awareness about e-banking frauds.

¥ = a + bx.
¥ =.393+.617$_{xi}$+.440$_{x2}$+.227$_{X3}$+.329$_{X4}$+.413$_{X5}$+.204$_{X6}$+.145$_{X7}$+.146$_{X8.}$

This model let Y represents the awareness about E-banking frauds and threats. Identify Theft and Fraud, Insurance Facilities Available, Banking Governance, Scam Through QR code, Fraud by Compromising Credentials on Result Through Search Engine, Fraud Using Screen Sharing Apps, Fraud by Compromising Credentials on Results Through Search Engine, Poor Monitoring, Awareness about Scam, Fraud Using Screen Sharing Apps.

Present exploratory study was aimed to study or evaluate about awareness about various factors of banking frauds among customers, to measure how well the banking customers are aware about banking frauds. The purpose of this study of the would be to evaluate whether bank customers from the private and public sectors were aware of internet banking practices, of fraud, and of prevention measures. This study research will look at the respondents' usage behavior for online banking as well as their demography in the study area. The existing study's findings are related to the research of fraud preventative measures in the Banking sector in India. The simultaneous significance of Internet banking sector in India fraud awareness on fraud prevention strategies in the has been intended to be researched. The primarygoal of the research of is to evaluate that both private and public sector bank consumers are aware of online banking practices, aware of online banking fraud activities, and aware of online banking prevention measures.

The prevailing study is descriptive in nature and by using the survey method to derive method of analyzing, guidelines, and beneficial impact based on the statistical output, also with the assistance of a structured questionnaire, the primary data was collected interpretation and analysis then subjected to data using SPSS. Each regression coefficient coefficient's p-value for the calculated t-statistics is less than 0.05, indicating that most of the of the are significant at the 5% level of significance.



4. Findings

1. Out age range a total 65 respondents, 76.92% of respondents are in the age range of 18 to 25, 10.76% are in the 20 to 30, 4.61% are in the 35 to 50, and 4.61% are the 50 to 65.
2. Majority of the respondents agree that they are familiar with the use online banking services.
3. Superiority of the respondents have received spam calls or links related to banking frauds.
4. From the study it is comprehended that official bank website and google are predominantly used to verify while having any banking related queries.
5. In consideration of the awareness about scam the lion’s share is having vague know how about types of E-banking scams.
6. Awareness about various legal procedures against banking frauds and about cyber insurance policy are enigmatic among the respondents.
7. The problem becomes worse by a lack of advances in technology and fraud monitoring entities, and fraudulent monitoring is the fundamental fix.
8. Not all the warnings provided by RBI and other banks not to share information like expiry dates, CVV, OTP, PIN Numbers with anyone are reaching the people evenly.

9. Suggestions

1. Banks need to strengthen policies related to threshold value and limit of online banking transactions based the customer requirement and ability and they should take responsibility for unauthorized online transactions.
2. Customers should enhance their awareness level, knowledge and literacy with respect to online banking transactions to eliminate all the apprehensions related to cybercrimes such as Denial of service attacks, Cyber stalking, SIM card swapping / SIM jacking, Skimming, Malware, Keylogging, Vishing, Mobile phishing and ATM card skimming and etc.
3. Customers are suggested to use online banking transactions regularly and also educate the other family members, peer groups and friends to kindle their minds for the adoption of cashless transactions and digital economy in India.
4. The members of banks should create awareness among their customers towards different types of online banking frauds with demonstrations, examples to educate the customers to overcome fraudulent transactions and loss of money.

10. Conclusion

The objective of the present exploratory study was to explore consumer awareness of online banking, online banking fraudulent activities, as well as prospective preventive measures to eradicate online banking fraud in India The study in fact, has found that factors such as, identifying theft and frauds, Awareness about scam, Insurance Facilities Available, Banking Governance, Poor Monitoring, Scam Through QR code, Fraud by Compromising Credentials on Results Through Search Engine, Fraud Using Screen Sharing Apps prevention, convenience, accessibility, authentication, connectivity security and technology are key factors of online banking usage. The study sufficiently captures all the relevant evidences to classify the bank customers based on their awareness about online banking frauds and fraud prevention measures awareness. The growth of digital transactions in the country shows crucial inclination to accept and adopt ‘online banking’, solely driven by higher usage and adoption of online banking platforms.

It is therefore concluded that ‘online banking’ through different digital platforms has gained momentum in recent years. In order to cope up with the customers, banks should focus on safety and security measures to gain customer trust and loyalty which are major factors for adoption and intention to use online banking. On the other hand, Government and RBI should devise appropriate strategies to eliminate and different types of frauds and fraudsters in Indian banking context. The present study is an eye opener for banking industry to develop holistic goal for the elimination of fraudsters from India and to achieve cashless economy in the form of digital transformation of the country.

12.References

Bhasin, L. M. (2006). Guarding Privacy on The Internet. *7*(1).

Mangala, D., & Lalitha, S. (2023). A Systematic Literature Review on Frauds in Banking Sector. *Journal Of Financial Crime, 30*, 285-301(17).

Ololade, M. B., & Salawu, K. M. (2020). E-Frauds in Nigerian Banks: Why and How? *Journal ofFinancial Risk Management, 9*(3).

Pani, L. K., & Swain, S. (2014). Comparative Analysis of Retail Banking Between Private andPublic Sector Banks in Odisha. *4*(3).

Reurink, A. (2018). Financial Fraud: A Literature Review. *Journal Of Economic Surveys, 32*(5),1292-1325.

S, R., & I, S. M. (2011). Impact of Electronic Crime in Indian Banking Sector. *The InternationalJournal of Business and Information*.

Sanjeev, G. M. (2006). Data Envelopment Analysis for Measuring Technical Efficiency of Banks. *The Journal of Business Perspective, 10*(1).

V, C., & Choudhary, V. (2015). Internet Banking: Challenges and Opportunities in Indian Context.