Quest Journals
Journal of Education, Arts, Law and Multidisplinary
Volume 16 ~ Issue 3 (May. – June. 2026) pp: 153-165
ISSN(Online): 2347-2895
www.questjournals.org

Research Paper

"A Study on Cybercrimes in Banking Sector: Views of Customers in Bengaluru City"

*Prof.Jalaja K R ** Chinmayi Shekar V ***Indumathi B
**Prof. K R Jalaja, Dean & Chairperson, Department of Commerce, Bengaluru City University.*
***Chinmayi Shekar V, Research Scholar, Department of Commerce, Bengaluru City University, Bengaluru.*
**** Indumathi B, Assistant Professor, Department of Commerce, Govt. First Grade College, Anavatti, Shimoga (D).*

ABSTRACT
Banking is the heart of India's financial service sector. Banks today operate in a highly globalized, liberalized and a competitive environment. In order to survive in this environment banks have to use IT. Indian banking industry has witnessed a tremendous development due to sweeping changes that are taking place in the information technology. With the effect of Liberalization, Privatization and Globalization (LPG) and increased competition, innovations have been made in the banking sector to improve banking service quality. All these resulted in reforms of banking sector from paper transactions to e-transactions. Now customers are using plastic money, e-money rather than paper currency and banking system has also improved to a great extent, now it is customer centric era where customer is the king and services are to be delivered as per customer needs. 68% of Indian consumers are now using online or mobile banking to conduct financial transactions. So banks are facing the dual challenges of increasing penetration and high growth trajectory. Though IT brings lot of changes in banking sector which includes both Positive and Negative impacts in Banking one of the major threat present world is facing is Cybercrimes. In 2021, there were over 4.8 thousand cases of online banking frauds reported across India. This was a big increase in the number of banking fraud cases than the previous year.

Key Words: *Cybercrimes, Digital Banking, Cyber Threats and Frauds, RBI Initiatives*

I. INTRODUCTION

The banking industry has reformed tremendously from past few decades. Indian banking system has improved to the level of international standards. Information technology has become a necessary tool in today's organizations. Even at present, India is a relative unbanked country as the credit-to-GDP ratio is one of the lowest in the developing economies. So banks are facing the dual challenges of increasing penetration and high growth trajectory. In this scenario technology plays a very important role. Tremendous progress took place in the field of technology which has reduced the world to a global village and it has brought remarkable changes in the banking industry. Branch banking in the brick and mortar mode has been transformed into click and order channel mode.

The internet was born around 1960's where its access was limited to few scientists, researchers and the defense only. Internet user base has evolved exponentially. Initially the computer crime was only confined to making a physical damage to the computer and related infrastructure. Around 1980's the trend changed from causing the physical damaging to computers to making a computer malfunction using a malicious code called Virus. Till then, the effect was not so widespread because internet was only confined to defense setups, large International Companies and Research Communities. In 1996, when internet was launched for the public, it immediately became popular among the masses and they slowly became dependent on it to an extent that it has changed their lifestyles. The Graphical User Interface (GUIs) was written so well that the users don't have to bother how the internet was functioning. They have to simply make few click over the hyperlinks or type the desired information at the desired place without bothering where this data is stored and how it is sent over the internet or whether the data can accessed by another person who is connected to the internet or whether the data packet sent over the internet can be snoofed and tampered. Now the focus of the computer crimes has shifted

from merely damaging the computer or destroying or manipulating data for personal benefit to financial crime. These computer attacks are increasing at a rapid pace. Every minute $2.9 million is lost to cybercrimes. Top companies pay $25 per minute due to cyber security breaches. As of 2020, the average cost of a data breach was $3.86 million. Cybercrimes is projected to cost the world $10.5 trillion annually by 2025. Malware has increased by 358% overall and Ransomware increased by 435% as compared to 2019. The world faces over 1,00,000 malicious websites and 10,000 malicious files daily.Phishing attacks account for more than 80% of reported security incidents. Google has registered over 2 million phishing sites as of January 2021- this is up from 1.7 million in January 2020, which equates at a 27% increase in 12 months. In 2019, 93.6% of observedMalware was polymorphic, meaning it has the ability to continually change its code to evade detection. 94% of Malware is delivered via email. 30000 websites are hacked every day and there is a cyber-attack once every 39 seconds. 2020 was a record year for DDOs Attacks. Internet is among the most important inventions of the 21st century which have affected our life. It has given rise to new opportunities in every field we can think of – be it entertainment, business, sports or education. There are many pros and cons of some new type of technology which have been invented or discovered. Similarly the new and profound technology i.e. using of INTERNET service, has also got some pros and cons. These cons are named as CYBERCRIMES, the major disadvantage, illegal activity committed on the internet by certain individuals because of certain loop-holes. The internet, along with its advantage has also exposed us to security risks. Computers today are being misused for illegal activities like e-mail, espionage, credit card frauds, Spam and software piracy etc. Criminal activities in the cyberspace are on rise.

NEED OF THE STUDY

There is a need to identify, study and analyze the loopholes existing in the Indian Banking sector in order to curb the fraudulent activities and to be able to take corrective actions, thereby enhancing the security measures of this sector. Online Banking is playing a unique role in strengthening the banking sector and improving service quality. Almost all the banks have adopted electronic banking services to attract their customers. Although there is a rise in electronic banking channels customers still have fear towards their safe and secure electronic banking transactions. There is a need to study the weak areas in the Information Technology Act and Cyber laws in India. In order to strengthen banking sector and boost up online banking it is necessary to know the impact of cybercrimes on the bank customers. This study attempts to create awareness with respect to various cybercrimes and cyber laws related to banking operation in India.

II. REVIEW OF LITERATURE

DIVYA VERMA GAKHAR. (2008). In this Paper "SECURITY ISSUES IN E- BANKING" the author explains that Banks are the backbone of any financial system. Information Technology (IT) has become an integral part of the banking system. With the introduction of IT in banking the industry has been able to meet customer's requirements in an efficient manner by providing them all-time available error free services system, E-security aspects in banking, cyber laws and RBI guidelines to regulate the e-security issues related to banks. The author has also made some suggestions to improve the security in banks.

CASSIM F. (2009). In this article "FORMULATING SPECIALIZED LEGISLATION TO ADDRESS THE GROWING SPECTRE OF CYBERCRIMES: A COMPARATIVE STUDY" the author has explained about the various cyber legislation formulated to address cybercrime in the United States of America, The United Kingdom, Australia, India, The gulf Countries and South Africa. The study reveals that the inability of national laws to address the challenges posed by cybercrime has led to the introductionof specialized cyber legislation.

IBRAHIM BAGGILI. (2010). In this paper the author has highlighted the points which have been discussed in the Second International ICST Conference on digital forensic and Cybercrimes (ICDF2C 2010) which was hosted in Abu Dhabi, United Arab Emirates during October 4-6, 2010. Topics like latest advancements in digital image forensics and issues of network forensic were also discussed in the conference.

DEBARATI HALDER AND JAISHANKAR KARUPPANNA. (2010). Authors in the article "CYBER VICTIMIZATION IN INDIA: A BASELINE SURVEY REPORT 2010" describes since 1990"s till today India has seen growth in IT Sector, almost every household falling in economic zone of moderate to high income groups have internet access and people from age group of 13 to 70 years access internet regularly but along with this there is victimization.

NATIONAL CYBER SECURITY POLICY GOVERNMENT OF INDIA (2011).This paper gives a detailed study about the cyber security, cyber space and its strategic perspective; it explains the legal framework, law enforcement and information sharing. This Paper also highlights about the awareness created at different level of users (Corporate, home users and students) through training. The paper is concluded by discussing the technologies used for ensuring security.

VICTOR O WAZIRI, NO OKONGWU, AUDU ISAH, OLAWALE SURAJUDDEEN ADEBAYO, SHAFII M ABDULHAMID.(2012).In this paper, the authors have presented the digital forensic open sources tools like Fiwalk, Bulk- Extractor, Foremost, Sleuth Kit, and Autopsy which are all Linux based forensic tools

to extract evidence that could be presented in the court of law. They have given detailed experiments since this work aimed at enhancing the utilities of open source forensic tools applications.

ASHWINI MANISH BRAHME, SUNIL B JOSHI. (2013). In this paper the author has analyzed the ratio of increasing cybercrimes and their effect on the society, e business and retailers. This paper also explains about the various cyber threats and the challenges faced by the banks while detecting and preventing those frauds.

AMITA CHARAN. (2014). In this Paper "E-BANKING AND CYBERCRIMES IN INDIA" the author defines E-banking as digital banking covering wider terms like e-banking, m-banking, SMS banking, App banking etc. Moreover he explains that our heavy dependency on electronic gadgets, mobiles and digital tools to commence business and routine transactions is increasing day by day. Unfortunately, we are exposed to many closed and open networks where the reliability and safety is an issue for regulatory authority.. This paper presents the overview of various types of cybercrimes against nation, Society and customers.

RAKSHA CHOUHAN. (2015). In this Paper "CYBERCRIMES ESCALATION VS SOLUTIONS: A LITERATURE SNAPSHOT" the author has done detailed study on the impact of cybercrimes on quality production time, overhead cost, consumer trust, market value as well as on the economy of the country. This paper also throws light on status of cybercrimes in current scenario, available solutions including steps taken by non-government and government organizations to avoid cybercrimes and forthcoming challenges as well as National, International accordance and solutions to deal with the same.

SANCHI AGRAWAL. (2016). In this paper on "CYBERCRIMES IN BANKING SECTOR" the author has explained the introduction to the concept of e-banking and its advantages in India. Further the author has provided the statistics of the increase in use of e-banking services in India and the role of Reserve bank of India in strengthening internet banking. Finally the author has suggested the safeguards the customer and a bank should undertake while dealing electronically.

CHITRA LEKHA, S. PRAKASAM (2017). In this Paper "DATA MINING TECHNIQUES IN DETECTING AND PREDICTING CYBERCRIMES IN BANKING SECTOR" the author has presented a general idea about the model of Data Mining techniques and diverse cybercrimes in banking applications. It also provides an inclusive survey of competent and valuable techniques on data mining for cybercrimes data analysis. In this paper the author has implemented a novel data mining techniques like K-Means, Influenced Association Classifier and J48 Prediction tree for investigating the cybercrimes.

SUSHIL KUMAR SINGH, NEHA RASTOGI. (2018). In this Paper "ROLE OF CYBER CELL TO HANDLE CYBERCRIMES WITHIN THE PUBLIC AND PRIVATE SECTOR: AN INDIAN CASE STUDY" the author explains that in India, internet users are increasing rapidly over a period of time because of communication among the smart devices. This rapid increase of internet users is not adequately handled by the service providers.

PIYUSH GINOTRA. (2019). In this Paper "INNOVATION IN INDIAN BANKING SECTOR" the author had discussed about the various technological advancements in banking sector like introduction of Automated Teller Machines, Debit &credit cards, NEFT, RTGS, internet banking etc. But the technological advancements all over the world had created a pressure for the use of better technology in the banking sector. This paper highlights different innovative products and services offered by Indian banks. Towards the end, the author has done a critical analysis of the level of acceptance and adoption of these innovations by the banking customers. For this analysis he has used primary data. This paper is descriptive in nature and aims to illuminate the knowledge of the readers.

P MARY JEYANTHI, A MANSURALI, V HARISH, V.D KRISHNAVENI. (2020). In this Paper "SIGNIFICANCE OF FRAUD ANALYTICS IN INDIAN BANKING SECTORS" the authors have discussed that the banks are the motors that drive the tasks in the monetary sector, currency markets and development of an economy. In the last three years, in India, Public Sector Banks (PSBs) have lost several crores of rupees on account of various banking frauds. According to the RBI laws, the number of account management extortion cases has declined, however the number of cases has increased in recent times. This paper has also focused on different fake and fraud cases for both internal and external misrepresentation plots in the banking sector.

CHANDRA SEKHAR BISWAL, SUBHENDU KUMAR PANI.(2021). In this paper "CYBERCRIMES PREVENTION METHODOLOGY" the authors explains that in the recent years, internet has very quickly changed starting with education, startups, and sports to entertainment medium. The prime focus of the authors is to give emphasis on various frauds and cybercrimes undertaken in India as well as different types of cyber-crimes along with possible solution.

DIVY SHIVPURI. (2021). In this Paper "CYBERCRIMES: ARE THE LAW OUTDATED FOR THIS TYPE OF CRIME" the author defines Cybercrimes as an "illegal act in which a computer is a tool or a goal or both". This paper mainly deals with the laws relating to cyber-crime in India. The objective of this research paper is to analyze the concept of cyber-crime in India and to give the suggestions to make the laws more effective to deal with it.

NIDHI SAXENA, VEER MAYANK. (2022). In this Paper "SCOURGE OF CYBER FRAUD DURING COVID-19: CHALLENGES AND RESOLUTIONS" the author has analyzed the existing applicable Indian

laws on cyber fraud cases while focusing on the numerous challenges that regulatory structures of the state are facing today. This research paper is based on two propositions: one, the specific roles and responsibilities of individuals; banking institutions, the second is the rules and procedures of cyber law enforcement have to be defined and polished because cybercriminals could range from an individual who is a child or novice to a well-accomplished software experts. This paper examines the various laws for regulating cybercrimes and attempts tooffer suggestions for modifying these laws for addressing the emerging challenges.

RESEARCH GAP

Through the review of literature it was found that, various studies have been carried out to know different dimensions of cybercrimes and causes and effects of cybercrimes, no attempts have been made to analyse the customer perspective of cybercrimes and reasons behind the cybercrimes and its impact on customers in Karnataka with reference to Bengaluru as reviewed so far. Hence, an attempt has been made in the present study to fill the research gap and highlights the perspectives of customers about the cybercrimes and its impact.

STATEMENT OF PROBLEM

Cybercrimes is a growing threat in the virtual world because individuals and organizations are relying more on internet at an increasing rate. The use of internet and other technologies have enhanced the risk of attack from cybercrimes. Further, the growing volume of online transactions and absence of stringent cyber security systems gives fraudsters the space to commit malicious acts. As the number of incidents of theft, phishing, computer virus, hacking is on the rise, there is a need to explore the cybercrime scenario. The main problem of the study is to analyze about the customers, affected due to cybercrimes in banking industry, measures taken by the banks and government authorities for the prevention of these crimes.

OBJECTIVES OF STUDY

1. To understand various cybercrimes with respect to digital banking operations.
2. To review the current scenario of cybercrimes.
3. To identify the reasons behind the bank frauds and the challenges faced by the banks in the detection and prevention of cybercrimes.
4. To suggest the preventive measures and safety tips for the control and prevention ofcybercrimes.

SCOPE OF THE STUDY

The purpose of this study is to examine awareness among individuals for making use of internet banking. It further tries to understand various cybercrimes and cyber legislationsmade in India with reference to cybercrimes related to internet and digital banking. Further the study is to analyze about the persons affected due to cybercrimes while using their internet banking and it will be helpful for the banks to rectify the errors in future period of time. The Government of any country must work to provide complete welfare to its citizens and it is the main duty of IT Departments to protect the customer's interest, as this study focuses on the major problem faced by the customers it helps the Government and IT Departments to bring changes in the existing laws related to cybercrimes and help its stakeholders.

III. RESEARCH METHODOLOGY

This study is based on both primary and secondary data. For this study, categories of cybercrimes in banking sector is analyzed by reviewing various literatures and Information Technology Act, 2000 as well as the web site of cybercrimes investigation cells Delhi, Mumbai and Bangalore. To review the tricks and techniques used by cyber criminals to hack the banking system and make the cyber fraud various case studies in various newspapers, news channels and cyber security books are referred. To review the status of cybercrimes in India and Bangalore City the data is gathered from annual reports of National Crime Record Bureau, Banks, News channels and websites.

DATA COLLECTION TOOLS

The primary data is that data which is collected in the initial phase of the research. The data is collected through questionnaire from the respondents. The secondary data comprises of that data which the researcher acquires from the sources like magazines, journals, websites etc. Basically it is the data which is already available in several different resources.

SAMPLE SIZE: The sample size can be defined as the total number of respondents that is to be taken from the population. In this research, 110 respondents were taken.

SAMPLING TECHNIQUE: Simple Random Sampling.

LIMITATIONS OF THE STUDY

- The scope of this research work has been limited to banking industry; in view of this research work may not necessarily fit into other industries in India. It was found that various measures undertaken by banks are

not enough to reduce the millions and billions of money being eroded due to cybercrimes.

- The study has been limited to customers of Bengaluru City only.

IV. DATA ANALYSIS AND INTERPRETATIONS

TABLE 1: RESPONDENTS OPINIONS ON VARIOUS ASPECTS OF CYBERCRIMES

SL. NO.	PARTICULARS		PARAMETERS		TOTAL
			Yes	No	
1.	Respondents Who Has Bank Accounts	N	110	0	110
		%	100%	0%	100%
2.	Awareness of Customers On Cyber Crimes	N	106	04	110
		%	96.4%	3.6%	100%
3.	Awareness Provided by the Banks onCyber Crimes	N	89	21	110
		%	80.9%	19.1%	100%
4.	Number of Customers Who Have FacedCyber Crimes In Banking	N	33	77	110
		%	30%	70%	100%
5.	Reporting of Cyber Crimes to CyberAuthorities	N	22	33	55
		%	40%	60%	100%
6.	Banks Support Towards Their CustomersIn The Cases Of Cyber Crimes	N	77	33	110
		%	70%	30%	100%
7.	Need For Training Bank Employees OnCyber Security	N	100	10	110
		%	90.9%	9.10%	100%
8.	Awareness Of Customers On ForeignPayments OTP	N	80	30	110
		%	72.70%	27.30%	100%
9.	Customers Awareness On The National Helpline No.155260 And Its Reporting Platform	N	46	64	110
		%	41.8%	58.2%	100%
10.	Customers Who Has Used National Helpline No.155260.	N	14	53	67
		%	20.9	79.1	100%

TABLE 2: TYPE OF BANKS WHERE RESPONDENTS HAVEMAINTAINED THEIR BANK ACCOUNTS

TYPE OF BANK	RESPONDENTS	PERCENTAGE
Public sector bank	76	**69.10%**
Private sector bank	34	**30.90%**
Foreign bank	0	**0**
TOTAL	**110**	**100%**

(Source: Primary Data)

From the above table it can be interpreted that out of 110 respondents highest of 69.10% of the respondents have maintained their Bank account in the public sector banks, lowest of 30.9% of them have maintained their bank account in private sector banks and there are no response from the foreign bank account holders. Majority of the respondents have maintained theirbank account in public sector banks.

TABLE 3: PERIOD OF MAINTENANCE OF BANK ACCOUNT BY THE RESPONDENTS

PERIOD	FREQUENCY	PERCENTAGE
Less than 1 year	6	**5.50%**
1 to 5 years	48	**43.10%**
5 to 10 years	39	**35.80%**
10-15 years	14	**12.80%**
15 years and above	3	**2.80%**
TOTAL	**110**	**100%**

(Source: Primary Data)

From the above table, it can be interpreted that out of 109 respondents who have shared their views that Highest

of 43.10% of the respondents have maintained their bank account from past 1-5 years, nearest to that 35.8% of the respondents have maintained their bank account from past 5-10 years and least of 2.80% of the respondents are maintaining their bank account from a verylonger duration of 15 years and above. It shows the gradual increase in the bank customers in the past 5 years.

TABLE 4: VIEWS OF CUSTOMERS ON E-BANKINGSERVICES

PARTICULARS	FREQUENCY	PERCENTAGE
Essential	55	**50%**
Desirable	14	**12.73%**
Necessary	27	**24.54%**
Cannot say exactly	14	**12.73%**
TOTAL	**110**	**100%**

(Source: Primary Data)

Table 4 shows the views of customers on e-banking services, out of 110 respondents 50% or half of the respondents say that e-banking is essential, 13 % of the respondents say that it is desirable, 24% of the respondents say that it is necessary. Remaining 13% of the respondents feel difficult to express their views on the subject it can be due to the drawbacks of e-banking or lack of understanding on e-banking. Hence itcan be interpreted that half of the respondents avails e-banking services for their banking transactions and also there are 13% respondents who has greater satisfaction on e-banking services and feels convenient to use it.

TABLE 5: MOST WIDELY USED ELECTRONIC BANKINGSERVICES

BANKING SERVICES	FREQUENCY	PERCENTAGE
Online banking	42	**38.20%**
ATM and debit card services	65	**59.10%**
Phone banking	29	**26.40%**
SMS banking	13	**11.80%**
Mobile banking	54	**49.10%**
Fund transfer services	16	**14.50%**
TOTAL	110	100%

(Source: Primary Data)

Through Table 5 it can be interpreted that Highest of 59.10% of the respondents use AMT and debit card services, Nearest of 49.10% of the respondents use mobile banking and least of 11,80% of the respondents use SMS banking. It can be observed that ATM and Mobile banking services are most widely used electronic banking services.

TABLE 6: FREQUENCY OF USING ONLINE BANKINGSERVICES BY THE RESPONDENTS

PARTICULARS	FREQUENCY	PERCENTAGE
Once in a day	38	**34.50%**
Once in a week	37	**33.60%**
Once in a month	16	**14.50%**
Less often	8	**7.30%**
Never used	11	**10%**
TOTAL	110	100%

(Source: Primary Data)

Through table 6 it can be understood that, maximum of 35% of the respondent's use online banking daily, nearest to that 34% of them use it weekly and only 7% of the respondents use it very often. Hence from it can be interpret that majority of the respondents are using online banking every day.

TABLE 7: SOURCES OF AWARENESS ABOUT CYBERCRIMES

SOURCES OF AWARENES	FREQUENCY	PERCENTAGE
Television	53	**48.2%**
Radio	10	**9.1%**
Newspapers and magazine	28	**25.5%**
Social media	46	**41.8%**
Friends, family and colleagues	38	**34.5%**
Internet	39	**35.5%**
TOTAL	110	100%

(Source: Primary Data)

Table 7 represents the sources of awareness about cybercrimes, highest of 48.20% of the respondents have seen about it on through television, nearest of 41.80% have got the awareness through television and least of 9.10% of the respondents got to know about cybercrimes through radio. It can be understood that television is providing more awareness about cybercrimes than any other source.

TABLE 8: CUSTOMERS AWARENESS ON VARIOUS CYBERTHREATS

TYPES OF CYBER THREATS	FREQUENCY	PERCENTAGE
Computer hacking	56	**50.9%**
Phishing	15	**13.6%**
Vishing	6	**5.5%**
Identity theft	16	**14.5%**
Dos attack	6	**5.5%**
SIM card fraud	10	**9.1%**
All the above	42	**38.2%**
None of the above	19	**17.3%**
TOTAL	110	100%

(Source: Primary Data)

From the above table, it can be interpreted that majority of 50.9% of the respondents have more awareness on computer hacking compared to other cyber threats, closest of 38.2% are aware of all the cyber threats and least of 17.30% of the respondents who are not at all aware of any of these cyber threats as a result there are a lot of chances of them becoming victims of cyber fraud.

TABLE 9: FREQUENCY OF CUSTOMERS WHO HAVE FACEDCYBER THREATS RELATED TO BANKING

PARTICULARS	FREQUENCY	PERCENTAGE
1 time	33	**71.7%**
2-5 times	9	**19.6%**
5-10 times	3	**6.5%**
More than 10 times	1	**2.2%**
TOTAL	46	100%

(Source: Primary Data)

Table 09 depicts the frequency of customers who have faced cyber threat related issues, highest of 71.7% of the respondents have lost their money one time due to cyber frauds, 19.6% of the respondents have lost their money 2-5 times, 6.5 % of the respondents have lost their money 5-10 times and there is a least of one respondent who has lost his money more than 10 times. As the technology is advancing cyber criminals are also becoming more advanced they use various techniques to commit fraud and a person who is unaware of the term cybercrime easily becomes the victim of such cybercrimes.

TABLE 10: REASONS BEHIND LOSING MONEY BY THE BANKCUSTOMERS

PARTICULARS	FREQUENCY	PERCENTAGE
Fake calls	17	**37%**
Fake SMS	11	**23.9%**
Card cloning	6	**13%**
Fake mails	0	**0%**
OTP fraud	1	**2.2%**
UPI payment fraud	7	**15.1%**
Through purchase on fake website	1	**2.2%**
Typing job	1	**2.2%**
Unknown	1	**2.2%**
No of the above	1	**2.2%**
TOTAL	46	100%

(Source: Primary Data)

Through table 10, out of 46 respondents maximum of 37% of the respondents have lost their hard earned money due to fake calls, 23.9% of the respondents have lost their money due to fake SMS, 15.1% of them have lost their money due to UPI payment fraud, 13% of them have lost their money due to card cloning and remaining respondents lost their amount due to OTP fraud, Typing job, fake websites and there are two respondents who have lost their money and are unaware of the reasons behind it. It can be observed that majority of the respondents have lost their money due to the fake calls and SMS.

TABLE 11: RANGE OF AMOUNT LOST BY THE RESPONDENTSIN THE CYBERCRIMES

AMOUNT	FREQUENCY	PERCENTAGE
Less than 10,000	34	**73.9%**
10,000-50,000	8	**17.4%**
50,000-1,00,000	2	**4.3%**
1,00,000 and above	2	**4.3%**
TOTAL	46	100

(Source: Primary Data)

The above table 11 shows the range of amount lost by the respondents, out of 46 respondents, 73.9% respondents have lost the amount less than Rs.10, 000, 17.4% respondents have lost the amount ranging from Rs.10, 000-50,000, least of 4.3% of them have lost Rs.50, 000-1, 00,000 and more than 1, 00,000 in the cybercrimes related to banking.

TABLE 12: CUSTOMER SATISFACTION LEVEL TOWARDSBANKS CYBER SECURITY

SATISFACTION LEVEL	FREQUENCY	PERCENTAGE
Fully satisfied	28	**25.5%**
Partially satisfied	65	**59.1%**
Not satisfied	17	**15.5%**
TOTAL	110	100%

(Source: Primary Data)

The above table 12 represents the customer satisfaction towards the current cyber security provided by their banks, out of 110 respondents highest of 59.1% respondents are Partially satisfied with the current cyber security, 25.5% respondents are fully satisfied and least of 15.5% respondents are not satisfied with the current cyber security which is provided by the banks. It can be interpreted that majority of the respondents are partially satisfied with the current cybersecurity provided by their banks in order to maintain customers trust on banking, banks must improve their cyber security measures.

TABLE 13: REASONS BEHIND BECOMING EASY VICTIMS OFCYBERCRIMES

PARTICULARS	FREQUENCY	PERCENTAGE
Lack of awareness about cybercrimes	58	**52. 7%**
Carelessness	45	**40.9%**
Greed of getting prize money, gifts and lotteryamount	53	**48.2%**
Fear Psychosis	8	**7.3%**
TOTAL	110	100%

(Source: Primary Data)

From the above chart it can be analyze that out of 110 respondents who have shared their valuable views on the subject, majority of 52.70% of the respondents says that the main reason behind becoming the easy victim of cybercrime is lack of awareness on cybercrimes, nearest to that 48.20% of the respondents says that people are more attracted towards money and prizes as soon as someone tells them that they have won lottery money, gifts and prize etc people share all there confidential information related to bank account to get the benefit of that money and becomes easy victims, 40.90% of the respondents says people become victim of cybercrime due to their carelessness, and least of 7.30% of the respondents says that people becomes victims due to fear psychosis if any unknown person calls and tells them that if you don't provide bank details your account gets block customers don't think who is there on the other side as a result in order to stop account getting block they share all their information and becomes easy victims. From the above figure it is clear that the main reason behind becoming a victim of cybercrime is lack of awareness and greed.

TABLE 14: SHOWING THE IMPACT OF GOVERNMENT'S REPORTINGPLATFORM ON FUTURE CYBERCRIMES

PARTICULARS	FREQUENCY	PERCENTAGE
Increase	39	**35.4%**

Remain Static	42	**38.2%**
Decrease	29	**26.4%**
TOTAL	110	100%

(Source: Primary Data)

The above table, It can be highlighted that out of 110 respondents who have put forth their opinions maximum of 38.2% of the respondent's opinion is that the cases of cybercrimes remains same, closest to that 35.4% of the respondents says that though the government has launched National helpline no.155260 for preventing financial losses due to cyber frauds majority of the people are unaware of this as a result there may be increase of cybercrimes, and 26.4% of the respondents thinks that as a result of this initiative there may be a chances of decrease in the future cybercrimes. The above figure shows that majority of the respondents doesn't have confidence on Government's initiatives.

TABLE 15: SUFFICIENT CYBER SECURITY MEASURES ANDCYBER LAWS

PARTICULARS	FREQUENCY	PERCENTAGE
Strongly agree	11	**10%**
Agree	24	**21.8%**
Strongly disagree	11	**10%**
Disagree	45	**40.9%**
Neutral	19	**17.3%**
TOTAL	110	100%

(Source: Primary Data)

Through the above table, it can be identified that majority of 40.9% of the respondents are not satisfied with the cyber security measures and cyber laws which are currently in practice and least of 10% combine the opinions of strongly agreed and strongly Disagreed this statement. Hence it can be understood that there is a need to improve cyber security in banks and enactment of strict cyber laws to control future cybercrimes.

TABLE 16: IMPACT OF SECURITY ISSUES ON CUSTOMERS

PARTICULARS	FREQUENCY	PERCENTAGE
Less likely to shop online	18	**16.4%**
Less likely to bank online	12	**10.9%**
Less likely to give personal information on Websites.	30	**27.3%**
All the above	50	**45.5%**
TOTAL	110	100%

(Source: Primary Data)

The above table 16 measures the impact of security issues on the customers, out of 110 respondents who have put forth their opinions highest of 45.5% respondents have agreed all the issues, closest to that 27.3% respondents feels insecure to givepersonal information on the websites, 16.4% that due to lackof cyber security they have reduced their online shopping and least of 10.9% respondents have reduced their online banking activities due to security issues, Majority of the respondents feel insecure to share their information on websites. Hence the concern about the security issues has made majority of the respondents change their shopping and banking patterns, so to enhance the confidence of online users there should be proper security measures.

TABLE 17: RESPONSIBILITY OF PREVENTING CYBERCRIMES

PARTICULARS	FREQUENCY	PERCENTAGE
An Individual himself	40	**36.4%**
Bank	54	**49.1%**
Cyber authorities	18	**16.4%**
Government	19	**17.3%**
IT Firms	11	**10%**
It is collective responsibility of All	36	**32.7%**
TOTAL	110	100%

(Source: Primary Data)

Table 17 represents the Responsibility for the prevention of Cybercrimes, maximum of 49.1% our respondents said that it is the responsibility of banks to protect its customers from cybercrimes, 36.4% agreed that an Individual himself responsible, , nearest of 32.7% agreed that it is the collective responsibility of all and least of 10% of the respondents opinion to some extent IT Firms are also responsible to protect the valuable online users data from getting leaked which may even contains the bank details of the customers. Hence it can be interpreted that in order to control future cybercrimes all the stakeholders directly or indirectly linked to the banking process should play an important role.

BANK GROUP-WISE FRAUD CASES OVER THE LAST THREE YEARS

Fraud Cases – Bank Group						
						(Amount in ₹ crore)
Bank Group/Institution	**2019-20**		**2020-21**		**2021-22**	
	Number of Frauds	**Amount Involved**	**Number of Frauds**	**Amount Involved**	**Number of Frauds**	**Amount Involved**
1	**2**	**3**	**4**	**5**	**6**	**7**
Public Sector Banks	4,410	1,48,224	2,901	81,901	3,078	40,282
	(50.7)	(79.9)	(39.4)	(59.2)	(33.8)	(66.7)
Private Sector Banks	3,065	34,211	3,710	46,335	5,334	17,588
	(35.2)	(18.5)	(50.4)	(33.5)	(58.6)	(29.1)
Foreign Banks	1,026	972	520	3,280	494	1,206
	(11.8)	(0.5)	(7.1)	(2.4)	(5.5)	(2.0)
Financial Institutions	15	2,048	24	6,663	10	1,305
	(0.2)	(1.1)	(0.3)	(4.9)	(0.1)	(2.2)
Small Finance Banks	147	11	114	30	155	30
	(1.7)	-	(1.6)	-	(1.7)	-
Payments Banks	38	2	88	2	30	1
	(0.4)	-	(1.2)	-	(0.3)	-
Local Area Banks	2	-	2	-	2	2
	-	-	-	-	-	-
Total	8,703	1,85,468	7,359	1,38,211	9,103	60,414
	(100.0)	(100.0)	(100.0)	(100.0)	(100.0)	(100.0)

(Secondary Data: (https://m.rbi.org.in//))

V. FINDINGS

- The security of the customers is at huge risk since it has become very easy to hack their personal details and there is a lack of cybercrimes awareness among the bank customers.
- Almost everyone irrespective of age, gender, income level and occupation has maintained their bank account.
- From the available electronic banking services ATM and Debit/Card services and Mobile banking are most widely used by the 59% and 41% of the respondents respectively. And it has been found that Mobile banking has become the boon for almost all the bank customers.
- Among 110 respondents 36% of the respondent receives cybercrime awareness once in a month this shows that there is a lack of regular awareness programs about cybercrimes under taken by the banks.
- Nearly 70% of bank customers have faced cyber threats during online banking and had lost their money.
- There is a lack of training and education of bank employees almost 91% of bank customers have also stated the same views on the problem.

- ❖ People have become more sensitive towards their security because of which 46% of respondents have reduced their online shopping and banking activities.
- ❖ Among the respondents 91% of respondents suggest that there should be proper education and training for bank employees.
- ❖ As there is lack of quick mechanism to solve customer complaints banks have pending cases more than the resolved ones.
- ❖ It has been found that cyber criminals have become more advanced and use new techniques to commit fraud which has become a challenging task for the less equipped banks.
- ❖ Online games have become a tool for the cyber criminals as many children are attracted towards it and there is a lack of awareness about these games among the customers.
- ❖ There is a lack of Cyber Police stations, infrastructure and qualified cyber officers in Bangalore City.
- ❖ The cost incurred to investigate a crime is double than the actual amount lost in the cybercrime.
- ❖ There is no direct awareness program from the banks about the cybercrimes because of which many customers becomes the victims of cybercrime.
- ❖ Many banks hide their cybercrime incidents from the public to maintain their goodwill and customers.
- ❖ Though Government has launched National Helpline No.155260 many people are unaware about it, which shows that there is no proper awareness among the public about the Governments initiatives.

VI. SUGGESTIONS

- It is easy for cyber criminals to send convincing emails which appears to be from your bank. Don't click on the links provided in such emails even if they look genuine. They could lead you to malicious websites.
- Whenever you receive a credit/debit card from the bank, make sure the letter is not damaged and it is sealed properly. In case, there are any signs of tampering with the package, please notify your bank immediately.
- Make sure to change the PIN of credit/debit card after receiving a new card from your bank. The PIN can be changed online by visiting your bank's website or at your nearest ATM machines.
- Always ensure that credit or debit card swipes at point of sale are done in your presence to avoid cloning/unauthorized copying of your card information. Do not let the sales person take your card away to swipe for the transaction.
- Take extra precaution while typing your password/PIN so that no one sees it. Try to cover the key-pad with your other hand while you type your PIN to avoid the number being picked up by someone monitoring CCTV footage.
- Register your personal phone number with your bank and subscribe to mobile notifications. These notifications will alert you quickly of any suspicious transaction and the unsuccessful login attempts to your net banking account.
- Always review transaction alert received on your registered mobile number and ensure that your transaction in billed according to your purchase.
- Keep an eye on the people around you while transacting at an ATM. Make sure that no one is standing too close to you while you transact at an ATM.
- Enable international transaction option on your credit card only when you are travelling abroad. Always ensure to disable international transaction option on your card upon return to your country.
- Always verify and install authentic e-wallet apps directly from the app store on your Smartphone. Do not follow links shared over emails, SMS or Social Media to install e-wallet apps.
- Do not save your card or bank account details in your e-wallet as it increases the risk of theft or fraudulent transactions in case of a security breach.
- Always type the information in online forms and not use the auto-fill option on your web-browser to fill your online forms they may store your personal information such as card number, CVV number and bank account number etc.
- Never disclose your net banking passwords, One Time Password (OTP), ATM or Phone Banking PIN, CVV number, expiry date to anyone, even if they claim to be from your bank. Also, never respond to mails asking for above details which seem to have received from your bank.
- No bank or its employees will ever call or email you requesting for your net banking passwords. One Time Password (OTP), ATM or phone banking PIN, CVV number, etc. such cases should be immediately reported to your bank.
- Always use strong passwords and prefer separate ID/password combinations for different accounts to prevent anyone from guessing them. Here are some examples of strong passwords.
- Always use virtual keyboards while logging into online banking services. This is specially adhered in-case

you need to access net banking facility from a public computer/cyber café or a shared computer.

- Do not make financial transactions over shared public computers or while using public Wi-Fi networks. These computers might have key loggers installed which are designed to capture input from keyboards and could enablefraudsters to steal your username and password.
- Always remember to log off from your online banking portal/website after completing an online transaction with your credit/debit card.
- Always delete the browsing data of your web browser (Internet Explorer, Chrome, FireFox etc.) after completing your online banking activity.
- Always be sure about the correct address of the bank website and look for the "lock" icon on the browser's status bar while visiting your bank's website or conducting an online transaction. Always be sure "https" appears in the website's address bar before making an online transaction. The "s" stands for "Secure" and indicates that the communication with the webpage is encrypted.
- Login and view your bank account activity regularly to make sure that there are no unexpected transactions. Report any discrepancies in your account to your bank immediately.
- Keep your bank's customer care number handy so that you can report any suspicious or unauthorized transactions on your account immediately.
- An awareness programs should be initiated by the Government in order to inform the public about the ongoing scenario and upcoming cyber threats.
- Apart from the SMS alerts banks must undertake direct awareness programs to spread awareness among all its customers to curb future cyber threats.
- The public should report these cases to the Cybercrime Branch in the matters related rather than just referring it to the banks, so as to ensure fast and strict actions.
- Punishment and penalties need to be exercised by the Government thoroughly in order to minimize the impact of these issues and penalize the attackers.
- Need for conducting training programs for the bank staff about recent cybercrimes and security measures.
- Need for connecting cybercafés with police control rooms.
- Banks should encourage cybercrimes victims to lodge complaints.
- The law enforcement should be very rigid and updated from time to time to keepa track of such crimes.
- Public should be informed not to use public Wi-Fi for banking.
- Bank customers should be informed not to respond to e-mail messages that askfor personal information.
- Scientific training to be provided by the Government to the investigating officersto deal with new frauds.
- Bank should develop cyber forensic and biometric techniques in its operations.
- Government should establish a computer crimes research and developmentcenters.
- Special Cybercrime investigation cell for Hi-tech crimes to be initiated andregulated by the government.
- Information technology department should be closely monitor Social networkingsites.
- Government should develop infrastructure of cyber investigation cell.
- The punishment for commission of cybercrime to be increased by the law makersto defer future offence.
- There should be proper implementation of the Government policies.
- Formulate separate department for Cybercrime investigation in the banks.
- Recruit the bank staff from the information technology disciplines.
- There should be compulsory paper for banking exam aspirants about cybersecurity.
- There must also be one subject related to ethical hacking and cyber security forlaw students so that they can solve the cybercrime cases more effectively.
- Banks should have Cyber Forensic experts to look after all the matters related toCybercrimes and cyber frauds.
- The customers must follow the below tips of safe online transactions to protecttheir hard earned money from cyber fraudsters

▪ Follow the 5Ps given by Michael Hauben that is (1) precaution, (2) Prevention, (3) Protection, (4) Preservation and (5) Perseverance. For ensuring cyber safety, he says that the motto for the "Netizen" should be "STRANGER IS DANGER".

VII. CONCLUSION

The conducted survey of this research based on 110 respondents made it possible to draw the conclusion of this research. It is important to understand and identify the security issues when dealing with online banking services. It is critical that customers must be aware about existing threats coming from computer fraudsters and criminals. Computer fraudsters use different techniques and methods such as computer hacking, phishing, vishing, identity theft, denial of services, social engineering and many more to steal the financial data of end users. Majority of our respondents are unaware of these threats, due to which they have become victims of cybercrimes. It is therefore important that online banking customers must be aware about these techniques

and methods used by computer fraudsters, banking industry must take positive initiative to achieve this objective. There must be complete privacy of customer's data in order to prevent cybercrimes.

It is not possible to eliminate cybercrimes from the cyberspace completely. But itcan be controlled by using preventive measures. History is the witness that no legislation has succeeded in totally eliminating cybercrimes. By the time regulators come up with preventive measures technology changes. This helps the criminals to find new areas to commit the fraud. Hence the only possible step is to make people aware of their rights and duties. Getting awareness about cybercrimes is customer's right and reporting cybercrimes is considered as their collective duty towards the society. Further there is a need to strengthen the enforcement of cybercrimes rules and regulations, and also there is a need to bring changes in the Information Technology Act to make it more effective to combat cybercrimes. Lastly it can be concluded saying that ***"INFORMATION IS WEALTH…"***

Information is the tool which the cyber criminals use to drain your wealth, hence be cautious while sharing your confidential Bank information online "*BE CYBER SMART, BE CYBER SAFE".*

BIBLIOGRAPHY

[1]. A. Sunitha, (2016, May), „E-Banking in India: Innovations, Challenges and Opportunities", Anveshana"s International Journal Of Research in Regional Studies, Law, Social Sciences, Journalism and Management Practices(AIJRRLJSM), Vol.1, Issue.4, (ISSN-2455-6602) Online.

[2]. Liaqat Ali, Faisal Ali, Priyanka Surendran, Bindhya Thomas(2017), „The Effects of Cyber Threats on Customer" s behavior in e-Banking Services", International Journal of e-Education, e-Business, e- Mangement and e-learning, Vol.7,Issue.1, pp.72-73

[3]. Divya Verma Gakhar.(2011) "Security Issues in E-Banking" Punjab Institute of Management and Technology (PIMT), Journal of Research Vol.1, NO.1, March-August 2008, pp.29-34.

[4]. Dr. Mrs. Suhasini V.Sant, Dr. R.P. Deshpande, Mr.K.R. Thaker, Mrs.Rakhi Pitkarand Mr.S.R Uchale, „Emerging Trends in Banking Industry", First Edition, Himalaya Publishing House, Mumbai, 2012.

[5]. Nina Godbole and Sunit Belapure, „Cyber Security", Second Edition, Willey IndiaPvt.Ltd., New Delhi, 2012.

[6]. https://gradeup.co/history-of-banking-in-india-i-e02deb86-f4ac-11e5-b410- 2f0cca4d3c07

[7]. https://en.m.wikipedia.org/wiki/History_of_banking

[8]. https://www.paisabazaar.com/banking/

[9]. https://cybersecurityventures.com/the-history-of-cybercrime-and-cybersecurity- 1940-2020/

[10]. https://www.mygreatlearning.com/blog/biggest-cyber-security-threats-indian- banking-sector

[11]. https://rebit.org.in/whitepaper/emerging-trends-and-challenges-cyber-security

[12]. https://en.m.wikipedia.org/wiki/State_Bank_of_India

[13]. https://www.sbi.co.in/corporate/AR1617/about_us_vision.html#:~:text=OUR%20 MISSION&text=We%20will%20create%20products%20and,do%20to%20those% 20in%20India.