International Journal of Managerial Studies and Research (IJMSR)
Volume 13, Issue 2, February 2025, PP 11-25
ISSN 2349-0330 (Print) & ISSN 2349-0349 (Online)
http://dx.doi.org/10.20431/2349-0349.1302002
www.arcjournals.org

A Study on Safe Banking Habits among Users in India.

Dr. Prashant Singh[1], Dr. Satrajeet Choudhury[1], Dr. Syed Aulia Mohiuddin[2], Ms. Chavi Jain[3], Ms. Rituparna Sharma[4]

[1]*Assistant Professor, Dept. of Management Birla Institute of Technology, Mesra, Ranchi India.*

[2]*Assistant Professor, Dept. of Business Management Gulf College Muscat Oman –Cardiff University UK.*

[3,4]*MBA Student, Birla Institute of Technology, Mesra, Ranchi India.*

Corresponding Author:** ***Dr. Syed Aulia Mohiuddin, *Assistant Professor, Dept. of Business Management Gulf College Muscat Oman –Cardiff University UK.*

Abstract: *The "Safe Banking Habits among Users in India" research aims to provide an in-depth analysis of cybercrimes in the banking sector, with a focus on India. The study will examine the different threats and vulnerabilities that banks face in the digital age, and suggest ways to prevent those threats from being realized. The primary objective of the study is to promote safe banking habits among users in India. By raising awareness about the risks associated with cybercrime, the study hopes to enhance consumer protection, support digital transformation, ensure regulatory compliance, promote financial education, and build trust in the banking sector. The research team believes that their study can aid in financial inclusion by making banking more accessible and secure for all users.*

1. INTRODUCTION

Banking has become an essential aspect of our everyday lives, as commercial transactions continue to increase in both quantity and complexity. The concept of banking initially arose from the need for a third party to act as a mediator between buyers and sellers, to hold custody of money and goods, remit funds, and collect proceeds. As the number of these intermediaries grew, there arose a corresponding need for control, which ultimately gave birth to the ideas of "banks" and "banking". Without credit and banks to issue it, most people would not be able to meet their financial requirements, and the world would not function smoothly. (Gajdhane, 2012)

Banking has evolved with trade, commerce, and politics. Temples were once safe havens for valuables, but banking became more widespread. Coins were the earliest form of money with a certificate of value stamped on them. Banks have advanced significantly since ancient times, but their fundamental business practices have remained the same. The primary goal of banks is to lend money and protect depositor funds.(Gajdhane, 2012)

Currently, there are various digital payment methods available in India. These include online or mobile wallets, which can be accessed through the internet or smartphone applications. Users can store money on the app by recharging through debit or credit cards or net banking. The consumer wallet limit is Rs. 20,000 per month, while the merchant wallet limit is Rs. 50,000 per month after self-declaration and Rs. 100,000 after KYC verification.

Prepaid credit cards function like gift cards, with funds pre-loaded into the individual's bank account. Customers can purchase using the available card balance instead of borrowing credit from the bank. The card can be recharged up to a prescribed limit, similar to mobile phone recharge.

Debit/RuPay cards are linked to an individual's bank account and can be used at shops, ATMs, online wallets, micro-ATMs, and for e-commerce purchases. In India, debit cards have surpassed credit cards in popularity. The number of debit cards increased to 630 million in December 2015 compared to 22.75 million in 2014.

The Aadhaar Enabled Payment System (AEPS) uses the 12-digit unique Aadhaar identification number to enable bank-to-bank transactions at PoS. AEPS offers services such as balance inquiry, cash withdrawal, cash deposit, and Aadhaar to Aadhaar fund transfers.

USSD is short for Unstructured Supplementary Service Data-based mobile banking. It is linked to a merchant's bank account and can be accessed via a mobile phone on a GSM network for payments up to Rs. 5,000 per day per customer.

The United Payments Interface (UPI) is a system that powers multiple bank accounts onto a single mobile application platform of any participating bank in India. It merges multiple banking features, ensures seamless fund routing, and allows for merchant payments. The UPI facilitates P2P fund transfers.(Singh & Rana, 2017)

1.1. Problem Statement

In recent times, with the increasing number of banks and financial institutions, there has been a significant rise in the number of threats related to banking. Therefore, our research study aims to investigate the safe banking habits practiced by users in India. We intend to delve deeper into the security measures adopted by individuals to protect their financial information and assets from various cyber threats such as identity theft, phishing scams, and malware attacks that have become increasingly common in recent years. By examining the practices and attitudes of users towards safe banking, we hope to provide valuable insights that can help improve the security of the banking system in India.

1.2. Theoretical Concepts and Framework

The banking industry in India has undergone a significant transformation over the years due to the rapid growth and cut-throat competition in the sector. The industry has seen a surge in technological advancements, fierce price wars, and product innovations, leading to the commoditization of services. Additionally, the public sector banks have lost their market share to private banks that have made an aggressive push to win over customers.

To gain insights into the Indian retail banking customers, a research study was conducted in the state of Karnataka. The study is empirical in nature and provides a detailed analysis of the various psychographic customer segments discovered. The paper covers two research studies. The first study analyzes the behavior and preferences of Indian retail banking customers using psychographics. The second study aims to understand users' behavioral tendencies towards passwords and identify the reasons behind the increasing vulnerability of passwords to cyber-attacks. Overall, both studies focus on safe banking habits and aim to provide a better understanding of the impact of user behavior on online security. (Srivatsa & Srinivasan, 2008)

The topic of safeguarding individuals from online attacks has always been a subject of debate, with arguments often arising over whether the responsibility should lie with technology manufacturers or end-users. To gain a better understanding of the users' behavioral tendencies in India towards safe banking habits, which are one of the cornerstones of online security, this paper aims to conduct a comprehensive study. The study will delve into various factors such as awareness levels, attitudes toward online security, common practices adopted by users, and the impact of such practices on the overall security of online banking transactions. The aim is to develop a better understanding of the challenges faced by users in India and to identify potential solutions for enhancing online security in the country.

The primary objective of this study is to conduct a comprehensive analysis of safe banking habits tendencies among the populace of India and their profound impact on online security. The study aims to explore the various factors that contribute to online security breaches and the measures that can be undertaken to prevent them. By examining the patterns of online behavior and identifying the vulnerabilities that exist in the current banking system, this study intends to provide valuable insights into how technology manufacturers and end-users can work together to create a safer online environment. The study will also offer a set of recommendations on best practices for safe banking habits that can help minimize the risk of online security threats and ensure the protection of personal and financial data.

1.3. Literature Review

The emergence of the Internet has given rise to new ways of conducting financial transactions. This has led to the introduction of "E-banking", a new era of banking that involves conducting financial transactions electronically. Previously, these transactions required a tangible exchange of information, but now they can be done electronically. While American customers have welcomed this development and its benefits, many Chinese customers are still hesitant to embrace E-banking due to concerns surrounding computer illiteracy, security, fraud, and theft. Chinese customers have traditionally

preferred tangible banking transactions. E-banking activities include buying and selling goods, paying bills, transferring funds, and managing investments. (Qiu, n.d.)

The COVID-19 pandemic has made India more adaptable to digital payment applications. They are user-friendly, convenient, and transparent. They have replaced traditional payment methods in many areas like shopping, ticketing, and fee payment. The Indian government has been promoting online payments aggressively through measures such as demonetization and Digital India. The COVID-19 crisis has further accelerated the adoption of online payment modes in India. Today, several service providers such as GPay, PhonePe, Paytm, Amazon Pay, and banking cards enable us to make payments with just one click. (Goplani et al., n.d.)

Growing concerns have been raised about the safety of young people online due to the increasing amount of technology being incorporated into their daily lives. Digital media poses a wide range of risks for youth, including exposure to risky posts and groups, fraud, misinformation, sexual violence, cyberbullying, harassment, and more. The media often draws attention to high-profile incidents involving sexual predatory behavior or catfishing to highlight the dangers of online activity. However, these well-publicized, viral tales often overshadow the much larger spectrum of less dramatic risks that young people frequently come across online. (Freed et al., 2023)

Convenience is the most critical factor when customers select a bank, irrespective of geographic region. While product utility and brand image are also essential, they are comparatively less significant than convenience. Customers are increasingly opting for newer channels, such as ATMs and internet banking, which are especially popular among those who are tech-savvy. However, some customers still prefer traditional branch banking due to safety concerns or a reluctance to embrace change. Regarding channel selection, convenience and security are crucial considerations. Telebanking, as a channel, was not widely adopted in any of the four regions, primarily due to concerns about safety and convenience. Concerning product selection, customers prioritize benefit maximization and convenience. Across all regions, customers look for products that offer more convenience at a lower cost, as well as additional benefits at no extra charge. (Srivatsa & Srinivasan, 2008)

As the prevalence of online fraud continues to grow, it is becoming increasingly important to take stronger measures to protect our sensitive information, particularly when we access banking websites. While some experts have suggested incorporating security features into websites that interrupt our browsing experience and guide us on how to stay safe, these measures may not be adequate. Features that are not immediately noticeable or rely on passive indicators may not be effective in safeguarding our data. Consequently, we need to adopt a more proactive approach to ensure that our sensitive information remains secure and protected from malicious cyber attackers. (Singh & Rana, 2017)

INTERNET BANKING – KEY RECOMMENDATIONS FOR BANKS

To help banks and other financial institutions address some of the critical concerns, here is a list of key issues and corresponding recommendations. These suggestions are designed to offer assistance to the financial sector in ensuring their operations are conducted effectively and efficiently.

Table 1.1

Consumer issues	Recommendations
Lack of awareness of internet banking and its benefits	-Attract consumer attention to internet services through better marketing -Inform consumers about the features, advantages and benefits of Internet banking, especially its convenience. -Allay consumer concerns about technology and support
Lack of dedicated unchallenged consumer internet access	-Establish facilities such as dedicated internet banking kiosks in banks and public places -Develop cheaper mobile alternative technologies * Both of the above would improve perceptions of convenience, shown to be a prime motivating factor in Internet banking use
Restrictive workplace access	-Offer incentives to businesses to facilitate internet banking
Lack of internet confidence	- Offer internet training
Competition with phone banking	- Offer training in internet banking

	- Market relative advantages of Internet banking, especially the convenience factors
Difficult initial setup procedure	- Streamline set-up procedures and provide set-up support
Difficult to use	- Improve screen design and navigation - Integrate banking systems
Lack of trust; Security and privacy risks	- Provide consumer reassurance and information - Improve application security and privacy, and bank information security and privacy - Assist consumers in developing secure Internet banking practices and risk management procedures
Inadequate knowledge and support	- Develop innovative consumer support solutions - Train branch staff in Internet banking - Develop new knowledge management strategies
Women's concerns	- Develop targeted strategies to improve women's access and internet self-efficacy, and address their technological concerns

Adapted from (Lichtenstein & Williamson: Consumer Adoption of Internet Banking) (Lichtenstein & Williamson, n.d.)

This table highlights a range of issues faced by consumers when using internet banking services and provides recommendations to address those challenges. Among the issues mentioned are a lack of awareness and confidence in using internet banking, difficulties accessing internet banking at work, competition with phone banking services, complex initial setup procedures, confusing user interfaces, and concerns regarding security and privacy. To address these issues, the table recommends a number of strategies, including better marketing to increase awareness and confidence, establishing dedicated internet banking kiosks, developing more affordable mobile alternatives, offering incentives and training to encourage adoption, improving the design and usability of internet banking interfaces, enhancing security and privacy measures, providing consumer education and reassurance, training staff to assist customers, and developing targeted strategies to improve women's access to and confidence in using internet banking services.

1.4. Significance of Study

Safe banking habits are crucial for safeguarding one's financial assets, personal information, and overall financial well-being. In today's digital era, where online banking and electronic transactions are widespread, consumers need to be aware of the best practices to protect their accounts and prevent fraud or identity theft. By developing and following safe banking habits, individuals can minimize the risk of becoming victims of financial scams, unauthorized transactions, or data breaches. Understanding safe banking habits among users in India has several significant advantages, as mentioned below:

- Financial Inclusion: Encouraging more individuals to engage with formal banking systems is possible by comprehending safe banking habits. Educating users about secure banking practices such as the protection of personal information, employing secure online banking platforms, and preventing scams, can help promote financial inclusion. This study can build trust in the banking sector and enhance financial literacy among users.
- Fraud Prevention: Preventing financial fraud, identity theft, and cybercrimes that can impact individuals' financial well-being is vital for safe banking habits. Informing banks, regulators, and policymakers about effective strategies to enhance security measures, detect fraudulent activities, and protect customers from financial losses by identifying common risky behaviors and vulnerabilities among users is crucial.
- Consumer Protection: Enhancing consumer protection measures in the banking sector can contribute to this study. Highlighting the importance of transparency, accountability, and fair treatment of customers can achieve this. Examining users' awareness of their rights, responsibilities, and recourse options in case of banking-related issues can inform regulatory efforts to strengthen consumer protection laws and mechanisms.
- Digital Transformation: Promoting secure online transactions, mobile banking practices, and digital payment methods is crucial with the increasing adoption of digital banking services in India.

Understanding safe banking habits among users can help banks improve their cybersecurity infrastructure and user experience by providing insights into user preferences, concerns, and behaviours related to digital banking technologies.

- Regulatory Compliance: Safeguarding customer data, preventing money laundering, and ensuring financial stability are regulatory requirements and compliance standards that banks and financial institutions are subject to. Assessing users' adherence to regulatory guidelines and best practices in banking operations can support efforts to enhance regulatory compliance, risk management, and governance frameworks within the banking industry.
- Financial Education: Safe banking habits are closely linked to financial education and literacy levels among users. Informing educational initiatives aimed at empowering individuals to make informed financial decisions, manage their finances effectively, and protect themselves from financial risks can be possible by examining users' knowledge of basic financial concepts, banking products, and security measures.
- Trust Building: Building trust between banks and customers is essential for maintaining a strong relationship based on transparency, reliability, and mutual respect. Exploring factors that influence users' trust in banks, such as data privacy policies, customer service quality, and dispute resolution mechanisms, can help banks strengthen customer trust, loyalty, and satisfaction levels.

Overall, the study on safe banking habits among users in India can promote financial inclusion, prevent fraud, enhance consumer protection, support digital transformation, ensure regulatory compliance, promote financial education, and build trust in the banking sector. Addressing these areas of concern can contribute to a safer, more secure, and resilient banking environment that benefits both users and financial institutions in India.

1.5. Objectives of the Study

- To assess the level of awareness among Indian banking users regarding safe banking practices and cybersecurity threats.
- To identify the common safe banking habits practiced by Indian consumers to protect their financial accounts and personal information.
- To analyse the factors influencing the adoption of safe banking habits among users in India, such as age, education, income level, and technological proficiency.

By addressing these objectives, the research paper aims to provide valuable insights into the current state of safe banking habits among users in India, identify areas for improvement, and offer recommendations to strengthen cybersecurity measures in the banking industry.

1.6. Hypothesis

Table 1.2

$H1_0$	There is no significant difference in checking bank balance behaviour with respect to gender.
H1	There is significant difference in checking bank balance behaviour with respect to gender.
$H2_0$	There is no significant difference in the willingness to share bank login credentials with anyone based on gender.
H2	There is significant difference in the willingness to share bank login credentials with anyone based on gender.
$H3_0$	There is no significant difference in falling victim to banking scams or fraud based on gender.
H3	There is significant difference in falling victim to banking scams or fraud based on gender.
$H4_0$	There is no significant difference in the frequency of reviewing bank statements and transaction history among different age groups.
H4	There is significant difference in the frequency of reviewing bank statements and transaction history among different age groups.
$H5_0$	There is no significant difference between age groups in being cautious before sharing bank details online.
H5	There is significant difference between age groups in being cautious before sharing bank details online.

$H6_0$	There is no significant difference in the frequency of changing their bank passwords among different age groups.
H6	There is significant difference in the frequency of changing their bank passwords among different age groups.
$H7_0$	There is no significant difference in number of people handing over their banking cards at places like petrol pumps with respect to their age groups.
H7	There is significant difference in number of people handing over their banking cards at places like petrol pumps with respect to their age groups.
$H8_0$	There is no significant difference in number of people using strong and unique passwords depending upon their educational background.
H8	There is significant difference in number of people using strong and unique passwords depending upon their educational background.
$H9_0$	There is no significant difference in number of people using 2-factor authentication for their bank accounts depending upon their educational background.
H9	There is a significant difference in number of people using 2-factor authentication for their bank accounts depending upon their educational background.

2. RESEARCH METHODOLOGY

This chapter explains the methodology that was utilized in conducting the research work. The key aspects discussed in this chapter include research design, sampling design, methods of data collection, analysis of data, and the limitations associated with the study.

2.1. Research Design

We carried out a study on Safe Banking habits among users in India and utilized a descriptive research design, which refers to the structure and plan of investigation employed to obtain pertinent answers to research queries. The descriptive research design is a methodical, empirical investigation that does not allow the researcher direct control over independent variables because those variables already exhibit or reflect the current situation. This design assesses the acquired findings using quantitative analysis. We chose this descriptive research design because it is ideal for studying variables that have already taken place. Additionally, this design enables our study to acquire original data for the research.

2.2. Sampling Design

Sample Size And Sampling Techniques

The process of sampling involves choosing a part of the population that accurately represents the entire population. For this particular research, the selection of respondents was done through a judgmental and convenience sampling method.

Sample Size: The sample consists of 286 respondents.

Sample Techniques: Judgmental sampling and convenience sampling are both types of non-probability sampling. In judgmental sampling, the researcher chooses participants based on their knowledge and professional judgment.

Sample size

The convenience sampling (sometimes known as accidental or opportunity sampling) involves the samples being drawn from that part of the population which is close to hand.

2.3. Data Collection Method

The data was collected both by primary and secondary methods .

- Primary data is the data that is collected for the first time through personal experiences or evidence, particularly for research. It is also described as raw data or first-hand information.
- Secondary data is a second-hand data that is already collected and recorded by some researchers for their purpose. It is accessible in the form of data collected from different sources such as government publications, censuses, internal records of the books, journal articles, websites and reports, etc.

A structured questionnaire comprising questions designed to fulfil the objectives of our research was used to gather the primary data. The secondary data was gathered from multiple research papers and

websites. (*CYBER CRIME IN BANKING SECTOR - CORE Reader.Pdf Case Study*, n.d.; "Cyber Crime in Banking Sector* "-Sanchi Agrawal, n.d.; Freed et al., 2023; Gajdhane, 2012; Goplani et al., n.d.; Lichtenstein & Williamson, n.d.; Metawa & Almossawi, 1998; Qiu, n.d.; Singh & Rana, 2017; Srivatsa & Srinivasan, 2008; Vyas, n.d.)

2.4. Analysis of Data: Tools and Techniques

For analysis of data collected we used Frequency tabulation, T-test for difference using SPSS and One-way Anova.

Table 2.1

Age						
			Frequency	Percent	Valid Percent	Cumulative Percent
Valid	18-24		226	79.0	79.0	79.0
	25-30		25	8.7	8.7	87.8
	31-45		27	9.4	9.4	97.2
	Above 45		8	2.8	2.8	100.0
	Total		286	100.0	100.0	

Out of the total sample surveyed 79% were of the age group 18-24; 8.7% were between 25-30; 9.4% were of 31-45 group and the rest 2.8% were above 45 of age.

Table 2.2

Gender					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	139	48.6	48.6	48.6
	Female	147	51.4	51.4	100.0
	Total	286	100.0	100.0	

Out of the 286 people surveyed 48.6% are male and the rest 51.4% are female.

Table 2.3

Education level					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Matric (10th)	5	1.7	1.7	1.7
	Intermediate (12th)	23	8.0	8.0	9.8
	UG	191	66.8	66.8	76.6
	PG	55	19.2	19.2	95.8
	Other	12	4.2	4.2	100.0
	Total	286	100.0	100.0	

Out of the total people surveyed 66.8% people did UG; 19.2% did PG; 8% studied till intermediate; 1.7 did matric and the rest 4.2% have some other qualifications.

Table 2.4

Profession					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Service	38	13.3	13.3	13.3
	Business	10	3.5	3.5	16.8
	Student	221	77.3	77.3	94.1
	Other	17	5.9	5.9	100.0
	Total	286	100.0	100.0	

Out of the total sample surveyed 77.3% were students; 13.3% were doing service; 3.5% were doing business and the rest 5.9% had others as their profession.

Table 2.5

Annual Income					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Upto 5,00,000	37	12.9	12.9	12.9

	5,00,000 to 10,00,000	17	5.9	5.9	18.9
	10,00,000 to 15,00,000	14	4.9	4.9	23.8
	Above 15,00,000	9	3.1	3.1	26.9
	Not Applicable	209	73.1	73.1	100.0
	Total	286	100.0	100.0	

Out of 286 people surveyed 12.9% earned upto 500000; 5.9% earned 500000-1000000; 4.9% earned 1000000-1500000; 3.1% earned more than 1500000 while the rest 73.1% were students and hence their annual income is not applicable

Table 2.6

Checking Bank Balance					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Multiple times a Day	32	11.2	11.2	11.2
	Once a Day	46	16.1	16.1	27.3
	Few times a week	103	36.0	36.0	63.3
	Once a week	49	17.1	17.1	80.4
	Less than once a week	25	8.7	8.7	89.2
	Rarely	31	10.8	10.8	100.0
	Total	286	100.0	100.0	

Out of 286 people surveyed 11.2% checked their bank balance multiple times a day; 16.1% checked once a day; 36% checked few times a week; 17.1% checked once a week; 8.7% checked less than once a week and the rest 10.8% checked rarely

Checking bank balance behavior with respect to gender

T-Test Group Statistics					
	Gender	N	Mean	Std. Deviation	Std. Error Mean
Checking Bank Balance	Male	139	2.98	1.396	.118
	Female	147	3.58	1.394	.115

Table 2.7

Independent Samples Test				
		Levene's Test for Equality of Variances		t-test for Equality of Means
		F	Sig.	t
Checking Bank Balance	Equal variances assumed	1.248	.265	-3.634
	Equal variances not assumed			-3.634

On the basis of T-test result the value of t is 3.634 which is more than the table value. There is a significant difference in checking bank balance behaviour with respect to gender. Hence, null hypothesis ($H1_0$) is rejected and the alternate hypothesis (H1) is accepted. We conclude that females more often check their bank balance as compared to males.

Sharing bank login credentials with anyone based on gender

T-Test

Group Statistics					
	Gender	N	Mean	Std. Deviation	Std. Error Mean
Sharing Bank Login Credentials	Male	139	4.50	.820	.070
	Female	147	4.46	.862	.071

Table 2.8

Independent Samples Test			
	Levene's Test for Equality of Variances		t-test for Equality of Means
	F	Sig.	t

Sharing Bank Login Credentials	Equal variances assumed	.387	.534	.412
	Equal variances not assumed			.412

On the basis of T-test result the value of t is 0.412 which is less than the table value. There is no significant difference in the willingness to share bank login credentials with anyone based on gender. Hence, the null hypothesis ($H2_0$) is accepted and the alternate hypothesis (H2) is rejected.

Falling victim to banking scams or fraud based on gender - Group Statistics					
	Gender	N	Mean	Std. Deviation	Std. Error Mean
Victim to banking scams or fraud	Male	139	1.94	.234	.020
	Female	147	1.93	.253	.021

Table 2.9

Independent Samples Test				
		Levene's Test for Equality of Variances		t-test for Equality of Means
		F	Sig.	t
Victim to banking scams or fraud	Equal variances assumed	.529	.467	.363
	Equal variances not assumed			.364

On the basis of T-test result the value of t is 0.363 which is less than the table value. There is no significant difference in falling victim to banking scams or fraud based on gender. Hence, the null hypothesis ($H3_0$) is accepted and the alternate hypothesis (H3) is rejected.

Table 2.10

Frequency of reviewing bank statements and transaction history among different age groups (Descriptive)						
Reviewing Bank statements and transaction history						
	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean	
					Lower Bound	Upper Bound
18-24	226	2.83	1.084	.072	2.69	2.97
25-30	25	2.44	.961	.192	2.04	2.84
31-45	27	2.63	1.182	.227	2.16	3.10
Above 45	8	3.38	.916	.324	2.61	4.14
Total	286	2.79	1.085	.064	2.66	2.92

ANOVA					
Reviewing Bank statements and transaction history					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	6.811	3	2.270	1.948	.122
Within Groups	328.601	282	1.165		
Total	335.413	285			

On the basis of One- Way ANOVA result the value of f is 1.948 which is less than the table value. There is no significant difference in the frequency of reviewing bank statements and transactions among different age groups. Hence, the null hypothesis ($H4_0$) is accepted and the alternate hypothesis (H4) is rejected.

Table 2.11

Cautious before sharing bank details online based on different age groups

Descriptives						
Cautious before sharing details online						
	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean	
					Lower Bound	Upper Bound
18-24	226	1.55	.904	.060	1.43	1.67
25-30	25	1.48	.653	.131	1.21	1.75
31-45	27	1.81	1.145	.220	1.36	2.27
Above 45	8	1.50	.926	.327	.73	2.27

Total	286	1.57	.910	.054	1.46	1.67

ANOVA

Cautious before sharing details online

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	1.959	3	.653	.786	.503
Within Groups	234.279	282	.831		
Total	236.238	285			

On the basis of One- Way ANOVA result the value of f is 0.786 which is less than the table value. There is no significant difference between age groups in being cautious before sharing bank details online. Hence, the null hypothesis ($H5_0$) is accepted and the alternate hypothesis (H5) is rejected.

Table 2.12

Frequency of changing their bank passwords among different age groups. Descriptives

Changing Banking Passwords/Pin

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean	
					Lower Bound	Upper Bound
18-24	226	3.55	.989	.066	3.42	3.68
25-30	25	2.64	1.221	.244	2.14	3.14
31-45	27	2.67	.832	.160	2.34	3.00
Above 45	8	2.63	.916	.324	1.86	3.39
Total	286	3.36	1.057	.062	3.24	3.49

ANOVA

Changing Banking Passwords/Pin

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	38.684	3	12.895	13.010	<.001
Within Groups	279.498	282	.991		
Total	318.182	285			

On the basis of One- Way ANOVA result the value of f is 13.010 which is more than the table value. There is significant difference in the frequency of changing their bank passwords among different age groups Hence, the null hypothesis ($H6_0$) rejected and the alternate hypothesis (H6) is accepted. We conclude that individuals of the age group 18-24 changes their banking passwords/pin more frequently than others.

Table 2.13

Handing over banking cards at places like petrol pumps with respect to different age groups.

Handing over cards to petrol pumps or other places

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean	
					Lower Bound	Upper Bound
18-24	226	3.71	1.216	.081	3.55	3.87
25-30	25	3.56	1.261	.252	3.04	4.08
31-45	27	3.07	1.542	.297	2.46	3.68
Above 45	8	4.00	1.414	.500	2.82	5.18
Total	286	3.64	1.267	.075	3.50	3.79

ANOVA

Handing over cards to petrol pumps or other places

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	10.885	3	3.628	2.290	.079
Within Groups	446.738	282	1.584		
Total	457.622	285			

On the basis of One- Way ANOVA result the value of f is 2.290 which is more than the table value. There is significant difference in number of people handing over their banking cards at places like petrol pumps with respect to their age groups. Hence, the null hypothesis ($H7_0$) is rejected and the alternate hypothesis (H7) is accepted. We conclude that the people above the age group 45 hand over their banking cards at petrol pumps or other places.

Table 2.14

Using strong and unique passwords depending upon educational background. Descriptives						
Using Strong and unique password						
	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean	
					Lower Bound	Upper Bound
Matric (10th)	5	2.00	1.732	.775	-.15	4.15
Intermediate (12th)	23	1.39	.499	.104	1.18	1.61
UG	191	1.65	.928	.067	1.52	1.78
PG	55	1.55	.919	.124	1.30	1.79
Other	12	1.42	.669	.193	.99	1.84
Total	286	1.60	.907	.054	1.50	1.71

ANOVA

Using Strong and unique password					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	2.824	4	.706	.857	.490
Within Groups	231.529	281	.824		
Total	234.353	285			

On the basis of One- Way ANOVA result the value of f is 0.706 which is less than the table value. There is no significant difference in number of people using strong and unique passwords depending upon their educational background. Hence, the null hypothesis ($H8_0$) is accepted and the alternate hypothesis (H8) is rejected.

Table 2.15

Using 2-factor authentication for bank accounts depending upon educational background

Descriptives						
Using two-factor Authentication						
	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean	
					Lower Bound	Upper Bound
Matric (10th)	5	4.80	.447	.200	4.24	5.36
Intermediate (12th)	23	2.35	1.465	.305	1.71	2.98
UG	191	2.34	1.370	.099	2.14	2.53
PG	55	2.42	1.524	.205	2.01	2.83
Other	12	2.83	1.749	.505	1.72	3.94
Total	286	2.42	1.445	.085	2.25	2.58

ANOVA

Using two-factor Authentication					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	31.865	4	7.966	3.972	.004
Within Groups	563.621	281	2.006		
Total	595.486	285			

On the basis of One- Way ANOVA result the value of f is 3.972 which is more than the table value. There is a significant difference in number of people using 2-factor authentication for their bank accounts depending upon their educational background. Hence, the null hypothesis ($H9_0$) is rejected and the alternate hypothesis (H9) is accepted. We conclude that individuals who have completed their matriculation (10th grade) use two-factor authentication more frequently than others.

2.5. Limitations to the Study

- The survey mainly included students as participants.
- The sample size was significantly smaller than the population.
- The study used convenience sampling which may have introduced bias as it relies on the availability of participants rather than random selection.
- Judgment sampling lacks objectivity. This can make it difficult to generalize findings to the broader population.

- Insufficient availability of resources such as budget, time, or access to necessary tools, equipment, et

3. Results and Discussion

- The survey was conducted at 286 people out of which 139 were males and 147 were females.
- Regarding the question "How frequently do you check your bank account balance?" There were 103(36%) who checked a few times a week; there were 49(17.1%) who checked it once a week; 46(16.1%) checked once a day; 32(11.2%) checked multiple times a day; 31(10.8%) checked rarely and the rest 25(8.7%) checked less than once a week.
- Regarding the question "Do you use strong, unique passwords for your banking accounts?" there were 172(60.1%) who always use strong passwords; 73(25.5%) who most of the time use strong passwords; 29(10.1%) who sometimes use strong passwords: 6(2.1%) who rarely use strong passwords; and the rest 6(2.1%) never use strong passwords.
- Regarding the question "How often do you share your banking login credentials with anyone?" There were 185(64.7%) who never share their banking login credentials; 68(23.8%) who rarely share their login credentials; 23(8%) who share their credentials sometimes; 6(2.1%) often share their credentials and the rest 4(1.4%) always share their credentials.
- Regarding the question "Do you make use of two-factor authentication (2FA) for your bank accounts?" there were 110(38.5%) who always use 2FA; 58(20.3%) who often use 2FA; 49(17.1%) who sometimes use 2FA; 27(9.4%) who rarely use 2FA and the rest 42(14.7%) who never use 2FA.
- Regarding the question "Do you reply to any phishing emails?" there are 278(97.2%) who do not reply to phishing emails and the rest 8(2.8%) have replied to phishing emails. Regarding the question "How often do you review your bank statements and transaction history?" there were 88(30.8%) who review their bank statements every month; 74(25.9%) who review every week; 74(25.9%) who rarely review; 40(14%) who review after every transaction and the rest 10(3.5%) never review their bank statements and transaction history.
- Regarding the question "Have you ever fallen victim to a banking scam or fraud?" 268(93.7%) never fell victim to a banking scam or fraud and the rest 18(6.3%) fell victim to a banking scam or fraud.
- Regarding the question "How cautious are you while providing personal or financial information online?" 175(61.2%) are very cautious while providing information online; 83(29%) are cautious that is they share only on trusted websites; 14(4.9%) are moderately cautious; 5(1.7%) are not very cautious and the rest 9(3.1%) are not cautious at all.
- Regarding the question "How often do you change your banking passwords/PIN?" 96(33.6%) who rarely change their passwords; 86(30.1%) who sometimes change their passwords; 52(18.2%) who often change their passwords; 41(14.3%) who never change their passwords and the rest 11(3.8%) who always change their passwords.
- Regarding the question "Do you hand over your banking cards to petrol pumps/at other places?" It is very unlikely for 98(34.3%) people to hand over their cards; for 66(23.1%) it is unlikely to hand over; 64(22.4%) samples are neutral; for 38(13.3%) samples it is likely and for the rest 20(7%) it is very likely to hand over their cards.
- When checking bank balance behavior is compared with respect to gender it is found that females check their bank balance more frequently as compared to males. There is no impact of gender while sharing bank login credentials, both males and females are cautious while sharing. Further, it was found that falling victim to a scam or fraud is not impacted by gender.
- There is no significant difference in the frequency of reviewing bank statements and transaction history as well as being cautious before sharing bank details online among different age groups. In frequency of changing passwords, it was found that the age group 18-24 change their passwords more frequently than others. Additionally, samples above the age of 45 were more likely to hand over their banking cards to petrol pumps or any other place.
- Samples who completed their matriculation use 2-factor authentication more frequently than others. There is no significant difference in the number of people using strong and unique passwords depending on their educational backgrounds.

4. CONCLUSIONS

Our research aims to delve into the different types of cybercrimes that are prevalent in the banking sector, particularly in India. We have conducted an in-depth analysis of the various threats and vulnerabilities that banks face in the digital age and have presented recommendations to prevent them.

In addition, we have also discussed several case studies that shed light on the cybercrime attacks that have occurred in Axis Bank, India's first ATM card fraud, CBI Threat-based fraud, and other similar incidents. These case studies provide valuable insights into the methods used by cybercriminals and the impact that such attacks can have on banks and their customers.

The study is focused on promoting safe banking habits among users in India. By raising awareness about the risks associated with cybercrime, we hope to enhance consumer protection, support digital transformation, ensure regulatory compliance, promote financial education, and build trust in the banking sector. We firmly believe that our study can aid in financial inclusion by making banking more accessible and secure for all users.

By addressing these areas of concern, we hope to contribute to a safer, more secure, and resilient banking environment that benefits both users and financial institutions in India. Our research project aims to achieve two significant objectives. Firstly, we intend to evaluate the awareness level of Indian banking users regarding safe banking practices and cybersecurity threats. In doing so, we will assess how well-informed the Indian banking user community is about the risks associated with banking transactions and the measures they need to take to protect themselves from cyber threats such as phishing, malware, and identity theft.

Secondly, we seek to examine the various factors that influence the adoption of safe banking habits among Indian users. These factors may include age, gender, education, profession, and other demographic variables. By analyzing the impact of these variables, we hope to identify the key drivers that motivate Indian banking users to adopt safe banking practices and take proactive measures to secure their financial information. Ultimately, our research will provide valuable insights that can help policymakers and financial institutions in India develop better strategies to enhance cybersecurity in the banking sector and safeguard the financial interests of Indian consumers.

As part of a research initiative, we conducted a comprehensive survey of 286 participants, with 139 males and 147 females. Our survey primarily focused on students between the age group of 18-24, who we found to be the most active users of banking services. We analyzed the result of our survey on three parameters those are age, gender, and education level.

After analyzing the survey results, we discovered that females tend to check their bank balance more frequently than males. This suggests that women are more mindful of their financial situation and are more proactive in monitoring their accounts.

However, we found no significant impact of gender when it comes to sharing bank login credentials with someone. Both males and females reported similar levels of caution when it comes to sharing sensitive financial information. This indicates that individuals of both genders are equally aware of the risks associated with sharing their bank login credentials, and take appropriate measures to protect their accounts.

Another interesting finding from our survey was that individuals between the ages of 18-24 tend to change their banking passwords/pin more frequently. This suggests that young people are more aware of the importance of cybersecurity and take proactive measures to protect themselves from potential threats.

The study has shown that individuals who have completed their matriculation tend to use two-factor authentication more frequently as compared to individuals holding other educational qualifications. This could be because matriculated individuals may have received more exposure to digital security measures during their education, leading to a greater awareness of the importance of securing online accounts. Additionally, individuals with higher educational qualifications may be more likely to have administrative access to accounts, which could reduce the need for using two-factor authentication as a security measure.

Lastly, we found that both males and females fall victim to banking scams and frauds irrespective of their gender. This highlights the need for increased awareness and education about the risks associated

with online banking, and the importance of taking proactive measures to protect oneself from potential threats.

Our research project has shed light on the critical issue of safe banking practices and cybersecurity in the banking sector. We have identified several factors that significantly influence the adoption of safe banking habits, such as user awareness, education, and trust in the banking system. Based on our findings, we believe that effective strategies can be developed to prevent cybercrimes and promote a safer banking environment for all users in India. We recommend that banks and financial institutions invest in advanced cybersecurity measures and prioritize customer education to help users understand the importance of safe banking practices. By doing so, we can create a more secure and reliable banking system that benefits everyone.

5. SUGGESTIONS

The following measures must be taken by banks and the government to promote safe banking practices among users in India:

- They should launch educational campaigns to raise awareness about safe banking practices among users. These campaigns can be conducted through various channels such as social media, workshops, seminars, and collaboration with educational institutions.
- They should provide guidance on how to securely conduct online banking transactions, including the importance of using strong passwords, avoiding public Wi-Fi networks for banking activities, and being cautious of phishing scams and fraudulent websites.
- They must encourage users to enable two-factor authentication for their online banking accounts. This additional layer of security helps protect against unauthorized access even if login credentials are compromised.
- They should advise users to regularly monitor their bank accounts and credit card statements for any unauthorized transactions or suspicious activities. Prompt reporting of such incidents to the bank can help mitigate potential losses.
- They must encourage users to keep their contact information updated with the bank to ensure timely communication of any security alerts or notifications regarding their accounts.
- They can provide tips for safe ATM usage, such as being vigilant of skimming devices, shielding the keypad while entering PINs, and avoiding using ATMs in secluded or poorly lit areas, especially at night.
- They should emphasize the importance of using unique and complex passwords for banking accounts and avoiding the reuse of passwords across multiple platforms. Recommending the use of password management tools can help users securely store and manage their passwords.
- They must ensure that users are aware of the procedures for reporting suspected fraud or security breaches to their bank. Providing a dedicated hotline or online portal for reporting such incidents can facilitate prompt action by the bank.
- They should educate users about legitimate channels for contacting customer support, such as verified phone numbers and official email addresses provided by the bank. Warn against responding to unsolicited communication claiming to be from the bank, especially requests for sensitive information.

REFERENCES /BIBLIOGRAPHY

CYBER CRIME IN BANKING SECTOR - CORE Reader.pdf case study. (n.d.).

"Cyber Crime in Banking Sector "-Sanchi Agrawal*. (n.d.). https://www.rbi.org.in/Scripts/PublicationsView.aspx?id=162

Freed, D., Bazarova, N. N., Consolvo, S., Han, E. J., Kelley, P. G., Thomas, K., & Cosley, D. (2023, April 19). Understanding Digital-Safety Experiences of Youth in the U.S. *Conference on Human Factors in Computing Systems - Proceedings*. https://doi.org/10.1145/3544548.3581128

Gajdhane, A. (2012). THE EVOLUTION OF BANKING IN INDIA Evolution of Banking System. In *Avishkar-Solapur University Research Journal* (Vol. 2).

Goplani, M. M., Goplani, M., Sabhani, J., & Gupta, A. (n.d.). *A STUDY ON USE OF DIGITAL PAYMENT APPLICATIONS FOR E-COMMERCE AMONG YOUTH*. https://doi.org/10.13140/RG.2.2.21134.08007

Lichtenstein, S., & Williamson, K. (n.d.). *UNDERSTANDING CONSUMER ADOPTION OF INTERNET BANKING: AN INTERPRETIVE STUDY IN THE AUSTRALIAN BANKING CONTEXT*.

Metawa, S. A., & Almossawi, M. (1998). Banking behavior of Islamic bank customers: Perspectives and implications. *International Journal of Bank Marketing*, *16*(7), 299–313. https://doi.org/10.1108/02652329810246028

Qiu, X. L. (n.d.). Chinese Customers' Banking Habits and E-banking Barriers. In *International Journal of Business and Management* (Vol. 3, Issue 2).

Singh, S., & Rana, R. (2017). Journal of Internet Banking and Commerce STUDY OF CONSUMER PERCEPTION OF DIGITAL PAYMENT MODE. In *Journal of Internet Banking and Commerce* (Vol. 22, Issue 3). http://www.icommercecentral.com

Srivatsa, H. S., & Srinivasan, R. (2008). NEW AGE YOUTH BANKING BEHAVIOR AN EXPLORATIVE STUDY IN THE INDIAN BANKING SECTOR. In *Journal of Services Research* (Vol. 8, Issue 2).

Vyas, S. (n.d.). *Impact of E-Banking on Traditional Banking Services*.

Neelanjit, D.(2024, March 2). 'Money Mule Scam, a new fraud': How to spot and safeguard your money from fraudsters. *The Economics Times.* https://m.economictimes.com/wealth/save/money-mule-scam-a-new-fraud-how-to- spot-and-safeguard-your-money-from-fraudsters/articleshow/108159178.cms

Fareha, N.(2024, February 26). 'NRI woman falls prey to ICICI Bank's fraud official, gets duped of 16 crore Rs.': 'We deposited our entire….'. *Livemint.* *https://www.livemint.com/news/nri-woman-falls-prey-to-icici-banks-fraud-official-gets-duped-of-rs-16-crore-we-deposited-our-entire-11708933038304.html*

How an ex-MD of an MNC lost Rs 4.8 crore from his bank account in online fraud. (2024, March 6). *The Times Of India. https://timesofindia.indiatimes.com/gadgets-news/how-an-ex-md-of-an-mnc-lost-rs-4-8-crore-from-his-bank-account-in-online-fraud/articleshow/108269791.cms*

Citation: *Dr. Prashant Singh, et.al., "A Study on Safe Banking Habits among Users in India. " International Journal of Managerial Studies and Research (IJMSR), vol 13, no.02, 2025, pp. 11-25. DOI: https://doi.org/10.20431/2349-0349.1302002.*