International Journal of Banking, Risk and Insurance
Volume 12 Special Issue (Contemporary Trends in Banking Risk and Insurance) 2024, 17-29
http://publishingindia.com/ijbri/
doi: https://doi.org/10.21863/ijbri/2024.12.sp.iss.003

Submitted: 17 May, 2024
Accepted: 21 May, 2024

Unraveling the Essence of Cybersecurity in Banking: Preserving Financial Integrity and Building Confidence

Priyanka Chadha*, Sonali P. Banerjee, Arhita Uppal***, Kanika Rana******

Abstract

There are more plastic cards in the wallet than currency notes. This change is because the Indian banking industry, is going through an IT revolution to be competitive with the other developed and developing nations and other regulatory reason has led to total banking automation in the Indian Banking Industry.

According to KPMG-CII report, India has the capability to become the third largest by 2025 and fifth largest in the world by 2020 in the banking industry. Also, India's banking industry is worth Rs. 81 trillion and it is utilising latest internet infrastructure to be competitive to other economies. The Indian banking system consists of 26 public sector banks, 20 private sector banks, and 43 foreign banks, together with 61 regional rural banks (RRBs) and over 90,000 credit cooperatives. The change towards internet banking is intensified by the changing dynamics in India as it is about to become one of the youngest countries in the world by 2020, the average age being 29 years. And this young population is technology savvy and wants real time online information. As the users of the online banking will increase rapidly in the years to come, these systems are becoming the most likelytargets of hackers and cyber criminals. Banking institutions must take all measures to make online banking system safe, to maintain the customer trust and satisfaction level for online banking. To be protected by the cyber security threat banking institutions will have to develop effective and efficient customer awareness programs as safety from cyber threats related to bank are equally interdependent on the level of awareness of using the banking online system and does not solely depend on the safeguards and practices implemented by the bank. This makes it very difficult for banking institutions to maintain the confidentiality and integrity of the banking system. The research will try to assess whether there is awareness of threats of online banking among the users that comprise online banking and to further analyse whether there is a difference in awareness of the users on the basis of Age and Gender.

Keywords: Economic Development, Financial Sector, The Banking System, IT Revolution, Cybersecurity, Online Banking

Introduction

Online Banking

Online banking is a process where a client can use a web browser to log onto the website of the bank which is installed on the client's personal computer or mobile phone, etc., and carry out activities such as online transactions, bill payments, account transfers, account inquiries and so on. At the fundamental level, online banking means setting up of an interface by a bank to provide information about its product and services to customers. To the next level in includes the series of different activities like transfer of funds, assessment of amounts and buying the products and services online It also involves newbanking services like electronic bill payments which assists the customers in

* Assistant Professor, Amity Business School, Amity University, Uttar Pradesh, India. Email: pnagarwal@amity.edu
** Assistant Professor, Amity Business School, Amity University, Uttar Pradesh, India. Email: Email: spbanerjee@amity.edu
*** Research Scholar, Amity Business School, Amity University, Uttar Pradesh, India. Email: arhitauppal@gmail.com
**** Research Scholar, Amity Business School, Amity University, Uttar Pradesh, India. Email: kanikarana71@gmail.com

receiving and paying bills online using the bank's website. This is also known as 'transactional' online banking.

Internet banking is done in four stages for a particular online transaction, firstly user should switch on the computer and browser, then open the online banking website of your bank and enter the id and password provided by the bank, secure socket layer encrypts the data between the user's computer and bank's server (Jhonson). As banks effectively decipher sent data and manage operations such as user verification, account queries, and transfers, the advancement of technology also comes a heightened risk of malicious assaults. These attacks present substantial dangers, which could result in victims losing their assets. The hackers tend to look for the weakest link, whether its host computer or banks server. Once the hacker gains the control of the whole system, can interrupt, intercept, modify and fabricate the information. So, security is one of the major concerns for E-Banking transaction. (Abrahams, 2023) In order to accomplish this goal, banks are prioritising the implementation of widely acknowledged cutting-edge technology standards for access control, data encryption/decryption, firewall protection, and verification of electronic signatures. Furthermore, there is equal importance given to teaching and increasing awareness regarding cyber risks (Petar, 2023).

E-Banking in India

E-banking in India is not a very old term in India, its origin is fairly recent. It is just started in India in early 90's before the only Branch banking system was prevalent. The traditional system on which the banking industry solely dependent upon seems to be slightly disappearing. In India the Internet banking was first launched by ICICI bank. Further HDFC and Citibank followed with E-Banking services in 1999. Government of India and RBI has taken many initiatives to develop the services of E-Banking in India. The legal recognition to electronic transactions and other electronic commerce means by Government of India came into effect from October 17, 2000 through IT act (Hasan, 2023). The Reserve Bank of India diligently oversees and assesses the legal and regulatory frameworks that regulate e-banking in order to promote its robust expansion. The purpose of doing so is to alleviate issues associated with e-banking and protect financial stability.

A renowned Committee, led by "Dr. K.C. Chakrabarty" and consisting of members from esteemed universities like "IIT, IIM, IDRBT," together with representatives from banks and the Reserve Bank, worked together to create the "IT Vision Document-2011-17." This document presents a strategic roadmap with the objective of enhancing the utilisation of IT in the banking sector providing guidelines for future progress (Kamuangu, 2024).

In order to maintain a leading position in the highly competitive worldwide market and in response to increasing pressure from multiple institutions, both commercial banks and the e-banking sector are implementing substantial measures. The main competitive leaders for e-banking services in comparison to public sectors in e-banking services are the private sector and foreign banks.

Consumer Awareness

The security of the banking system is contingent not only on the protective measures and protocols provided by the bank but also heavily on the users' awareness. This makes it very difficult for banking industry to protect information confidentiality and integrity. Institutions have made substantial historical and ongoing endeavours to educate clients. These efforts arise from the understanding that user awareness plays a vital role in protecting against information security threats. The unintended execution of malicious programs on users' PCs remains the most major hazard to internet banking. The hackers attack the weakest link, and once they have control the control information flow can be modified easily and take advantage. The institutions must periodically evaluate awareness and education programs. Management should periodically make changes to the customer awareness programmes.

Security Issues in Online Banking

Personal data of people such as their passwords, property, secrecy, identity information may get leaked if not taken care of. Theft or illegal data leak can lead to high security concerns (Pakojwar & Uke, 2014). The various information security breaches are:

Phishing: It is a type of cyber threat where hackers tends to be a trustworthy source to gain important information of users such as PINs, password and credit debit card data etc. through online network. These hackers use emails, messaging and such other tools to fool the users and hack their important information. These websites or emails look genuine and the users are often trapped in them (Khonji).

Pharming: It is a kind of cyber threat technique where the hackers reroute the users to a fake website which looks authentic to the users. Such websites look absolutely genuine to the users and so they do not hesitate in carrying out transactions using their debit or credit cards (Oškrdalová, 2014). As soon as they do these transactions, their card details get stolen.

Keystroke Logging: In this case the users download software without being aware of the threat that might follow. The hackers take control of the user's network and they are easily able to steal their passwords, credit cards and net banking details (Sbai, 2018).

Public Wi-Fi: Public Wi-Fi usually proves as a threat to people who carry out transactions using their smartphones. It usually proves to be an opportunity for hackers and thieves who want to steal the card details from the user's phone (McShane).

Malware: This is the software which under the control of the computer virus which once get a passage in a computer system or ATM and a bank server and allow hackers to access confidential data (Custers).

Merchant or Point of Sale Theft: Salespeople collect the user's credit/debit card to swipe or process a transaction, extracting data from the magnetic strip, so exposing it to potential harmful and unlawful exploitation.

Unsafe Apps: Unsafe online applications on online stores can gain access of the information on mobile phones and computers, such as passwords, PINs etc. and can be used for unauthorised transactions (Balakrishnan, 2016).

Skimming: Cybercriminals implant a data skimming device into the card reader slot to illicitly obtain information from the magnetic strips during the card swiping process. In addition, they strategically place a camera in close proximity to the machine to monitor the process of entering the password.

Card Trapping: This is a card trapping device installed by hackers in machines once the card is inserted it gets trapped inside. Hacker will take the card once the individual leaves to get help from the branch. Also in this case, Fraudster will try to see Card's secret code. (Suleman).

Shoulder Surfing: It is basically the use of the observation technique, like looking over one shoulder to get information, it is usually used to obtain password (Rajarajan, 2014).

Card Cloning: A common technique used for card fraud is the utilisation of a device referred to as a card skimmer. This device is specifically engineered to covertly acquire all the information stored on a card, allowing criminals to gain unauthorised access to the victim's funds. Usually, card skimmers are attached to the card slots of ATMs. However, criminals have been observed installing them on any device that takes debit or credit cards, like ticket terminals found at train stations. In less advanced techniques, criminals also attempt to obtain the victim's PIN by putting small cameras near the keypad. These cameras are frequently hidden behind a deceptive facade on the device, making them difficult to identify (Fatimah, Marzanah & Aida, 2013).

Identity Theft: This is a kind of cyber threat where the personal data of the user, like date of birth, driving license number, bank information, etc. is obtained and then used for carrying out illegal transactions. The fraudsters use this information to carry out criminal activities for buying goods and services, apply for credit, or other activities related to the user's bank account (Rajarajan, 2014).

Review of Literature

Pakojwar and Uke (2014) reported in their paper that Internet banking allows customer to conduct transactions easily and also increases effectiveness and efficiency for banks. But, implementing of safe and convenient web-based banking is challenging. For smooth functioning, effective planning is required. Studies in the past have revealed that advanced technology have played an important role in controlling the factors that have caused risk through authentication system. For implementing the proper authentication system there is a need of assessing the risks faced by the Internet Banking System. Study

also revealed that public bank is having only 20–30% net banking user's while 70–80% users are there in Private banks. Most of the banks get their server secured by Symantec Corporations USA with secure protocol and message Authentication.

"Chauhan, Vikas and Choudhary, Vipin" (2015) in their paper have tried to elaborate about the concept of internet banking and studied its benefit from consumer's Point of view. The research related with the internet banking in Indian, its challenges and opportunities have been discussed. This study concluded that the Internet banking in India is slowly and gradually gaining acknowledgement and the government is making efforts to make it more prevalent and users more aware of it.

Jassal (2013) this study examined the underlying reasons for cybercrimes and the roles played by both users and banks in facilitating the infiltration of other networks by cybercriminals or hackers. Furthermore, its objective was to pinpoint the diverse weaknesses in networks that provide risks to both account holders and financial institutions. It is imperative to comprehend that cybercrimes arise not only from the incompetence of financial institutions or deficiencies in cybercrime units, but also from the level of awareness among users. Consequently, it is imperative to provide users with similar education regarding these offences.

"Dagar, Anju" has presented in her paper that E-Banking has changed the basic meaning of bank by creating the new opportunities and by not limiting the banking to the boundaries of the branch of the bank. The study also compared the traditional banking with online banking and presented its benefits. Customer satisfaction is the most basic goal of banking service providers because customers can access their account whenever and wherever they want and creating more involvement in banking. (Abrahams, 2023) Banks should provide more convenient facilities to customers and also implement awareness programs so that user can easily make transactions through online banking system safely and securely, as it is a bit difficult.

Pakojwar and Uke (2014) presented in the paper that through internet banking it becomes easy for the customers to conduct transactions easily and effectively for banks. But, implementing of safe and convenient web-based banking is challenging. For smooth functioning, effective planning is required. Studies in the past have revealed that advanced technology have played an important role in controlling the factors which have caused risk through authentication system. For implementing the proper authentication system there is a need of assessing the risks faced by the Internet Banking System. This study also reported that only 20–30% of the net banking users are there in the public bank whereas about 70–80% users are of the private bank. Most of the banks get their server secured by Symantec Corporations United states of America with secure protocol and message Authentication (Kamuangu, 2024).

(Morufu & Idris, 2014) In their study discussed that cyber security threats mostly effects the online banking users who negligently provide their details during online banking. There is a need for proper banking awareness for the users so that they don't become victims by losing their important information online. Many users readily embrace online banking services without fully comprehending the accompanying cyber risks. Ensuring information security awareness is essential for providing guidance to customers who use online banking services. Consequently, banking institutions must improve and fortify their awareness initiatives to guarantee efficacy.

(Fatimah, Marzanah & Aida, 2013) Have found in their study that there is no level of association in genders of respondents in case of cyber security awareness both males and females have similar level of awareness. However, the users with higher education level are more aware than the user of low education level i.e. there is a level of association between both. It can be seen form the result revealed in the study as people with higher education level focus more on the security measures such as password changing, creating unique password and checking the status bar. While both males and females with lower education level has low awareness in terms of technical measures such as reading privacy and policy information, updating latest software and scanning e-mail attachments.

The study underscores the necessity of proactive cybersecurity measures in financial institutions by examining the strategies used by cybercriminals and how they change their strategies in response to security

measures. It also points out areas of missing research in the body of current literature and makes suggestions on how to solve these problems. Additionally, in order to improve cyber threat identification and response procedures in the banking sector, the paper presents the Digital Forensics and Incident Response (DFIR) methodology. The paper's complete strategy attempts to protect the integrity of financial institutions and their clients by reducing the dangers associated with ransomware and crypto jacking assaults (Naresh Kshetri, 2023).

This study paper's main goal is to examine the state of e-banking today and the new technical tools that the banking industry is using. As a result, more and more knowledgeable clients—especially young ones—are using mobile applications for e-banking services. Customers can use internet banking for a variety of services, such as bill payments and money transfers (RTGS and IMPS). Compared to the public banking sector, the private banking business is growing at a far faster rate. The banking industry has seen tremendous transformation due to the advent of new technical breakthroughs, which is responsible for this expansion. The knowledge gained from this study will help Indian banks better understand how people are using developing technologies and how aware they are of them. Additionally, it will support the development of fresh approaches to improve the efficacy and efficiency of banking operations (Kunte).

This article presents an improvement to the extremely successful financial fraud detection system, Bank sealer. In contrast to earlier versions, Bank sealer was not able to use analyst comments for performance enhancement and self-tuning. It also depended on a complicated set of settings that needed to be manually adjusted before to deployment (Carminati, 2017).

It suggests an evolutionary wrapper method that is supervised in order to overcome these drawbacks. By using analyst input on fraudulent transactions, this method improves Bank sealer's detection capabilities by automatically adjusting feature weighting. To do this, our approach uses a multi- objective genetic algorithm. The paper put solution into practice and tested it in a major national banking group's operating setting. We show through thorough experimentation that our suggested system is able to detect complex fraud efforts. In fact, in certain cases, our method helped Bank sealer achieve performance gains of up to 35% (Carminati, 2017).

Research Methodology

This chapter underlines the methodology and the approaches being used in the study to examine how much the customer are having the awareness about the cybersecurity with respect to banking. This chapter delves to focus on the sample size that has been chosen along with the different techniques being employed for the collection of data. To addition to this chapter also indicates about the methods used for data analysis and the type of data being collected along with the appropriate research design for the study.

Research Objective

- To analyse whether users of online banking are completely aware of the threats or dangers that comprises online banking.
- To analyse the level of online banking user's awareness.
- To assess whether there is different in awareness of the users on the basis of Age and Gender.

Research Design

Given the research objective and framework, we have opted to undertake this study using a quantitative technique. For the collection of data, the methodology which is applied for this study is survey-based. There are different methods which are part of this methodology for the collection of data such as telephonic interview, surveys through mail, personal interviews and surveys conducted online, etc. For this research use of self-administered questionnaire was selected.

Data Collection Method

The researchers employed a survey distributed to participants to examine customers' perspectives on brand loyalty in the hotel industry. The questionnaire was meticulously crafted to ensure user-friendliness and

understanding for the respondents. Technical language was avoided to reduce the possibility of misinterpretation. A range of sources, including books, research papers, periodicals, newspapers, journals, and the internet, were used to gather secondary data.

In order to conduct a thorough analysis, a sample of 150 individuals was chosen from the target population. The sample included both males and females, and their ages ranged from 21 to 50 years old.

Sampling Design

The study employed a straightforward random sampling technique to collect data. The study utilised convenience sampling, a non-probability sample technique, where respondents were selected based on their convenience. Questionnaires were provided to the respondents in a systematic manner in order to gather data for the study.

Sample Description

The demographic distribution of the respondents is depicted in the following table:

Table 1: Gender Demographics

		Gender		
		Female	Male	Total
Age	21-30	41	41	82
	31-40	13	15	28
	40+	15	25	40
Total		69	81	150

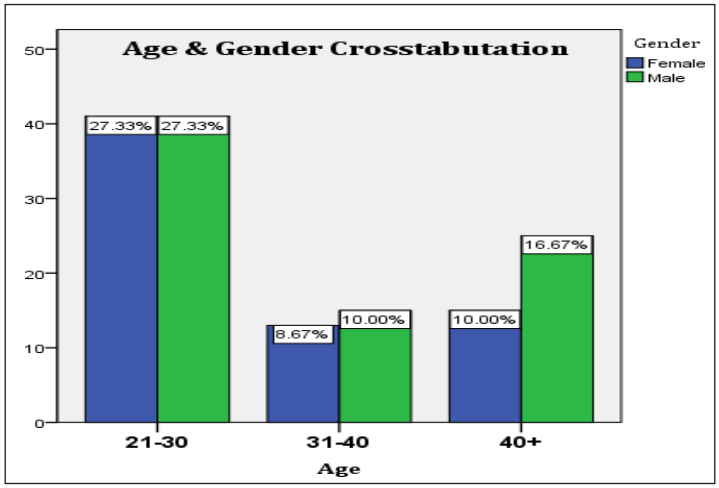
Tools for Analysis

For the statistical analysis of this study the tools which have been used are cross tabs and Chi-Square test and with the use of bar graph and column charts for data interpretation.

Data Analysis and Interpretation

Table 2: Analysis on the Basis of Demographic Profile (Age & Gender)

Table1 Age & Gender Cross Tabulation				
		Gender		
		Female	Male	Total
Age	21-30	41	41	82
	31-40	13	15	28
	40+	15	25	40
Total		69	81	150



Graph 1

Table 2 and Graph 1 presented above illustrate the demographic distribution of the respondents from whom the data was gathered. Among the 150 responses, there were 69 girls and 81 boys. Out of the total respondents, 81 individuals were between the ages of 21 and 30, 28 individuals were between the ages of 31 and 40, and 40 individuals were over the age of 40. The gender distribution exhibits a very equitable representation. In terms of age distribution, 18% of the respondents fell within the 31-40 age range, 26% were above the age of 40, and the remaining 56% were between the ages of 21 and 30 years old.

Graph

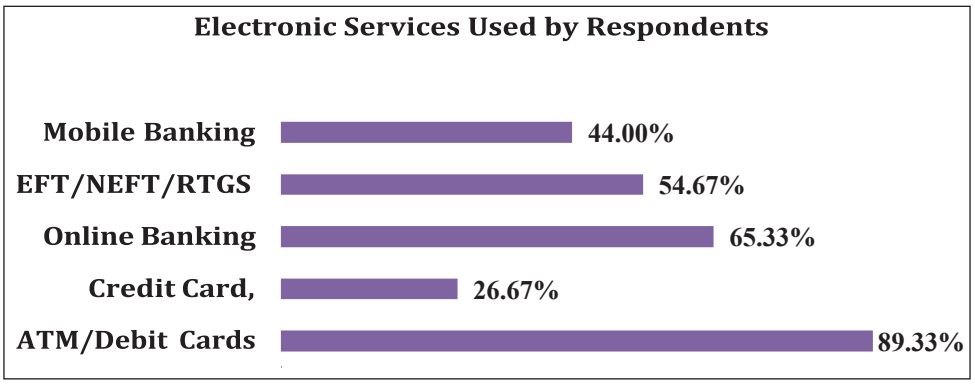


Fig. 1: Electronic Services Used by Respondents

Fig. 1 represents the frequency of the electronic services provided by bank used by the respondents. Out of 150 respondents 90% respondents use Debit Cards that is the highest level of electronic service used then only 65% of the respondents use Online Banking while only 55% and 45% of the respondents use electronic fund transfers and mobile banking services respectively. While the lowest credit card showed the lowest result only 27% of respondents use credit cards.

Graph

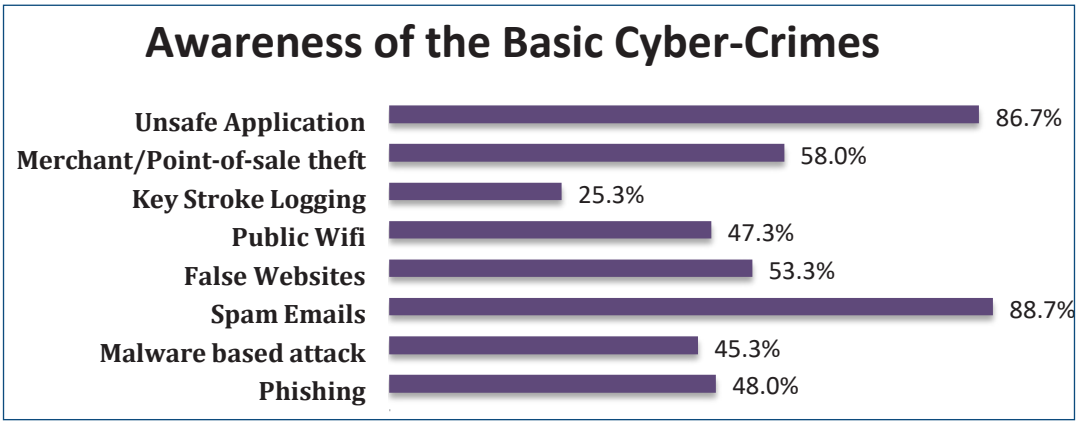


Fig. 2: Analysis of Awareness Level of Respondents of Cyber Crimes

The above bar graph (Fig. 2) highlights the data of the respondents who are aware of the basic cyber crimes with respect to online banking. From the results, it can be comprehended that on an average, typically respondents are not much knowledgeable about the cybercrimes. Around 85-90% of Respondents are aware about crime related to spam emails and usage of unsafe applications which is the most basic cyber security crime, while

around only 50% of the respondent were about the crimes such as Phishing, malware-based attack, false websites, and public Wi-F and point-of-sale cyber security crimes which is very low and only 25% of respondents were aware about Key stroke login.

Table 3: Gender and Cyber Crimes Cross Tabulation

Table_ Gender &Cyber Crimes Cross Tabulation					
		Gender			
		Female	%	Male	%
Cyber Crimes	Phishing	37	53.62%	35	42.68%
	Malware based attack	28	40.58%	40	48.78%
	Spam Emails	64	92.75%	69	84.15%
	False Websites	42	60.87%	38	46.34%
	Public Wifi	33	47.83%	38	46.34%
	Key Stroke Logging	18	26.09%	20	24.39%
	Merchant/point-of-sale theft	43	62.32%	44	53.66%
	Unsafe Application	65	94.20%	65	79.27%

Table 3 above shows that awareness of the basic cybercrimes related to online banking varies on the basis of age there is difference respondents younger age, i.e. 21-30 are more aware of the crimes as compared to the respondents of age between 31-40 and more than 40.

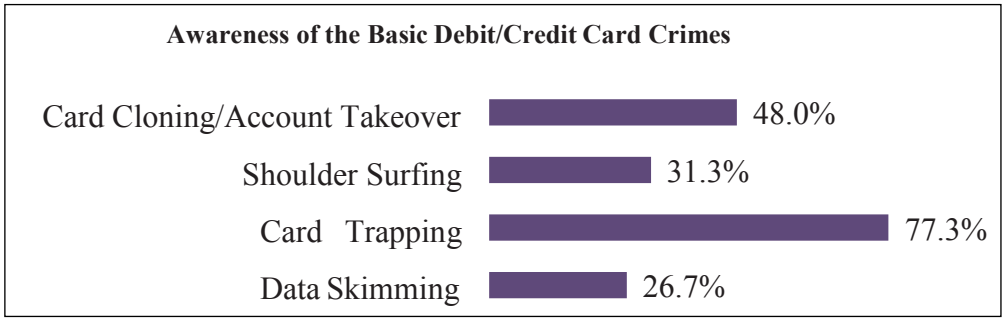


Fig. 3: Analysis of Awareness Level of Respondents of Cyber Crimes Related Debit/Credit Card

The graph above represents the data about the awareness of the respondents of the basic cyber-crimes related to Debit/Credit Card. Result shows that on an average respondent are not much aware about the cybercrimes. Most of the respondents (i.e.70%) were only aware about card trapping, while only 48% about card cloning. only 31% and 27% respondents were aware about Shoulder Surfing and Data Skimming respectively.

Table 4: Gender and Card Crimes Cross Tabulation

Table Gender& Card Crimes Cross Tabulation					
		Gender			
		Female		Male	
		Count	%	Count	%
Card Crimes	Data Skimming	15	**21.74%**	25	**30.86%**
	Card Trapping	53	**76.81%**	65	**79.26%**
	Shoulder Surfing	26	**38.23%**	32	**39.51%**
	Card Cloning/Account Takeover	35	**50.72%**	40	**48.78%**

After doing a more thorough examination of the data provided in the table about awareness of cybercrimes associated with debit/credit cards, it is clear that there is only a slight variation in awareness levels between genders. Both male and female respondents exhibit comparable levels of awareness regarding cybercrimes. Nevertheless, it is important to acknowledge that the general level of awareness remains rather limited.

Table 5: Age and Card Crimes Cross Tabulation

Table Age & Card Crimes Cross Tabulation							
		Age					
		21-30	%	31-40	%	40+	%
Card Crimes	Data Skimming	25	30.49%	5	17.86%	8	20.00%
	Card Trapping	68	82.93%	14	50.00%	31	77.50%
	Shoulder Surfing	30	36.59%	8	28.57%	12	30.00%
	Card Cloning/Account Takeover	43	52.44%	11	39.29%	14	35.00%

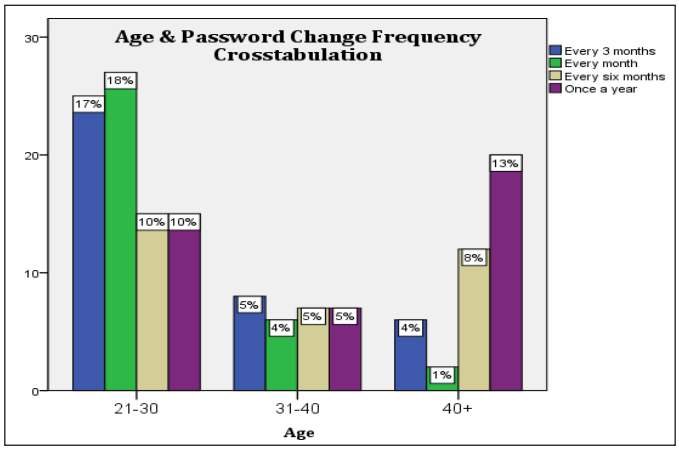
Further analysing the data on the basis of age as shown in Table 5 above it can be concluded that there is association between age and the awareness level of respondents. The respondents of younger age tend to know more about the cyber-crimes related to cards. On each of the different cyber-crime terms i.e. data skimming, card trapping, shoulder surfing and card cloning respondents of the age group 21-30 are more aware as compared to age group 31-40 and 40+.

Table 6: Age and Password Change Frequency Cross Tabs

Table_ Age & Password Change Frequency Cross Tabulation					
		Age			
		21-30	31-40	40+	Total
Password Change Frequency	Every month	27	6	2	**35**
	Every 3 months	25	8	6	**39**
	Every six months	15	7	12	**34**
	Once a year	15	7	20	**42**
Total		**82**	**28**	**40**	**150**

Table 7: Age and Password Change Frequency

Table_ Age & Password Change Frequency			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	23.080[a]	6	.001
Likelihood Ratio	24.786	6	.000
N of Valid Cases	150		
a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 6.35.			



Graph 2

Hypotheses

H0: There is no significant association between gender and password change frequency.

H1: There is a significant association between gender and password change frequency.

Results

Table 7 presents the frequency and result of the Chi-square test, which indicates the statistical analysis performed on the data.

- The value of the test statistic is 23.080.
- The exception that no cell should have an expected count less than 5 was met.
- The test statistic is calculated based on a 3x4 cross-tabulation table. The degrees of freedom (df) for this test statistic can be calculated by subtracting 1 from the number of categories and multiplying it by the number of levels in each category minus 1.
  - df = (R−1) * (C−1)

    (3−1) * (4−1) =6
- The p-value of the test statistic is $p = 0.001$

Conclusion: from Chi-Square test statistics of 23.080 where significance value < 0.05 (i.e. .001) it can be concluded that there is significant association between.

Table 8: Gender and Password Change Frequency, Cross Tabs, and Chi-Square Test

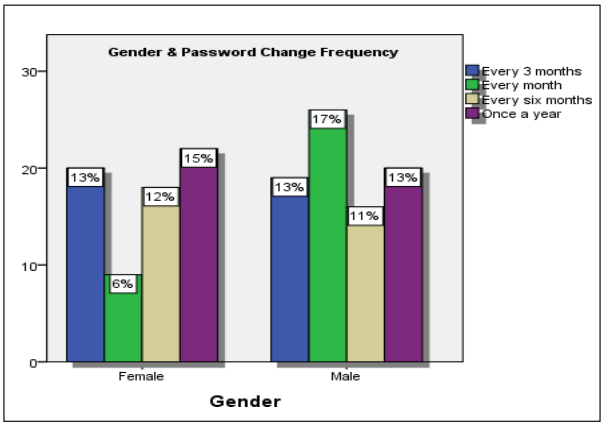
Table _Gender & Password Change Frequency Cross Tabulation

		Gender		
		Female	Male	Total
Password Change Frequency	Every 3 months	20	19	**39**
	Every month	9	26	**35**
	Every six months	18	16	**34**
	Once a year	22	20	**42**
Total		**69**	**81**	**150**

Table_ Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	7.584[a]	3	.055
Likelihood Ratio	7.895	3	.048
N of Valid Cases	150		

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 15.64.



Graph 3

Hypotheses

H0: There is no relationship between age and password change frequency.

H1: There is a relationship between age and password change frequency.

Results

The frequency and result of the Chi-Square test as shown in Table 8 represents the following:

- The value of the test statistic is 7.584.
- The exception that no cell should have an expected count less than 5 was met.
- Because the test statistic is based on a 2x4 cross tabulation table, the degrees of freedom (df) for the test statistic is:

$$df = (R-1)*(C-1)$$
$$(2-1)*(4-1) = 3$$

- The p-value of the test statistic is $p = 0.055$

Conclusion: From Chi-Square test statistics of 7.584 where significance value > 0.05 (i.e. .055), null hypotheses is accepted there is no significant association between the 2 variables(i.e. Gender & Password Change Frequency).

Table 9: Age and Password Change Frequency Cross Tabs and Chi-Square Test

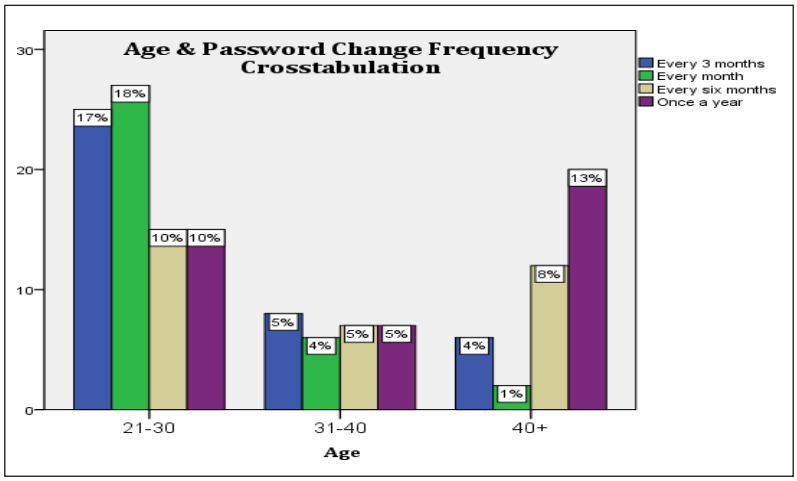
Table_ Age & Password Change Frequency Cross Tabulation

		Age			
		21-30	31-40	40+	Total
Password Change Frequency	Every month	27	6	2	**35**
	Every 3 months	25	8	6	**39**
	Every six months	15	7	12	**34**
	Once a year	15	7	20	**42**
Total		**82**	**28**	**40**	**150**

Table_ Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	23.080[a]	6	.001
Likelihood Ratio	24.786	6	.000
N of Valid Cases	150		

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 6.35.



Graph 4

Hypotheses

H0: There is no significant association between gender and password change frequency.

H1: There is significant association between gender and password change frequency.

Results

The frequency and result of the Chi-Square test as shown in Table 9 represents the following:

- The value of the test statistic is 23.080.
- The exception that no cell should have an expected count less than 5 was met.
- Because the test statistic is based on a 3x4 cross tabulation table, the degrees of freedom (df) for the test statistic is

  $df = (R-1)*(C-1)$

  $(3-1)*(4-1) = 6$
- The p-value of the test statistic is $p = 0.001$

Conclusion: From the Chi-Square test statistics of 23.080 where significance value < 0.05 (i.e. .001) it can be concluded that there is significant association between the 2 variables (i.e. Age & Password Change Frequency). With people with age tend to become negligent towards changing their password frequently. This is a basic and very importantfactor to be safe against cybercrimes.

Findings

The findings from the studies were as follows:

- Although the government has made significant efforts to promote digitalisation through projects such as Digital India, a significant number of respondents still show a clear preference for traditional banking methods. An overwhelming majority, accounting for almost 89%, predominantly use debit cards for ATM purchases. However, the rates of usage for internet banking and mobile banking are far lower, at 65% and 44% respectively.
- Awareness of the respondents about basic cybercrimes related to online banking is very low, only around 50% respondents knew about the most prevalent cyber-crimes like Phishing, Pharming and malware-based attacks.
- The study's findings indicate that most respondents utilise debit cards, yet there is a worrisome lack of information regarding crimes related to debit/credit cards. Only 26% of participants demonstrated awareness of data skimming, while 31% were familiar with shoulder surfing. A mere 48% possessed knowledge regarding card cloning.
- There is no association between gender and password changing frequency null hypotheses was accepted both males and females have same awareness level.
- There is an association between the age and the password changing frequency in this case null hypotheses were rejected. Respondents of the younger age group i.e. 21-30 tends to change password more frequently as compared to the older age group i.e. 31-40 and 40+.

Conclusion

The main aim of the study was to evaluate the extent of awareness regarding security risks associated with online banking, specifically among individuals who utilise online banking services. The findings suggest a pervasive lack of knowledge among participants, despite frequent utilisation of computers and the internet for professional and educational purposes. Notably, gender did not have a major impact on awareness levels, as both male and female respondents exhibited similar levels of awareness. Nevertheless, there was a distinct disparity in knowledge between younger and older age cohorts, with younger participants exhibiting a greater degree of awareness regarding computer security measures and cybercrimes.

Younger participants exhibited a greater emphasis on security measures, such as proficient password management and awareness of cybercrimes. In contrast, older participants, regardless of gender, displayed a lack of proficiency in technological measures, such as regularly upgrading passwords and comprehending cybercrimes.

Considering the unavoidable rise of cybercrime, it is crucial to carry out further promotional initiatives to

increase awareness among respondents and safeguard them against online banking threats. According to the results, it is recommended to focus promotional campaigns on older age groups, as they seem to be more susceptible and require increased knowledge and education on online banking security.

References

Abrahams, T. O. (2023). Review of strategic alignment: Accounting and cybersecurity for data confidentiality and financial security. *World Journal of Advanced Research and Reviews, 20*(3), 1743-1756.

Verma, A. K., & Sharma, A. K. (2014). Cyber security issues and recommendations. *International Journal of Advanced Research in Computer Science and Software Engineering, 4*(4), 629-634.

Balakrishnan, L. (2016). A study on the security problems in mobile banking services provided by banks. *Surya-The Energy*.

Carminati, M. V. (2017). *A supervised auto-tuning approach for a banking fraud detection system.* In Cyber Security Cryptography and Machine Learning: First International Conference, CSCML 2017, Beer- Sheva, Israel (pp. 29-30). Springer International Publishing.

Custers, B. H. (n.d.). Banking malware and the laundering of its profits. *European Journal of Criminology, 16*(6), 728-745.

Fatimah, S., Marzanah A., J., & Aida, M. (2013). Measuring computer security awareness on internet banking and shopping for internet user. *Journal of Theoretical and Applied Information Technology*, *53*(2), 210-216.

Hasan, M. T. (2023). Cybersecurity in bank: A case on employee engagement and responsibility for a Secure Digital Environment (SDE) in the selected branch.

Jhonson, D., Smith, J., & Shehzadi, T. (2023). Digital trust and financial transactions: Building confidence in internet banking systems.

Kamuangu, P. (2024). A review on cybersecurity in Fintech: Threats, solutions, and future trends. *Journal of Economics, Finance and Accounting Studies, 6*(1), 47-53.

Khonji, M. I. (n.d.). Phishing detection: A literature survey. *IEEE Communications Surveys & Tutorials, 15*(4),2091-2121.

Kunte, B. (n.d.). A study on e-banking and emerging technology tools in Indian banking industry.

Lal, R., & Saluja, R. (2012). E-banking: The Indian scenario. *Asia Pacific Journal of Marketing & Management Review*, *1*(4).

McShane, I. G. (n.d.). Practicing safe public wi-fi: Assessing and managing data-security risks.

Morufu, O., Victor O., W., & Idris, I. (2014). Assessment of information security awareness among online banking customers in Nigeria. *International Journal of Advanced Research in Computer Science and Software Engineering*, *4*(6), 13-24.

Kshetri, N., Rahman, M. M., Sayeed, S. A., & Sultana, I. (2023). CryptoRAN: A review on cryptojacking and ransomware attacks w.r.t. banking industry - Threats, challenges, & problems. *arXiv preprint arXiv:2311.14783*.

Oškrdalová, G. (2014). Pharming in the e-banking field and protection techniques against this type of fraud. *European Financial Systems*, 455-461.

Petar, R. (2023). The rise and fall of cryptocurrencies: Defining the economic and social values of blockchain technologies, assessing the opportunities, and defining the financial and cybersecurity risks of the Metaverse. *Financial Innovation.*

Rajarajan, S. M. (2014). Shoulder surfing resistant virtual keyboard for internet banking. *World Applied Sciences Journal, 31*(7), 1297-1304.

Rajpreet, K. J. (2013). Online banking security flaws: A study. *International Journal of Advanced Research in Computer Science and Software Engineering*, *3*(8), 1016-1021.

Samir, P., & Uke, N. J. (2014). Security in online banking services – A comparative study. *International Journal of Innovative Research in Science, Engineering and Technology*, *3*(10), 16850-16857.

Sbai, H. G. (2018). *A survey of keylogger and screenlogger attacks in the banking sector and countermeasures to them.* In Cyberspace Safety and Security: 10th International Symposium (pp. 18-32).

Suleman, M. S. (n.d.). Combating against potentially harmful mobile apps. In *The International Conference on Artificial Intelligence and Computer Vision*, 154-173.

Utakrit, N. (2012). *Security awareness by online banking users in Western Australian of phishing attacks.* Edith Cowan University.