A Study on Customer Experience on Cybercrime and protection Measures

Authors
Dr. Dhananjaya and Dr. Manjushree. S

Abstract

The global network of interconnected computer network is termed as internet that connects billions of devices globally using the common internet protocols. The most common crime that is wreaking havoc in modern world is cybercrime. With the rapid adoption of digital technology, the scale and sophistication of cyber-attacks have increases dramatically. Digitization and remote operations lead to increased vulnerabilities and open up opportunities for cyber criminals, exposing bank to breaches or hacking. The present study focuses on the experiences of cybercrime, types of cyber fraud in banking transaction, hardship faced by cyber victims and techniques to avoid most of the banking fraud.

Keywords: Digitization, Cyber security, Cybercrime etc.

1.1. Introduction

With the rapid adoption of digital technology, the scale and sophistication of cyber-attacks have increases dramatically. Cybercrime are a global menace to individuals, Governments and organization. Billions of people worldwide are victims of cybercrime. It refers to the use of a computer to advance illicit activities like fraud the trafficking of child pornographic material and other intellectual property identity theft privacy invasion etc. It entails spreading viruses downloading files unlawfully, engaging in phishing schemes, and stealing personal data like bank account numbers etc. thus, a crime can be identified as a "cybercrime". The majority of cyber-attacks fall under the category of cyber-attacks of "economic crimes", which are typically carried out by highly organized criminals and employ the most cutting-edge technologies.

The number of cases of financial fraud has risen along with the rate of innovation. Different methods are being used by cyber criminals to gather bank have employed a number of specific procedures to protect against these frauds, yet the problem persists. This is explained by the fact that the security measures currently available through banks are also available in public or in other places where they can simply breach security measures.

Banking sector has suffered an impact of cybercrimes. RBI has defined bank fraud has as "A deliberate act of omission or commission by any person. Carried out in the course of a banking transaction or in the course of a banking transaction or in the books of accounts maintained manually or under computer system in banks, resulting into wrongful gain to any person for a temporary period or otherwise, with or without any monetary loss to the bank."

1.2 Review of literature

S. Chandra sekhar, (2023). "An overview of cyber security in digital banking sector". In this study the authors opinioned that 21st century the online technology as updated with high performance. In top five the digital banking sectors is also online technology. Constantly such as NEFT Google pay, phone pay, etc. Online banking, but still the cybercrime in the banking sector. As reported to ATM, debit card and net banking. Banking sector is facing cyber-attacks more times compared to other sectors.

Dr. S. Nagaraju (2022), "A Research study on cyber security issues affecting online banking and online transactions in India". On 8 November 2016, the Government of India announced the demonetization in India. That time public is huge consuming online transactions, as well they are suffered with cybercrimes, cybercrime accused is entering into unauthorized way and hacking the data and personal information, here some important methods are suggested to get protection from cyber-attacks.

1.3. Objectives of the study

1. To know the customer's perception and experience on cybercrime in the study area.
2. To analyse the nature of cybercrimes affected by the customers.
3. To assess the satisfaction of customers towards adoption of cyber security in India.

1.4 Statement of the Problem

In the digital age, the use of online banking services has become increasingly prevalent, and with this comes the significant risk of cyber threats and attacks. While banking institutions have implemented security measures to protect their systems, customers themselves must also play an active role in safeguarding their personal and financial information. However, not all banking customers have the necessary knowledge and skills to identify and respond appropriately to cyber threats. This lack of cyber literacy among banking customers poses a significant problem, potentially leading to financial losses, identity theft, and other negative consequences. Therefore, the study aims to explore the significance of cyber literacy among banking customers and identify potential avenues for improving cyber literacy among this population.

1.5 Scope of the Study

The scope of the study would be to provide insight into the current state of cyber literacy among banking customers and to identify areas of improvement regarding the cyber security awareness programs provided by banks. The findings of the study would be used to develop recommendations for banks to enhance their cyber security awareness programs, improve customer trust and confidence, and mitigate the impact of cyber-attacks on customers.

1.6 Research Methodology

The present study is carried out to make intensive enquiry on various cybercrimes in banking sector the information for the present study is being collected through primary and secondary sources. **Primary data:** For the present study the primary data has been collected from account holders of various banks who are respondents to this study. The data has been collected by using a well-structured questionnaire with the help of interview technique.

Secondary data: For the present study secondary data has been collected from various secondary sources like, articles, journals, books, newspaper, websites, etc.

Sample size

For the present study sample size is 50 respondents who are bank account holders and this sample has been selected by using a simple random sampling technique.

1.7 Limitations of the study

The major limitations of the study are as under:

1. The number of respondents is only 50.So it is difficult to generalize the conclusion.
2. The findings of suggestions is based on the information given by respondent which might be biased.

1.8. Results and Discussion

Table 1: Shows Socio-Economic Profile and Opinion of the Respondents

Particular	No. of Respondents	Percentage (%)
Age (Years)		
Less than 30 years	15	30
30-40	07	14
40-50	18	36
Above 50 years	10	20
Total	**50**	**100**
Gender		
Male	41	82
Female	9	18
Total	**50**	**100**
Educational qualification		
Upto SSLC	10	20
PUC	11	22
Graduate	15	30
Post graduate	7	14
Technical Education	7	14
Total	**50**	**100**
Types of Bank Account		
Savings A/c	42	84
Current Account	4	8
Both	4	8
Total	**50**	**100**
Usage of Online Banking Services		
Always	4	8
Sometimes	8	16
Occasionally	25	50
Rarely	9	18
Never	4	8
Total	**50**	**100**
Frequency of changing Passwords		
Every 1-3 months	5	10
Every 4-6 months	2	4
Every 6-7 months	17	34

Rarely or never change	26	52
Total	**50**	**100**
Frequency of Checking Unauthorized banking information		
Every day	7	14
Every Few days	16	32
Once in a week	6	12
Once in a month	21	42
Total	**50**	**100**
Action taken to protecting personal and financial information		
Used Multi-factor authentication	6	12
Updated password regulators	6	12
Installed Anti-virus system	4	8
Used A VPN	8	16
No Action taken	16	32
Others	10	20
Total	**50**	**100**
Measures taken to protecting banking information		
Use antivirus software	8	16
Avoid Public Wi-fi	7	14
Use strong image password	5	10
Regulatory monitor bank A/c	2	4
Total	**50**	**100**
Types of Cybercrime faced by customer		
Phishing	5	10
Software Attack	3	6
Account Takeover	15	30
DPOS attack	15	30
Others	12	24
Total	**50**	**100**
Banks cyber security concern are helpful		
Very Helpful	**11**	**22**
Somewhat what help	**9**	**18**
Not very helpful	**10**	**20**
Not at all helpful	**20**	**40**
Total	**50**	**100**
Rating about bank communication about online security and fraud prevention		
Excellent	**11**	**22**
Good	**6**	**12**
Average	**15**	**30**
Poor	**8**	**16**
Very poor	**10**	**20**
Total	**50**	**100**
Changes in PIN/UPI		
Once in a quarter	**21**	**42**
Never changed	**23**	**46**
Only prompted by bank	**5**	**10**
Others.	**1**	**2**
Total	**50**	**100**

- **Sources: Field Survey**

It is understood most of the respondent belong to the age group of 40- 50 years. Majority of the respondents selected for this study are male. Majority of the respondents are having graduation level of educational

qualification. Shows the 84% respondents are savings a/c holders and 8% respondents are having current a/c and remaining 8% are having both a/c. The study reveals that 52% of respondents are change online banking passwords every 7-12 months. The study reveals that 44% of respondents say bank offers a wide range of financial products and services is neutral. It clears that 42% of respondents are check their bank account once a month for any unauthorized transaction. The study reveals that 32% of respondents are no steps taken to protect personal and financial information. It clears that 34% of the respondents are concerned about cybercrime when it comes to banking information. The majority of 30% of the respondents DDOS attacks of cybercrime concern most for banking information. The majority of 40% of respondents are not helpful find banks customer service in dealing with cyber security concerns. The majority of 24% respondents are dissatisfied the communication and resolution of the issue. Majority of the respondents never changed their PIN or Passwords.

Table 2: Showing the Testing of Hypothesis of Cyber security and satisfaction level.

Null Hypothesis (H_0): There is no association between Cyber security experience and Customer satisfaction level.

Alternative Hypothesis (H_1): There is an association between Cyber security experience and Customer satisfaction level

Experience with cyber security	**Positive**	**Neutral**	**Negative**	**Total**
Yes	15	5	5	25
No	10	8	7	25
Total	25	13	12	50

Sources: Field Survey

Result of Analysis: The Chi-square test statistical value is **2.026** which is less than the table value of **5.99 at 5%** level of significance for the degree of freedom is 2. So there is no significant association with cyber security and their satisfaction level**. Therefore null hypothesis is rejected.**

Table 3: Showing the Testing of Hypothesis of Cyber security and AI based security tools

Null Hypothesis (H_0): There is no significant association between customer's experience with AI based cyber security tools and their satisfaction.

Alternative Hypothesis (H_1): There is a significant association between customer's experience with AI based cyber security tools and their satisfaction

AI Use satisfaction level	Used AI- based security	Not use AI based Security	Total
Satisfied	18	7	25
Not Satisfied	12	13	25
Total	30	20	50

Sources: Field Survey

Result of Analysis: The Chi-square test statistical value is **3**.0 which is less than the table value of 3.841 **at 5%** level of significance for the degree of freedom is 1. So there is no significant association between customer's experience with AI based cyber security tools and their satisfaction. **Therefore, null hypothesis is rejected.**

1.9 Suggestions

- **Stay Up-to-Date with Cyber security Best Practices**: Banking customers should regularly update their knowledge of cyber security best practices and stay informed about the latest cyber threats and scams. They should also educate themselves on how to identify phishing and social engineering attacks.
- **Use Secure Wi-Fi Networks:** Customers should avoid conducting sensitive transactions on public Wi-Fi networks and instead opt for secure Wi-Fi networks or their mobile data plan.
- **Choose Two-Factor Authentication**: Two-Factor Authentication is an extra layer of security that requires users to provide an additional form of identification beyond a password. Banking customers should choose two-factor authentication for their accounts as it adds an additional layer of security.
- **Regularly Review Account Activity:** Banking customers should keep an eye on their account transactions regularly to identify any unusual or unauthorized activities. If they notice something odd, they should report it to their bank immediately.
- **Avoid Clicking Unknown Links and Downloading Unknown Files:** Clicking on suspicious links or downloading files from unknown sources can compromise a customer's device. Banking customers should avoid unknown links and only download files from trusted websites and sources.
- **Use Secure Payment Methods**: Online shopping should be done with secure payment methods such as credit cards or e-wallets. These payment methods usually have fraud protections and dispute resolution policies in case of unauthorized transactions.
- **Use Biometric Authentication:** Biometric authentication, such as facial recognition or fingerprint ID, can provide an additional layer of security when accessing banking accounts. This technology makes it harder for cybercriminals to impersonate banking customers and access sensitive data.

Conclusion

In conclusion, banks and financial institutions must prioritize educating their customers on digital safety practices. Cyber literacy among banking customers is crucial in preventing fraudulent transactions, data breaches, and identity theft. By implementing these tips and best practices, banking customers can protect themselves and their personal information while using online banking services. Fostering a culture of cyber hygiene among banking customers can help prevent cybercrime and promote trust in digital financial transactions.

Bibliography

1. Changsok Yoo, Byung-Tak Kang and Huy Kang Kim, (2015) Case study of the vulnerability of OTP implemented in internet banking systems of South Koreal, Multimed Tools Appl, vol. 74, pp. 3289- 3303.
2. Mr. Shakir Shaik and Dr. S.A. Sameera, *(2014) "Security Issues in E-banking Services in Indian Scenario", Asian Journal of Management Sciences 02 (03 (Special Issue)),pp 28-30.
3. Dr. Devaraju etal., (2016) International Journal of Advance Research in Computer Science and Management Studies Volume 4, Issue 11, Pg. 114-1202016, IJARCSMS All
4. 24 Aparna Desikan, (2016) Mobiles making India less cash conscious, Times of India, 22nd February, 2016, pg 1. Volume 3, May "ISSN 2455-2488" "Udgam Vigyati" - The Origin of
5. McCullagh, A., & Caelli, W. (2005). Who goes there? Internet banking: A matter of risk and reward. Paper presented at the Information Security and Privacy.
6. Reddy. G.N, (2009), "IT- Based Banking Services Enhancing Efficiency", Financial Analyst, November.p.69
7. Alaganandam, H., Mittal, P., Singh, A., & Fleizach, C. (2007). Cybercriminal Activity.
8. Bhasin M (2007). "Mitigating Cyber Threats to Banking Industry". The Chartered Accountant, April 2007, p.1622-1623
9. Claessens, J., Dem, V., De Cock, D., Preneel, B., & Vandewalle, J. (2002). On the security of today s online cyber banking systems, Computers & Security, 213: 253-265.
10. M Sravika, (2022) A Study on Cyber Security Issue Affecting Banking and Online Transactions, Sridevi Women's Engineering College.