Social Engineering Attacks on Mobile Banking System in Bangladesh

By

N H M Ahsanul Gani Faysal

ID 171-35-220

This report presented in partial fulfillment of the requirement for the degree of Bachelor of Science in Software Engineering.

Supervised By

SK. Fazlee Rabby
Lecturer
Department of SWE
Daffodil International University

DAFFODIL INTERNATIONAL UNIVERSITY

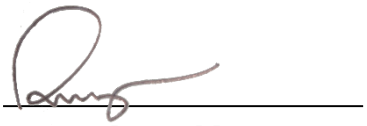
DHAKA, BANGLADESH

JUNE 2021

APPROVAL

This Thesis titled “Social Engineering Attacks on Mobile Banking System in Bangladesh”, submitted by N H M Ahsanul Gani Faysal, ID: 171-35-220 to the Department of Software Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of B.Sc. in Software Engineering (SWE). The presentation has been hold on June 2021 and approved as to its style and contents.

Supervised by:



SK. Fazlee Rabby
Lecturer
Department of SWE
Daffodil International University

THESIS DECLARATION

I hereby declare that this report has been completed by me under the supervision of Mr. Sk. Fazlee Rabby, Lecturer, Daffodil International University Department of Software Engineering. I also declare that neither this study nor any component of it has been submitted elsewhere for award of any degree.

Supervised by:

SK. Fazlee Rabby
Lecturer
Department of SWE
Daffodil International University

Submitted by:

N H M Ahsanul Gani Faysal
ID: 171-35-220
Department of SWE
Daffodil International University

ACKNOWLEDGEMENT

I would like to express our gratitude to my honorable supervisor, SK. Fazlee Rabby, Lecturer, Department of Software Engineering. This thesis would not have been completed without his support and guidance. He supervised me on every step. He motivated me to learn new things, provided all the important files and information and taught me how to make the work done. I express my heartiest gratitude towards the entire department of Software Engineering at Daffodil International University for providing good education and knowledge. I also express my gratitude to all my teacher's SAM Matiur Rahman, Associate Professor; Dr. Imran Mahmud, Professor, and Head, Dept. of Software Engineering. The knowledge that I have learned from the classes in my degree of bachelor's in software engineering level was essential for this thesis. In course of conducting the study, the necessary information was collected through books, journals, electronic media, and other secondary sources. I also want to thank my friends for providing me support and encouragement. Their optimism and encouragement have allowed overcoming any obstacle at any phase.

DEDICATION

I would like to express my gratitude to my honorable supervisor, SK. Fazlee Rabby, Lecturer, Department of Software Engineering. This thesis would not have been completed without his support and guidance. He helped me a lot to complete this thesis. So I would like to dedicate this to him (SK. Fazlee Rabby).

ABSTRACT

Mobile Banking is a service provided by a bank or other financial institution that allows its customers to conduct financial transactions remotely using a mobile device such as a smartphone or tablet. As the service is easy to use the number of transactions is increasing drastically. Although the number of mobile banking users is increasing day by day, it is seen that the rate of mobile banking fraud is not decreasing and the reason behind this is that users have less idea and unawareness about fraud. Based on this unawareness of mobile banking users, the attackers have been committing fraud. M-banking users are often the victims of mobile banking frauds and most of the users are suffering financial loss. The attackers are conducting mobile banking fraud and they are committing this fraud by making fake phone calls, sending fake messages to the users and such frauds are included into social engineering attacks. The primary intent of this research is to find out the reasons behind the increasing number of mobile banking frauds and also to find out which kind of attack on mobile banking fraud is increasing along with which types of people are most vulnerable behind this attack. This research will help the authorities to take effective steps to reduce the rate of mobile banking fraud in the future.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATION

M-banking = Mobile banking.

HAPTER 01
INTRODUCTION

Considering the history of mobile banking in the context of Bangladesh, it's a kind of new technology. City bank was the first bank to give the idea about mobile banking first in 2009 by introduced mobile banking software named 'city wallet and its full and this technology fully started its functional journey on March 31, 2011. Dutch Bangla Bank Limited initiated the concept of mobile banking services(MBS) in Bangladesh. Before that mobile financial services like foreign remittance, using m-wallets for cash in/out was approved by central bank. BRAC Bank limited entered into this industry as the 2nd bank. Then all other banks Followed their examples. (Global Mobile Banking Market Research Report, 2021)

The whole concept of mobile banking is an advanced online system provide on the latest mobile phone where clients are offered dynamic banking services. With the advancement of the internet becoming the advanced trend for the latest technology users, mobile banking no doubt has become the most important and popular technology for young users and this issue is growing day by day. The clients are no longer needed to visit local banks for daily undergoing banking transactions. Advance mobile banking gives clients a significant moment to provision to bank from wherever on every side the world at any time as per their satisfaction. The universal mobile banking industry in the market is grabbing new confront and the latest imagination so that it could be able to drive and meet consumer's projections and pleasure.

In Bangladesh, every month transaction via Mobile Banking Service increasing by the rate of 20%. About 25 banks already has the approval of the central bank to operate Mobile Banking services. The rule of banking and other financial services like cash-in/out merchant payment, utility bills payment, payment of salaries, foreign remittance handling, disbursement of money to the beneficiaries of government allowances and other financial supports are under the operational zone of Mobile Banking. (Barua, 2016)

Worldwide mobile banking market analysis shows that users subscription to the whole market is huge. The COVID-19 pandemic has extremely impacted the mobile banking market share over the world and for that situation people are making transaction a lot on online to keep away visiting the bank branch.

Statistics from the central bank, around 36.22 million registered mobile banking customers in Bangladesh served by 0.6 million agents. On average, 4.2 million transactions taking places through m-banking every day and valued around Tk 7.71 billion which means the users of mobile banking services is increasing day by day. Significantly, the problem is mobile banking fraud. An increase in the number of users and the rate of transactions are the reason behind the mobile banking fraud. (Raihan, Apr 18, 2012)

In stipulations of mobile banking services in Bangladesh it can be seen that even after the rise of mobile banking fraud the amount of work done in this sector is insufficient and so far the authority has not taken any significant steps and So we are interested in working on this.

Since no effective steps have been taken despite the rise in mobile banking fraud. From This research discussion it will be easy to take effective steps by the authority to reduce the risk of fraud.

CHAPTER 02
LITERATURE REVIEW

Every system has some flaws similarly there are some flaws in the mobile banking system. In Bangladesh the number of mobile banking users in increasing day by day as well transactions are increasing due to the increase in the number of users. Although there have been numerous cases of mobile banking fraud, only a few number of cases have come to our notice. As a result, the causes of fraud remain elusive. Some opportunists are exploiting the flaws of the mobile banking system and stealing a large amount of money through banking fraud. As a result of the authority not taking any effective steps, it is not possible to find out the cause of fraud as well the group of vulnerable people . (Islam, 2013)

Bangladesh has become very popular in terms of using mobile banking system. Mobile banking services are very easy to use. It is very popular with everyone because of the ease of opening new accounts and transactions. Due to the ease of money transactions it is very effective for those people who live in rural areas. The mobile banking is as easy to use as it is risky as well it is from this risk that mobile banking fraud occurs. Bkash is popular than any other m-banking system in Bangladesh. A study shows that to reduce the m-banking fraud the authority of bkash work in four steps. By working on this four steps the authority of bkash have been able to figure out that how their m-banking platform is being misused by many attackers. They have also been able to figure that out why the number of victim of this m-banking fraud is increasing. Less educated person and who does not have better understanding about mobile banking fraud are the most vulnerable and the people does not get aware of the risk until they get affected by the fraud . (Shahrin, Fraud risk management of bKash Limited, 2018)

Since the launch of the mobile banking service, the number of users has been steadily increasing and its popularity been on the rise. Mobile banking fraud has started since the popularity of mobile banking services. The attackers make fake phone calls, sending fake SMS to the user to get their fraudulent done. There are two types of mobile financial fraud. Those are user driven fraud and agent driven fraud. Attacker appears as a fake customer in this user driven fraud. This fake customer mainly targets other customer, agents and mobile financial service providers to make his fraudulent done. Agent driven fraud is more threatful because of this fraud starts off and utilizes by m-banking services own agent and employees and this agent driven fraud makes it very difficult to know the cause of mobile banking fraud so that m-banking fraud is on the rise. (Shahrin, Fraud Risk Management of bKash Limited, Sep 7, 2018)

Fraud in mobile banking continues unabated and for that reason the attackers using their old strategy to extort money. By taking advantages of the widespread use of mobile banking, the scammers continue to harm consumers financially. Those who are less educated and have little knowledge about this m-banking technology are the victims of mobile banking fraud. A study shows that the fraudulent mainly targets the bkash and rocket users to cause fraud as well inflict financial loss on them. A study also shows that bkash and rocket bank officials do not want to take any liability for the fraud. The bank authority continuously making the users aware through advertisement in tv, radio but even after that m-banking fraud continues because this

awareness advertisement does not reach to everyone and the scammers continue to conduct m-banking fraud by taking advantage of the fact that awareness ads does not reach everyone. (Ullah, 14 March, 2019)

Fraudulent cycle is mainly divided into four groups and carry out fraudulent activities. The first group took a stand at the field level. They took a picture of the transactional development book and sent it to the second group on WhatsApp, mentioning the area and in this way the attackers continue to commit fraud without any sign that the sign will help the bank authority to identify the scammer. (Fraud in mobile banking transactions is on the rise, 2020)

Mobile banking services are popular all over the world as well m-banking fraud is not only a national issue but also a global issue. A report shows that in UK has the policy that if a consumer suffers financial loss through m-banking fraud and if it is proved, the authority will compensate his/ her for the loss. To reduce the risk of online banking fraud the UK online banking authority called for a nationwide campaign to raise awareness about fraudulent crimes. As a result of this campaign, the rate of online banking fraud in UK was significantly reduced to 21%. (Peachey, 2015)

With the increase of mobile banking and online banking, financial fraud has also increased in the system. In India a survey on financial fraud in the financial sector by Assocham and PwC found that financial fraud is causing about 20 billion dollars in financial losses every year. Young people are using more and more online banking as smartphone are increasing day by day and as a result banks are becoming more interested in getting a large share of customers "digital wallet". Attackers are exploiting the interest of banks to get a bigger share of "digital wallet" from their consumers by increasing the number of fake bank officials. Therefore, vulnerable risk like phishing, identity theft, card skimming is increasing drastically. A report shows in India till now the most common type of fraud in the banking sector is identity theft. Bank officials in India says that to secure transactions via mobile phone or a two –factor authentication is needed. (Reporter, July 10, 2015)

Information technology has always played an important role in mobile banking or online banking. The banking sector has completely changed since the advent of internet mainly in terms of security and for that because now money is coming into user's hand in a click. Banking fraud and cybercrime has also increased due to the simplification on m-banking and online banking system. A report says after Japan and USA India is the most affected country by online banking malware. The report further shows that increasing the number of smart phones and tablets for online banking have increased the risk of fraud. To reduce the risk of fraud Indian m-banking and online banking authority took some steps such as never ever click on a link, do not share personal bank account information with anyone ever without officials over the phone. (Dr. Manisha M. More, 2016)

Social engineering (not a new paradigm) has steadily grown with no-end-in-sight. Its continued growth borders on human nature of trust instincts, on which hackers manipulate human emotion and ultimately, exploit this trust to steal valuable information. Common technique for

achieving this feat are: phishing, vishing, smishing etc. – with the most popular being phishing. (Andrew Eboka, 2016)

Nowadays the use of technology is often carried out on mobile devices and the development of both mobile and online technologies has been a notable solution for the banking sector to expel the tiring and time-consuming of the typical system that creates difficulty for the users. With the rapid development of the technology, the banking sector uses technology to provide convenience and speed for its users. Therefore, the development of mobile and online banking continues with the same acceleration as the development of technology. Financial companies had to undertake a challenging task with the convenience offerings to their users like providing their information and data security. (Nilay Yildirim, 2019)

CHAPTER 03
RESEARCH METHODOLOGY

A descriptive research design is adopted for this study. This kind of research includes surveys and facts discovering inquiries of different kinds. Since mobile banking fraud is increasing every day and this problem hasn't received a good deal of research so far. At this point, this kind of research is very necessary. Two methods can be used for descriptive research: survey and observation.

3.1 Data Collection

A survey method was used to collect primary data for this study through a structured questionnaire. The questionnaire was designed in close collaboration with the supervisor and checked by experts from bKash. Almost one thousand primary data were collected through this survey which includes different kinds of people. Since the beginning of mobile banking fraud no effective steps has been taken to reduce the risk. Therefore, due to not taking any effective steps, the opportunity of mobile banking fraud remains. This research has tried to find out the reasons for mobile banking fraud and point out the group of vulnerable people by analyzing the collected data through a survey.

3.2 Data Pre-processing

After collecting the data through a survey it was needed to pre-process. There were many categories of data in this data set and because there were so many categories there was missing value too. To fix the missing values which were from categorical columns we have replaced those missing values with the most frequent category.

3.3 Data visualization

Almost all the values were in categorical form and all of them were not equally important for this research outcome. The dataset was pushed through a feature importance algorithm to find out the most important features. We could use correlation coefficient instead of feature importance to find out the most important features but correlation coefficient does not provide a sufficient output for categorical data and that is why we choose this feature importance algorithm. Before pushing the data through the feature importance algorithm encoding was done because maximum was in string form. One-hot encoding and Label encoding were used to encode the data. To visualize the data some python libraries were used like matplotlib, pandas, and NumPy. The most important features were put together and compared to find out the result.

CHAPTER 04
RESULT AND DISCUSSION

4.1 Data visualization result

Table: 01: Feature score

Feature name	Feature importance score
Age	0.010828
Gender	0.004525
Education qualification	0.011316
occupation	0.008384
district	0.008598
How long have you been using mobile banking services?	0.009671
ever been a victim of mobile banking fraud?	0.279949
How did you get cheated?	0.601913
have you suffered any financial loss?	0.033549
aware of mobile banking fraud before deceived?	0.019216
Have you seen any awareness ads on tv	0.000826
How good are you at using the internet?	0.009454

The term mobile banking is known to 94% of people and 55% of them think they should use mobile banking and others don't find this system necessary. In the present world, everyone is busy with their job. They don't have much time to visit the bank for any transaction. Since banks have to agree with their clients and save their valuable time, they introduce such services as mobile banking which can make the customers carefree or well pleased.

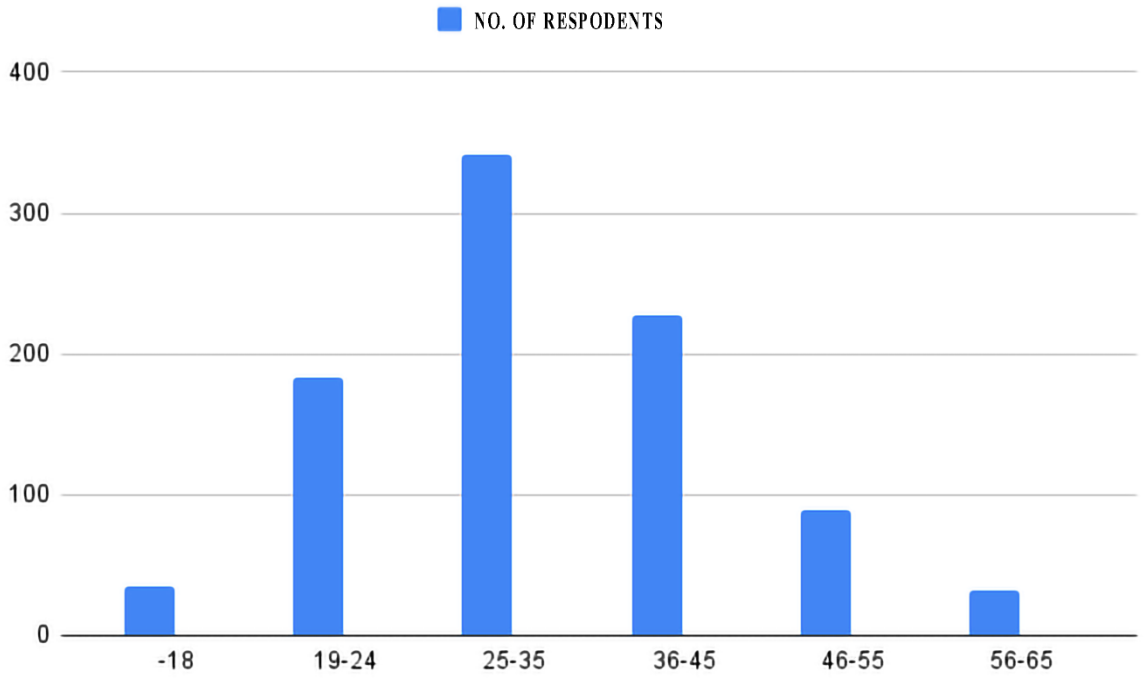


Fig 01: Age range vs no. of respondent

Figure -01 contains some age ranges which were collected through the survey. The highest response was received from the age range 25-35. The main content of this survey was about mobile banking fraud. Figure -01 shows that the age range of 25-35 is more interested in this subject. Then, through more documentaries, it will be possible to understand who was attacked and where the deficit was.

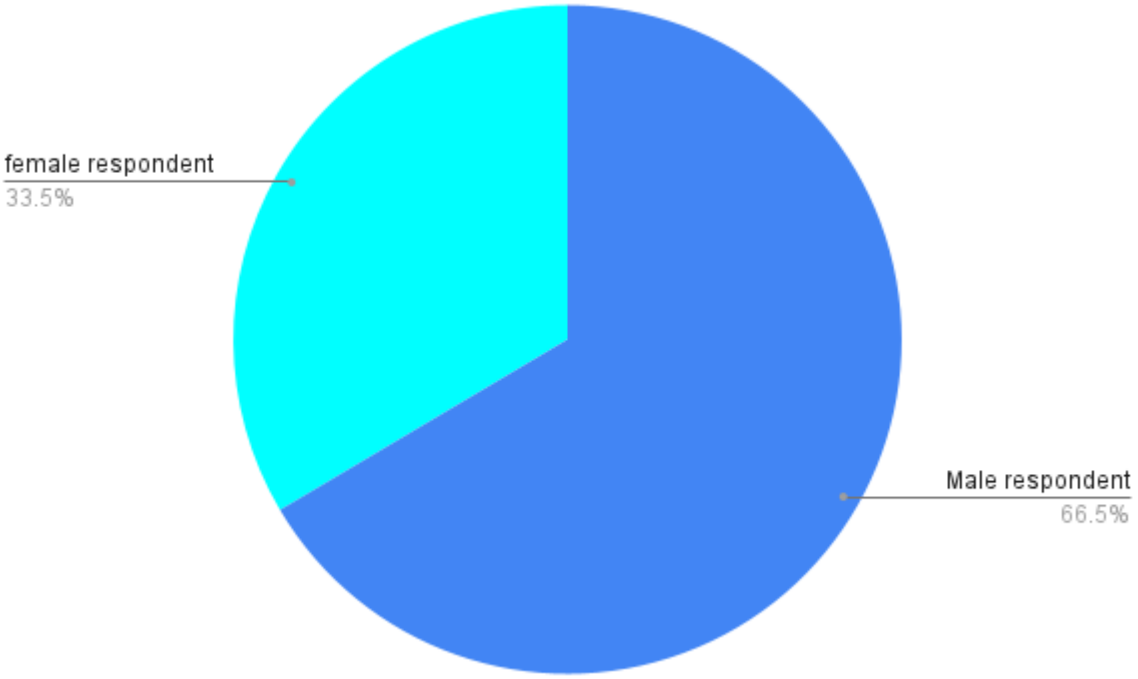


Fig 02: No. of male/ female respondent

Figure -02, from total respondents, 33.5% of respondents were female and 66.5% of respondents were male. From the diagram, it is clear that the male respondent was more than double the female respondent. This diagram contains not a lot of information inside it but it is important when it comes to calculating the number of attacks on men and women.

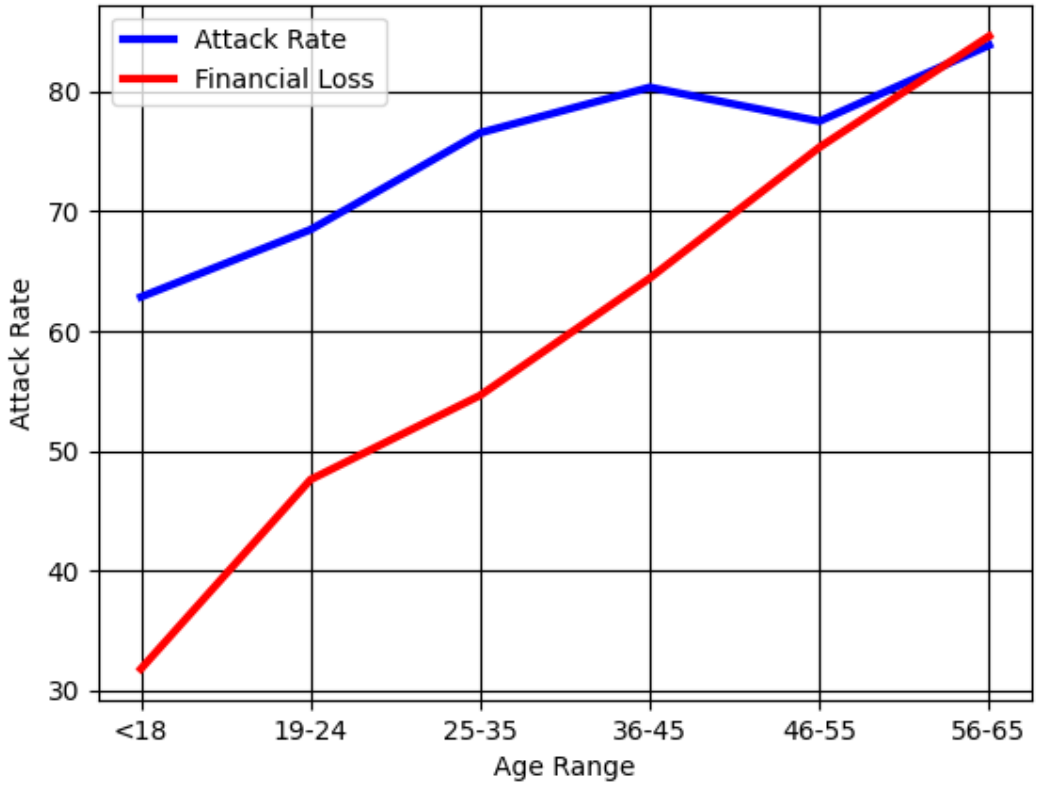


Fig 03: Age range vs attack rate vs financial loss

Figure -03 points out 3 things. Those are Age Range, Attack Rate, and Financial Loss (From all the attacked cases which have faced a loss of money). These three features are so important for this discussion. The outcome of figure one is-

Age range	% of respondents
>=18	3.86
19-24	20.18
25-35	37.60
36-45	25.03
46-55	9.81
56-65	3.53

Table 02: Age range with percentage of respondent

People around 18 years of age range was only 3.86% respondent and though attack rate was almost 70% and financial loss for this age range was below 35%. The 19-24 age range was 20.18% of total respondents where the attack rate was 70% and financial loss was almost 50%. The response in the 25 to 35 age range is 37.60% and the attack rate for this age range is almost 80% and financial loss for this age range is also above 50% a large amount. The response in the 36-45 age range is 25.03%, the attack rate for this age range is above 80% and the financial loss is above 60%, another large amount. The response in the 46-55 age range is 9.81%, attack rate and financial loss for this age range is almost the same 70% to 78%. The last age range is 56-65, the response of this age range is low around 3.53%. The attack rate and the financial loss for this age range is maximum which is about 86% to 87%.

From the analysis of figure -03 and table -01, it is clear that considering the age people between the ages of 56 to 65 have the lowest response but the attack rate and the financial loss for this group is maximum.

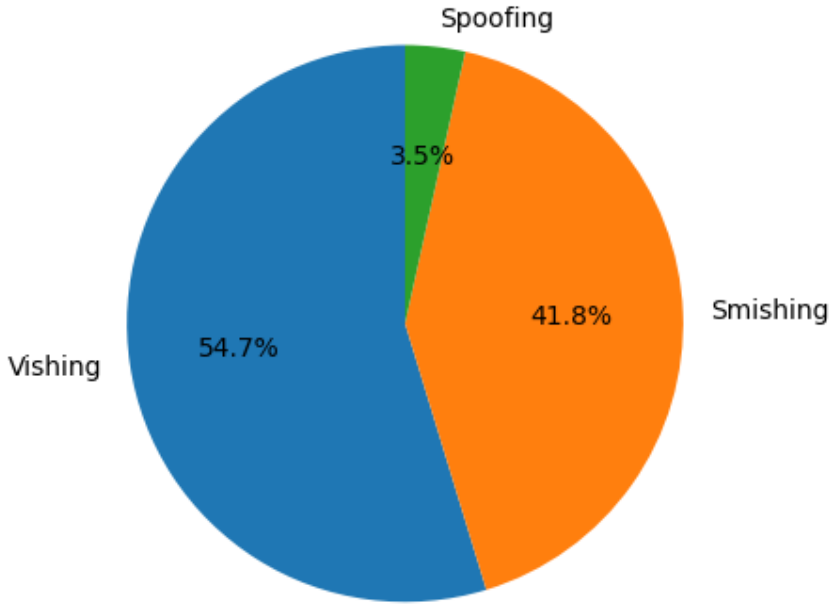


Fig 04: Attack type

Figure -04 reveals the type of attack. Vishing attacks are basically what happens through voice calls. Another one is smishing attacks which basically happen through SMS (via phone). One more is spoofing attacks, it could be through IP spoofing or email spoofing. From the above figure, it is highlighted that from the total respondent 54.7% faced vishing, 41.8% faced smishing and a small amount of 3.5% has fallen victim to spoofing.

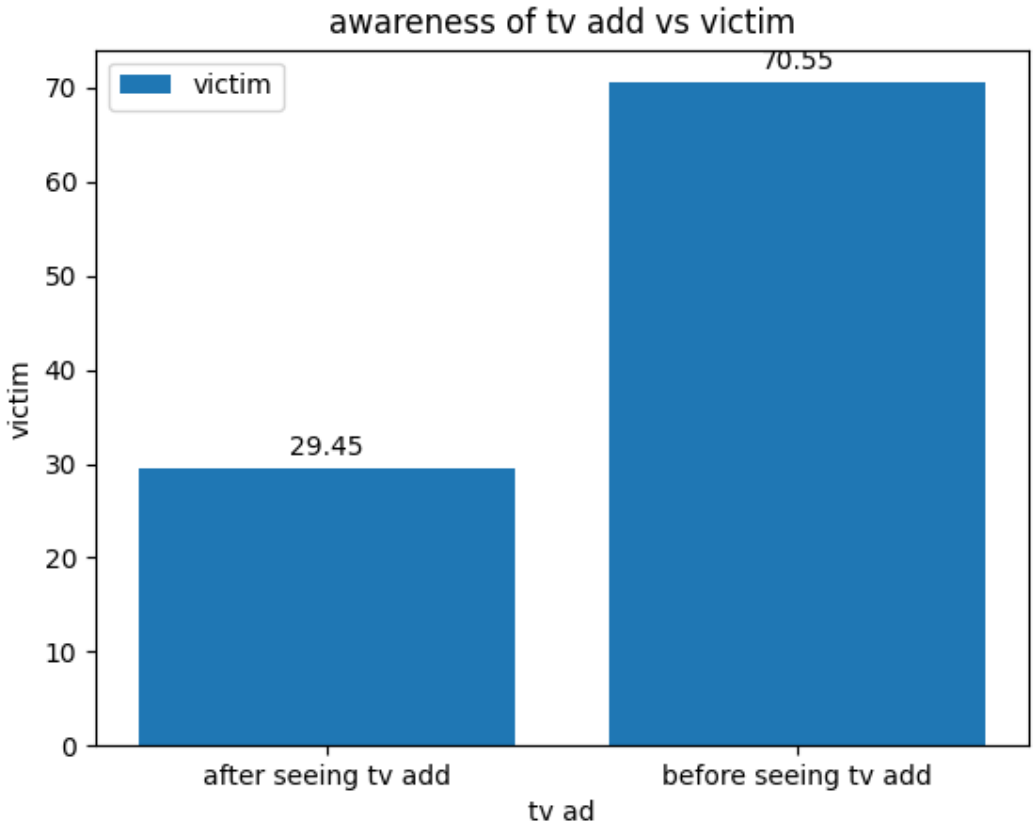


Fig 05: Awareness of tv. advertisement vs victim

Figure -05 shows how much the respondents were aware before watching the advertisement on television compared to what they were aware of after watching the advertisement on tv. The figure shows almost 29.45% of respondents were attacked even after watching the awareness advertisement on television and 70.55% of respondents were attacked before watching the awareness advertisement on television.

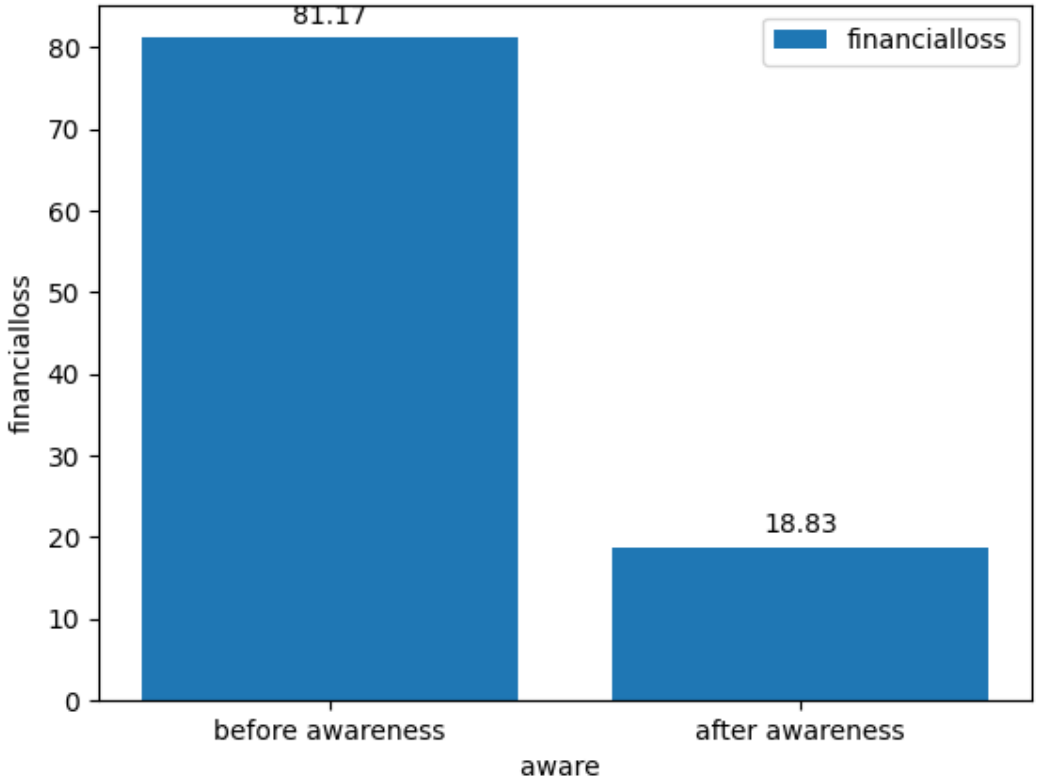


Fig 06: Aware of fraud vs financial loss

Figure -06 basically shows the percentage of respondents who have suffered financial losses after being aware of mobile banking fraud and the percentage of respondents who have suffered before being aware of mobile banking fraud. This figure shows that 81.17% of respondents have suffered financial loss before being aware and 18.83% of respondents have suffered financial loss even after being aware.

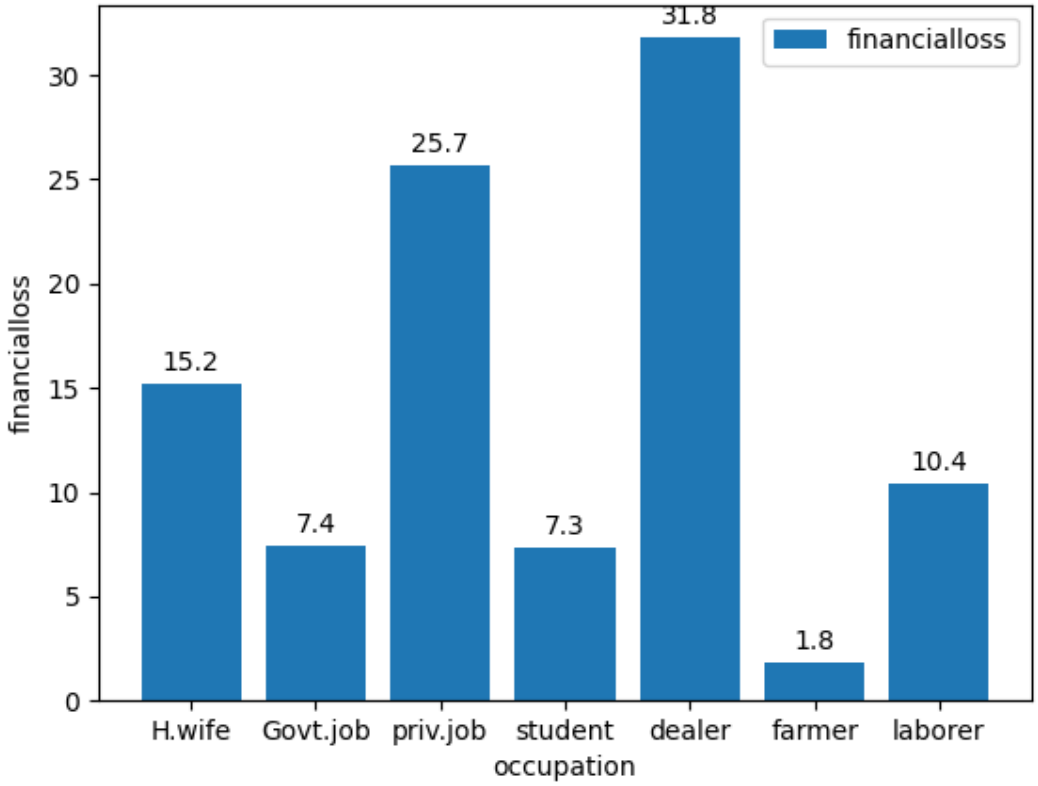


Fig 07: Occupation vs financial loss

Figure -07 shows the percent of people depending on occupation who have faced financial losses. From total respondents, a housewife was 15.2%, a government employee was 7.4%, a private job holder was 25.7%, a student was 7.3%, a businessman was 31.8%, a farmer was 1.8% and laborer was 10.4%.

4.2 Discussion

After analyzing all the above figures, some things can be reached. From the analysis of figure -03, several things can arrive, a vulnerable group of people can be pointed out. This can be done by considering the age range and the victim. The age range between 56 to 65 is most vulnerable in this case. Because the financial loss they have suffered corresponding to the amount they are being attacked was maximum among all. On the other hand, people in the 25 to 35 age range are in the third position in terms of attack rate which was quite unexpected, because young people are more aware than the older ones. Despite being aware they were victims so they were also included in the list of vulnerable groups of people. The authority has introduced some awareness advertisements on television to reduce mobile banking fraud. Many have survived the attacks after watching the awareness advertisement on television and many have been attacked. Nevertheless, those who didn't watch the awareness advertisement on tv are more likely to be infected. This means that those who didn't watch awareness advertisements on tv are more vulnerable than those who watch awareness advertisements on tv. Work can be done on how to increase the tendency of people to watch awareness advertisements on tv. Traders are risky because money transactions are a daily incident for their business so they also fall under the category of vulnerable people. From the outcomes, it can be said that people of different professions, different ages who didn't watch the awareness ads on tv are basically vulnerable people.

CHAPTER 05
RECOMMENDTAION AND CONCLUSION

5.1 Recommendation

The survey and the findings from those data analyses recommend some points to reduce mobile banking fraud. These recommendations may grow awareness and reduce further risks.

1. In the case of mobile banking, replying to an unknown text message which is from an unauthentic source must be prohibited. Authorities must make people aware not to respond to these kinds of messages.

2. Personal secret PIN, OTP, password, or any sensitive information about a personal account cannot be shared. This problem should be taken care of by the authorities through awareness growing programs.

3. One very constructive approach for fraud observation is to inform clients in real-time while there has been unusual activity related to their accounts. For example, if an electronic payment is made to a new payee the bank can inform the clients by text or phone call for confirmation that the transaction is authorized. This procedure may reduce mobile banking fraud.

4. User guidance should be provided to all the customers.

5. Rules and regulations must be stricken in mobile banking.

6. The authorities can arrange a training program to raise awareness among the masses about mobile banking fraud.

7. Banks may provide better training to recipients and representatives through a campaign.

5.2 Conclusion

The mobile banking system is a rapidly growing sector in Bangladesh and it is becoming very popular day by day and also the number of customers is increasing every day. Since mobile banking and mobile banking fraud are increasingly corresponding to each other it is high time to mitigate further risks. Moreover, mobile banking is only well-known for its mobile airtime service, even though it has various multidimensional uses. From this research perspective, mobile banking is a more noteworthy business than others in Bangladesh. The research has shown how hackers or attackers are taking new faces every time and for that reason, it has become very hard to track them (attackers) down. A lot of people are falling into the trap of these kinds of attackers consciously or subconsciously. It is unfortunate that till now the authorities have not taken any effective steps. If mobile banking fraud happens continuously then such a time will appear that the authority will fail to control the risk of fraud and fail to track the attacker's new move. This research shows that mitigation of risk is possible but 100% mitigation is quite unthinkable. Therefore, the authorities must take the right decision at the right time to track down them (attackers) and to lower down the risk of fraud. This research prefers to mitigate the risk by increasing awareness and creating knowledge through training, campaign, and advertisement among users, agents, etc. In Bangladesh, very few works have been done on social engineering attacks on the mobile banking system. To get this research done we took help from some similar works. There is a huge scope to do research in this field. It is high time the authority takes the right decisions and saves the future of the mobile banking system of Bangladesh.

REFERENCES

(n.d.).

Andrew Eboka, A. A. (2016). Social Engineering Detection Model for the Mobile Smartphone Clients. *ResearchGate*(2016).

Barua, A. (2016). *Present Conditon of mobile banking in bangladesh.* San Francisco, California, USA: Academia.

Dr. Manisha M. More, M. P. (2016). Online Banking and Cyber Attacks: The Current Scenario. *ResearchGate*(2016).

Fraud in mobile banking transactions is on the rise. (2020). *Banking news*(2020).

(2021). *Global Mobile Banking Market Research Report.* India: Market Research Future.

Islam, P. (2013). Mobile banking fraud. *The Daily Star*(2013).

Nilay Yildirim, A. V. (2019). A Research on Security Vulnerabilities in Online and Mobile Banking Systems. *IEEE.* Barcelos, Portugal.

Peachey, K. (2015). Online banking fraud 'up by 48%'. *BBC*(2015).

Raihan, F. K. (Apr 18, 2012). *Mobile Banking System in Bangladesh.* San Francisco, California, USA: Scribd, Inc.

Reporter, B. (July 10, 2015). *Cyber frauds on rise with increase in digital banking.* Mumbai : Business Standard Private Ltd.

Shahrin, S. (2018). *Fraud risk management of bKash Limited.* Bangladesh: BRAC University.

Shahrin, S. (Sep 7, 2018). *Fraud Risk Management of bKash Limited.* Bangladesh: BRAC University.

Ullah, A. (14 March, 2019). Mobile banking frauds continue. *Daily Sun*(2019).