Social engineering on Social network in Bangladesh

By

Shoab Mahmud Miad

ID: 171-35-207

This Report Presented in Partial Fulfillment of the Requirements for the Degree of Bachelor of Science in Software Engineering

Supervised By

Ms. Marzia Ahmed
Lecturer
Department of SWE
Daffodil International University

DAFFODIL INTERNATIONAL UNIVERSITY

DHAKA, BANGLADESH

JUNE 2021

APPROVAL

This thesis titled “Social engineering on Social network in Bangladesh”, submitted by Shoab Mahmud Miad, ID: 171-35-207 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).

BOARD OF EXAMENERS

Dr. Imran Mahmud
Associate Professor and Head
Department of Software Engineering — **Chairman**
Faculty of Science and Information Technology
Daffodil International University

Mr. SK. Fazlee Rabby
Lecturer
Department of Software Engineering — **Internal Examiner 1**
Faculty of Science and Information Technology
Daffodil International University

Mr. S A M Matiur Rahman
Associate Professor and Associate Head
Department of Software Engineering — **Internal Examiner 2**
Faculty of Science and Information Technology
Daffodil International University

Dr. Shamim Al Mamun
Associate Professor
Institute of Information Technology — **External**

DECLARATION

I hereby declare that this report has been done by me under the supervision of Ms. Marzia Ahmed, Lecturer, Dept. of Software Engineering, Daffodil International University. I also declare that this report nor any portion of this report has been submitted elsewhere for the award of any degree.

Supervised by:

Date: 29.06.21

Ms. Marzia Ahmed
Lecturer
Department of SWE
Daffodil International University

Submitted by:

Shoab Mahmud Miad
ID: 171-35-207
Department of SWE
Daffodil International University

ACKNOWLEDGEMENT

I would like to express our gratitude to my honourable supervisor, Marzia Ahmed, Lecturer, Department of Software Engineering. This thesis would not have been completed without her support and guidance. She supervised me on every step. She 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.

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATION

SNS = Social Networking Sites

SN = Social Engineer

Abstract

In this age of globalization, social networking sites have brought a revolutionary change in the communication system. Social networking sites (SNS) have made communication faster and easier than before. Social networking sites are some of the most popular sites on the internet. The popularity of SNS is immense. With this popularity, they have also become one of the riskiest sites for users because SNSs contain large amounts of information. Which have made SNSs a hunting ground for social engineers. The social engineers use users' mistakes to manipulate them into traps. This study aims to mitigate the risks of social engineering (SE) attacks. Similarly, in Bangladesh, social engineering attacks on social networking sites in Bangladesh are on the rise. The collected primary data through the survey method was analyzed. The study has identified common SE attacks conducted on Bangladeshi SNS users. The study has found some issues concerning information sharing and the internet privacy of the users. The study has provided suggestions to mitigate risks.

Keywords: Social engineering, Social networks, Online privacy, Information sharing

Chapter 01
INTRODUCTION

Social networks are a kind of web service that establishes virtual connections between people. They allow users to communicate, share data between friends and many more. The use of SNS has brought a revolution in communication. The first modern social networking site (SNS) was Friendtester. It was basically a dating website that was not all about dating. After the launch in just three months, it achieved three million users. This means, at that time about 1 per 126 users were members of this website. [1]

In recent years the social networking system has accumulated so much popularity that it has become part of people's daily life. About 53.6% of the World's population uses social networking sites with 2 hours and 25 minutes of daily average usage. [2] Social networking sites are getting more popular day by day because they not only help to meet new people but are also easy to access. Besides, SNS is helping people in the job market and helping businesses to reach out.

For users, social networking sites can be beneficial because they shrink geographic borders to establish communication. In addition, they can be used for entertainment sources and they can be used in a commercial way to achieve the goal of job and business and education. However, the popularity of SNS comes with high risk. Users share a large amount of personal data in SNS which makes them potential targets for attackers. With the obtained data from the users simply by using SNS, the attackers can carry out various kinds of attacks like spam, malware, identity theft, etc. Moreover, by analyzing the personal data of users the attacker can find significant information such as bank account information and commit cybercrimes. [3]

Social networking sites are a massive goldmine of data this allures social engineers. SNSs provide the social engineers a large volume of targets. These facts have made SNSs a hunting ground for social engineers in which they manipulate users into traps. [4]

Bangladesh is a developing country. Just like any other country Social networking sites are very popular in Bangladesh. This country has a good number of SNS users. In January 20201 there were 45 million SNS users. Between 2020 and 2021 about 25% of SNS users increased in Bangladesh. This shows that SNS is very popular in Bangladesh. With this increasing popularity, the attack rate on Bangladeshi SNS users is increasing. A report shows that SNS penetration in Bangladesh stood at 22% in January 2020. [5] And this cannot be ignored.

The objective of this study is to identify common types of social engineering attacks among vulnerable users and help mitigate the risks of these attacks.

Since SE attacks are on rise on social networking sites and Bangladeshi users are getting affected by these. Essential steps must be taken to mitigate the danger. This study may help concerned groups to help take necessary steps to inform SNS users to mitigate the risk of the attacks.

This paper explores the Literature review in chapter 2 followed by Research methodology in chapter 3, Results and Discussion in chapter 4 lastly Conclusion and Recommendation in chapter 5.

Chapter 02

LITERATURE REVIEW

Social networking sites make communication easier between people by establishing virtual relationships. M. Raggo (2016) has described how some popular social engineering attacks like account hijacking, scams and phishing are being executed on social networking sites. The author has provided brief demonstrations about these social engineering techniques which provides a better understanding of these types of attacks. The literature should be helpful for this study to understand the SE attacks on SNS in Bangladesh. [6]

Weimin Luo, Jingbo Liu, Jing Liu, Chengyu Fan (2009) have provided details about various attacks on social networking sites, attacker's motivations behind these attacks. The authors have provided their analysis regarding these various attack methods and countermeasures of these attacks. This literature provides much vital information regarding attacks on social networking sites and ways to mitigate them which may prove beneficial for this study. [7]

With the increasing popularity, social networking sites are continuously facing various attacks. Shailendra Rathore, Pradip Sharma, Vincenzo Loia, Young-Sik Jeong (2017) in their literature has highlighted various social engineering attacks and other types of attacks, potential threats and ways to countermeasure. They have described how some traditional attack techniques like phishing and malware can be used to obtain valuable information from the user. With this information, the attacker has the potential to launch a large-scale attack. [8]

For this study, the work of N. A. G. Arachchilage, Steve Love (2014) can provide valuable information regarding awareness of phishing attacks. Their work displayed much valuable information about phishing methods and their threats. They have also worked for security education. [4]

Social networking sites are a great medium for information sharing but they can be dangerous sometimes. Nurul Nuha Abdul Molok, Shanton Chang, Atif Ahmad (2012) has provided great knowledge about information sharing and phishing attacks on SNS. They how information sharing can be dangerous for people and makes the job for social engineers easier. They have displayed that even a simple post on the SNS bears the risk of information leakage and it helps the SE attacker to launch a devastating attack. [9]

Social networks encourage people to share information it attracts people more as people always have the habit of sharing information. Heidi Wilcox, Maumita Bhattacharya (2015) has drawn special attention to information sharing and online privacy. It is known that information sharing can sometimes be risky. To control this risk some corporate organizations have already implemented some policies. Unfortunately, for average SNS users, there are not many available instructions provided by concerned organizations. [10]

Chi Kin Chan, Johanna Virkki (2014) has shown special concern about personal information sharing and privacy. It shows that a large number of people shares personal information about

half of them have the habit of sharing about another person on SNS. The study displays that female user are more active in sharing personal information than male users. The research shows the importance of implementing some limitations for information sharing to protect privacy. [11]

The issues needed to be dealt with to mitigate the risks regarding information sharing and privacy issues. Susan Alexandra (2019) has provided knowledge about online privacy, Spying and spoofing. This information should be helpful for this study for helping in awareness about online privacy and ways to mitigate privacy issues. [12]

Many people share so much information about them it makes SNS another life for them. Their information-sharing habit makes social networking sites a goldmine for the social engineers containing personal data. Henry Collier (2020) has demonstrated that the behavior of a can makes them vulnerable on SNS. A social engineer observes the behavior of the targeted person based on their SNS using habits. After the observation social engineer makes contact with people to exploit their vulnerability. [13]

With the increasing number of social networking users, social engineering attacks on them come as a consequence. As a result, the number of victims of SE attacks escalating consecutively. Akib, Md & Antu, Sourov & Haque, B.M. & Hosen, Saber & Uddin, Mostafa. (2021) has shown exclusive concern about the cause of vulnerability of the user and ways to prevent SE attacks on SNS. Their study provides some knowledge that can be helpful for increasing awareness. [14]

However, there is a lack of work on social networking issues in Bangladesh. Particularly the existing works are not enough to mitigate the risks of social engineering attacks on social networking sites in Bangladesh.

Chapter 03

RESEARCH METHODOLOGY

For this study, Descriptive research design was adopted. This type of research describes a population, situation or phenomenon which is being studied.

3.1 Data collection

For this study survey method to collect primary data from end users of some social networking sites users. This web-based survey had 5 sections. First section included questions for their identity. The second chapter included questions for their social networking sites using habits. Third chapter had questions about information sharing habits of the users. Fourth section was about privacy and security. Lastly the fifth section was for the affected users.

3.2 Pre-processing and Analysis

In the pre-process step missing values were covered replaced with the most frequent category. The data set was encoded using One-hot encoding and Label encoding because the dataset was in the string form. Then the dataset was pushed into the Feature importance algorithm to find out most important features

3.3 Data visualization

For data visualization some python libraries like pandas, NumPy and Matplotlib were used. Result was found by comparing the most important features.

Chapter 04

Result and Discussion

4.1 Results

Background information:

Table 01: Age range of respondents

Age range	Number of respondents	Percentage
12 to 17	120	23.8
18 to 23	156	31.0
24 to 29	82	16.3
30 to 35	74	14.7
30 to 40	37	7.3
Over 40	35	6.9
	Total = 504	Total = 100.0

The age range of the respondents were from 12 to over 40 years old. Most of (31.0%) them were between 18 to 23 years of age. Followed by (23.8%) between 12-17 years, (16.3%) between 24 to 29 years, between 30 to 35 years (14.7%), between 36 to 40 old (7.3%) and over 40 years old age range (6.9%). As displayed in table 01.

Table 02: Occupations of the respondents

Occupation	Number of respondents	Percentage
Student	250	49.6
Businessman	56	11.1
Employee	169	33.5
Workers	9	1.8
Unemployed	20	4.0
	Total = 504	Total = 100.0

Among respondents, half of them were students (49.6%). The percentage followed by employees (33.3%), businessmen (11.1%), unemployed (4.0%) and lastly workers (1.8%). Which is shown in table 02.

Table 03: Gender of the respondents

Gender	Number of respondents	Percentage	Victims percentage
Male	300	59.52	17.46
Female	204	40.48	12.50
	Total = 504	Total = 100.00	Total = 29.96

Among the respondents, 59.52% of them were male and 40.48% were female. Among them the male respondents have a higher victim rate (17.46%) compared to female respondents (12.50%) As displayed in table 03.

Table 04: Feature importance

Label	Score
Age	0.016438
Occupation	0.010932
Internet_usage_skill	0.034578
Daily_usage	0.022528
Most_used_service	0.011640
Attack_method	0.590233
Sex	0.004398
Publish_personal_information	0.091352
Shares_personal_informationwith_people	0.086166
Account_contains_sensetive_informations	0.026952
Awares_of_privacy	0.104782

The encoded dataset was pushed into the feature importance algorithm to get the importance of other features for “Victims_of_attack” column (given in Table 04). The top 5 features were selected among them.

Privacy awareness rate and social networking system users

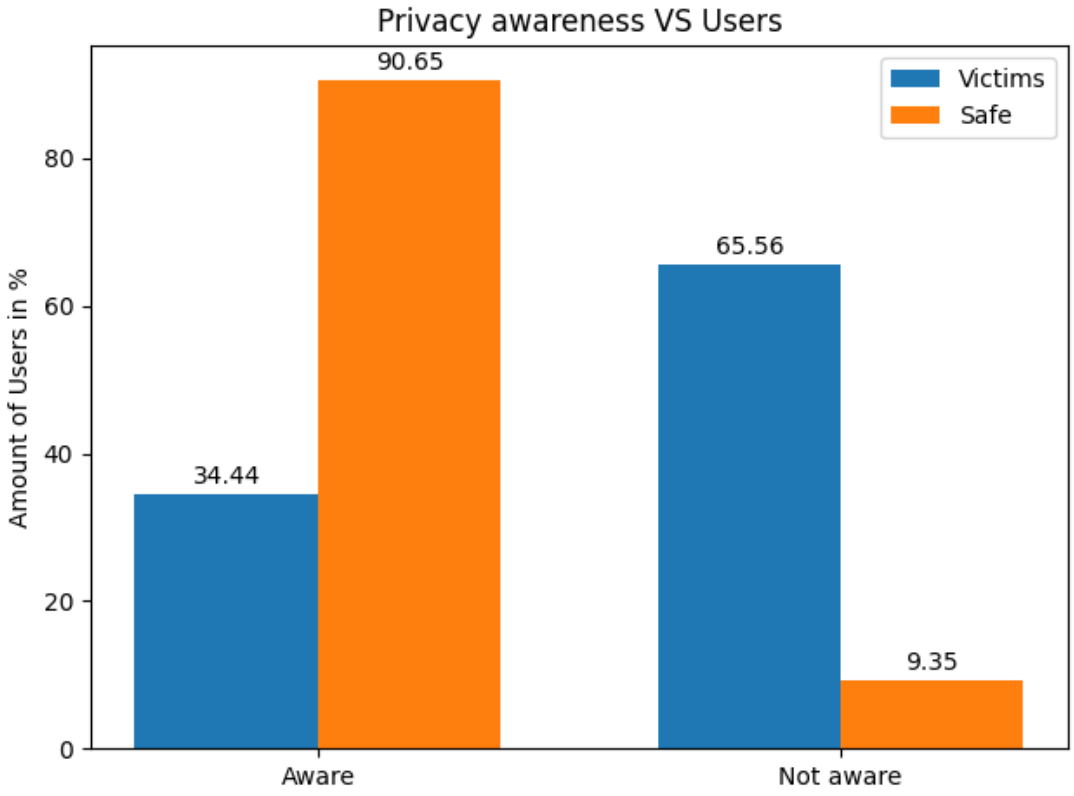

Figure 01: Privacy awareness among the SNS users

The bar chart illustrates information about the percentage of privacy awareness between both victims and safe users. Overall, most of the users that did not fall victim to the attacks were conscious of internet privacy. Among the victims most of them were unaware of internet privacy. Among the safe users of social networking sites 90.65% of them were aware of internet privacy and the rest 9.35% were unaware. Which indicates people who are aware of internet privacy are less likely to fall victim to social engineering attacks. Users who fall victim to attack among them 65.56% of them were unaware of internet privacy and 34.44% of them were aware of internet privacy. This points that unawareness of internet privacy makes people more vulnerable.

Internet using skill hierarchy of the victims

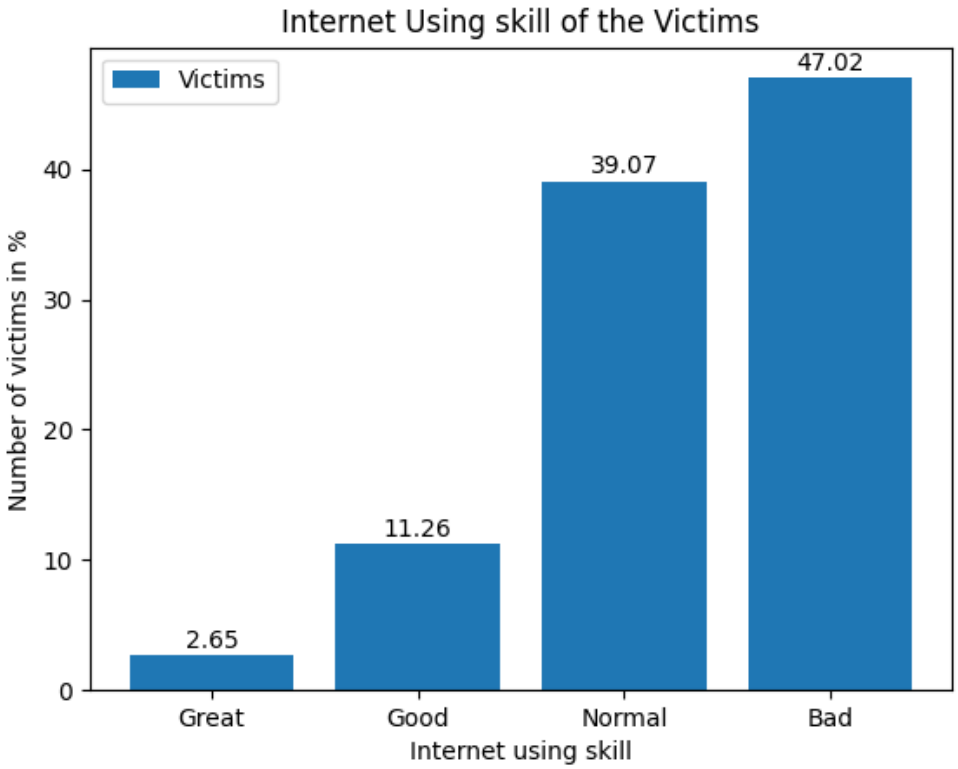

Figure 02: Internet using skill of the victims

The bar chart shows the percentage of victims according to their internet usage skill. Overall, the users with the lowest internet usage skill are the highest number of victims. Percentage of victims is lower if the users are more skilled using the internet. Among the victims who have bad internet usage skills are the highest. Which is 47.02%. victims with normal internet usage skill are 39.07%, with good internet usage skill is 11.26% and 2.65% have great internet skill. This shows that among the victim users with normal and bad internet skills are the highest.

Users and information sharing

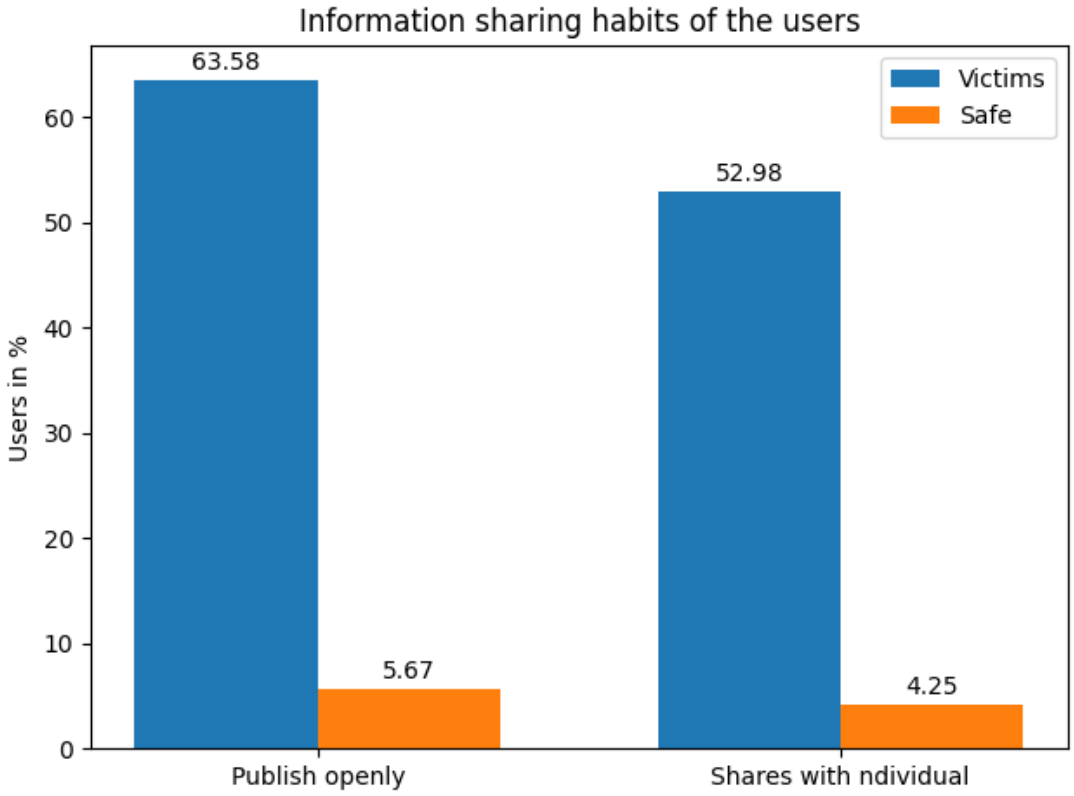

Figure 03: Information sharing rate of SNS users

The bar chart expresses the percentage of information sharing among both safe and victim users. Overall, most of the victims share information on social networking sites. Compared to them, the number of safe users that share information on SNS are low. Among the victims 63.58% of them publish their personal information openly and 52.98% of them share their personal information with other SNS users. Only 5.67% of safe users publish their personal information openly and 4.25% of them share personal information with other users.

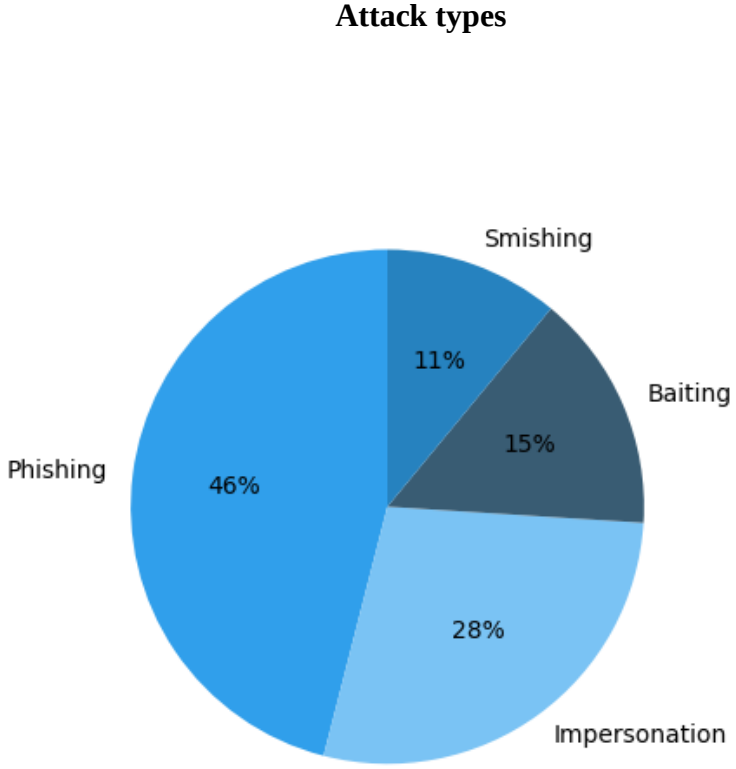

Figure 04: Various SE attacks on the victims

The pie chart provides information about different types of social engineering attacks conducted on social networking sites users. Overall, percentage of victims faced various social engineering attack. Among the social engineering attack techniques, the phishing technique occupy largest segment and the lowest contribution is smishing technique. On social networking sites Bangladesh users that experienced social engineering attacks, among them 46% faced phishing attacks. Which holds the largest portion. Second is impersonation at 28%. With 15% of the victims, bating holds the third place. The smallest part is 11% inhabited by smishing.

4.2 Discussion

Figure 01 illustrates information about the privacy awareness of the respondents. It shows the contrast between the victims and safe users about internet privacy awareness. Almost every one of safe users is aware of internet privacy. Contrarily among the victims, most of them are unaware of internet privacy. In this spotlight, users that are aware of internet privacy are less likely to be victims of social engineering attacks on social networking sites and unawareness of internet privacy makes the users potential victims of attacks. Figure 02 manifests the relation between victims and their internet using skills. This figure has constructed a hierarchy of victim's numbers according to internet usage skills. Most of the victims have bad internet usage skills. This number is followed by normal, good, and lastly victims with great internet usage skills. This result concludes better internet usage skill makes users less likely to fall victims. Information sharing rate in social networking sites between victims and safe users has shown in figure 03. It shows a large difference in information sharing rates between safe users and victims. The victims have the highest rate in both publishing their information openly and sharing it with other social network users where the safe users have very little information sharing rate in both categories. This proves that higher information sharing on social networks comes with a high risk of falling victim to social engineering attacks. Sharing less information makes users safer. Among the respondents, 29.96% of victims (displayed in table 03) have experienced social engineering attacks. Figure 04 represents these various social engineering attack rates on the victims. Most of the social engineering attacks are phishing attacks. These attack rates are followed by impersonation which also occupies a large amount then comes, baiting attacks and lastly smishing attacks.

Chapter 05

RECOMMENDATION AND CONCLUSION

5.1 Recommendation

The findings of this study have implications for the risk mitigation of social engineering attacks on social networking sites. For this awareness among users is essential. To reach the goal, the following suggestions may benefit**.**

1. Increase awareness about online privacy: Unaware of privacy makes the user an easy target for Social engineers. [12] Even posting a picture online and comments can expose a user's sensitive information to social engineers. [15] The user needs to be aware of their privacy options on social networking sites.

2. Increase awareness about the importance of better internet using skills: Users with bad internet using skills are mostly unaware of privacy and security threats. Their unawareness makes them easy targets for social engineers. [16] Better internet usage skills are needed to mitigate the risk of various social engineering attacks.

3. Awareness about information sharing: Users need to be aware of the risk of information oversharing. Oversharing benefits the social engineers to collect many sensitive data of users by stalking them which may help them to launch future attacks like account hijacking, forge identity and many more. [8] The user needs to think before posting anything online.

4. Awareness about common SE attacks: The user needs to be aware of some common SE attack method used in SNS like Phishing, Impersonation, Baiting and Smishing. Their awareness may mitigate the risk of these attacks.

5.1 Conclusion

Social networking sites have become so popular and become a digital lifestyle of the people of Bangladesh. They use numerous features of these SNS in their daily life. These features have made communication and information sharing easier than before. The popularity comes with security risks. With social networking sites being a goldmine of massive information, it attracts social engineers. Attack on social networking users is rising. Social engineers are making a strong impression in these attacks. They are using various social engineering techniques to trick people into deception. They use the art of deception to exploit human error. If this goes on then many people could lose interest in using social networking sites. This research has found some common social engineering attacks that were conducted on Social networking users of Bangladesh. The recommendation part has some suggestions to mitigate the risks of social engineering these attacks. The security concerned groups and authorities should take necessary steps to raise awareness before it is too late.

REFERENCES

[1] E. Team, "The History of Social Networking: How It All Began!," *1stWebDesigner*, 2016.

[2] S. KEMP, "Digital 2021 Laos (January 2021) v01," *DataReportal*, vol. 01, no. 2021, 2021.

[3] M. Raggo, "Anatomy Of A Social Media Attack," *Informa PLC Informa UK Limited*, no. 2016, 2016.

[4] S. L. Nalin Asanka Gamagedara Arachchilage, "Security awareness of computer users: A phishing threat avoidance perspective," *ElseEvior*, 2014.

[5] S. KEMP, "DIGITAL 2020: BANGLADESH," Kepios, Singapore, 2020.

[6] M. Raggo, "Anatomy Of A Social Media Attack," *informatech*, no. 2016, 2016.

[7] J. L. J. L. C. F. Weimin Luo, "An Analysis of Security in Social Networks," in *IEEE*, 2009.

[8] P. K. S. V. L. Y. S. J. J. H. P. Shailendra Rathore, "Social network security: Issues, challenges, threats, and solutions," *Information Sciences*, vol. 421, no. 2017, p. 27, 2017.

[9] S. C. A. A. Nurul Nuha Abdul Molok, "Information Leakage through Online Social Networking: Opening the Doorway for Advanced Persistence Threats," in *ResaeachGate*, 2012.

[10] M. B. Heidi Wilcox, "Countering Social Engineering Through Social Media: An Enterprise Security Perspective," in *Springer International Publishing Switzerland*, 2015.

[11] J. V. Chi Kin Chan, "Perspectives for Sharing Personal Information on Online Social Networks," ResearchGarte, 2014.

[12] S. Alexandra, "3 Major Internet Privacy Issues and How to Avoid Them," *1105Media Inc.*, no. 2019, 2019.

[13] H. Collier, "Social Media is a Social Engineers Goldmine," in *ResearchGate*, 2020.

[14] S. R. A. B. J. H. M. R. U. Md. Shanewaz Akib, "Social Engineering Attack for Availability of Social Media," *ResearchGate*, 2021.

[15] "Information, People, and Technology," *Emerald Publishing Limited*, no. 2005, 2005.

[16] P. K. S. V. L. Y. S. J. J. H. P. Shailendra Rathore, "Social network security: Issues, challenges, threats, and solutions," *JournalInformation Sciences*, vol. 421, no. 2017, p. 27, 2017.

