DETERMINING CORRELATION BETWEEN SOCIAL ENGINEERING AWARENESS AND BECOMING VICTIM OF SOCIAL ENGINEERING

BY

K.B.M. TAHMIDUZZAMAN
ID: 181-15-11150
TANMOY MONDOL
ID: 181-15-11214
FARZANA BABI
ID: 172-15-9945

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

Supervised By

Md. Sadekur Rahman
Assistant Professor
Department of CSE
Daffodil International University

Co-Supervised By

Dr. Fizar Ahmed
Assistant Professor
Department of CSE
Daffodil International University

DAFFODIL INTERNATIONAL UNIVERSITY
DHAKA, BANGLADESH
04,JANUARY 2022

APPROVAL

This Project/internship titled **Determining Correlation Between Social Engineering Awareness and Becoming Victim of Social Engineering**, submitted by K.B.M. Tahmiduzzaman, Tanmoy Mondol, Farzana Babi, ID NO: 181-15-11150,181-15-11214,172-15-9945 to the Department of Computer Science and Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of B.Sc. in Computer Science and Engineering and approved as to its style and contents. The presentation has been held on 04-01-2022.

BOARD OF EXAMINERS

Chairman

Dr. S.M Aminul Haque (SMAH)
Associate Professor and Associate Head
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Tania Khatun

Internal Examiner

Tania Khatun (TK)
Assistant Professor
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Internal Examiner

Md. Sazzadur Ahamed (SZ)
Senior Lecturer
Department of Computer Science and Engineering
Faculty of Science & Information Technology

External Examiner

Dr. Shamim H Ripon
Professor
Department of Computer Science and Engineering
East West University

DECLARATION

We hereby declare that; this project has been done by us under the supervision of **Md. Sadekur Rahman, Assistant Professor, Department of CSE** Daffodil International University. We also declare that neither this project nor any part of this project has been submitted elsewhere for award of any degree or diploma.

Supervised by:

Sadik

Md. Sadekur Rahman
Assistant Professor
Department of CSE
Daffodil International University

Co-Supervised by:

ফিজার আহমেদ

Dr. Fizar Ahmed
Assistant Professor
Department of CSE
Daffodil International University

Submitted by:

K.B.M. Tahmiduzzaman

K.B.M.Tahmiduzzaman
ID: 181-15-11150
Department of CSE
Daffodil International University

Tanmoy Mondol
ID: 181-15-11214
Department of CSE
Daffodil International University

Farzana Babi
ID: 172-15-9945
Department of CSE
Daffodil International University

ACKNOWLEDGEMENT

First, I express my heartiest thanks and gratefulness to almighty God for His divine blessing makes me possible to complete the final year project successfully.

I really grateful and wish my profound my indebtedness to **Md. Sadekur Rahman, Assistant Professor, Department of CSE,** Daffodil International University, Dhaka. Deep Knowledge & keen interest of my supervisor in the field of social engineering and security, influenced me to carry out this project. His endless patience, scholarly guidance, continual encouragement, constant and energetic supervision, constructive criticism, valuable advice, reading many inferior drafts and correcting them at all stage have made it possible to complete this project.

I would like to express my heartiest gratitude to **Dr. Touhid Bhuiyan**, **Head, Department of CSE,** Daffodil International University, Dhaka, for his kind help to finish my project and also to other faculty member and the staff of CSE department of Daffodil International University.

I would like to thank my entire course mate in Daffodil International University, who took part in this discuss while completing the course work.

Finally, I must acknowledge with due respect the constant support of my parents.

ABSTRACT

The purpose of social engineering is to hack into a person's security system and lure them in with luring human behavior. The art of social engineering, also known as human hacking, involves tricking employees and customers into disclosing their credentials - then using those credentials to gain access to networks or accounts. Social engineering attacks are difficult to protect against for various reasons. For one thing, they aren’t well documented. For another, social engineers are limited only by their imaginations. Regardless of the method of attack they use, social engineering is always unpredictable. The best thing you can do is remain vigilant, understand social engineers' motives and methods, and ensure ongoing security awareness within your organization to guard against the most common attacks. We survey Bangladeshi people to know how much they are aware about social engineering attacks and at the same time what is the correlation between awareness and becoming the victim of social engineering attack. It was observed through our research that there is positive correlation between these two variables though not too much.

TABLE OF CONTENTS

CONTENTS **PAGE**

CHAPTER

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

INTRODUCTION

1.1 Introduction

Nowadays people are connected to each other through the internet. We use social networking sites, online transactions, until we go to sleep on the bed. However, very few of us are aware of cyber securities through cyber-attacks are a common occurrence in the internet age. If we become aware of these threats then we can ensure a safe journey to the internet. In the recent COVID-19 pandemic period people are facing huge threats from cybercrime and losing money, personal information, and data. Among these cybercrimes social engineering is very common at present and considered one of the most devastating crimes also.

Social engineering is a way to manipulate people psychologically and obtain confidential information. The concept of performing a social engineering experiment is a really cute one. Bangladeshi people attack social engineering with their online transactions. In rural areas people, affected more by these types of attacks. Bangladesh Govt gives money for student accounts. That time, Attacker called those numbers and said I am from school or the government office. Please give me your account password and I will fix the account problem. Those people are not aware of social engineering and for this reason they give passwords to unknown people. The Attacker performs successfully.

Social engineering attacks are the most common and powerful type of attack against people. Bangladesh and the whole world face the biggest social engineering threat. Hackers sent fake news about covid-19-affected areas, hospitals, the WHO, and free medical tests to people. The victim of people responded to those mail and SMS they affected social engineering. People compromise their personal information because of this.

A good social engineer can't perform an attack one day. They gather information and analyze targets then perform. Social engineers gather information for social networking sites. We share our daily moments on social sites and share our information. The goal of attackers is some time to gain money, fun, revenge. We know about people and how they are affected by social engineering in Bangladesh. Aware of people about social engineering attacks and preventing solutions.

The aim of this research is to study the cases of social engineering that occurred in Bangladesh to understand the pattern of social engineering in Bangladesh. At the same time to make a dataset based on the information collected from these cases to predict the awareness of social engineering among the people of Bangladesh.

1.2 Motivation

Bangladesh is a small country where most of the village people are illiterate. Though our government is trying their level best to develop our country, a group of mean-minded people are trying to abuse our less techno literate people. They are taking chances with every new technology or tool launched by the government or any other technical organizations as most of the people are even able to use these technologies or tools properly. It has been observed that many people rely on others to use those tools and these make them vulnerable to social engineering.

It is also observed that people in rural areas are not aware of using a secure password also. Most often they use very simple passwords which they consider easy to remember. Unfortunately, social engineers are aware of this weakness and grab this opportunity to expose their weakness most often for gaining money and valuable information, sometimes even for vengeance.

In the recent past, Bangladesh has been through a number of devastating cybercrimes. Among those incidents, the Bangladesh Bank case, which took place in 2016, is especially notable. It cost the nation a loss of almost 8 crore and 10 lakh US dollars. In April 2020, there was another attack in different organizations which cost almost 200 billion takas. Hackers also tried to fool illiterate financial app users to gain money from them. Among these incidents, BKash users are mostly known as victims. Whereas in India, some people target ATM booth users. They attach a scanner to the ATM machine keypad. And scan all the cards and their passwords and take money from the account. Many YouTubers lose their account by clicking on suspicious links. In 2019 December 31-night Microsoft internal custom database was breached and 250 million entries were cloned [25].

All this pathetic news motivated us to conduct research to predict the awareness of social engineering threats among the people of Bangladesh.

1.3 Rationale of the Study

Social engineering is a popular tactic among hackers because exploiting people is much easier than finding a software or network vulnerability. It is often used as a first step in a larger campaign to steal sensitive data or disperse malicious software from systems or networks. In the case of Bangladesh, where a lot of people who are less aware or completely not aware of social engineering, are under immense threat of being victims of this crime. Therefore, in order to understand the awareness level of the mass people of the country is very crucial and undoubtedly this research would play a significant role in understanding the actual situation of the country. It may be vital in the future to adopt necessary policies to educate the people of our country about social engineering.

1.4 Research Questions

In order to conduct the research, the following research questions have been adopted.

1. What are the primary targets of social engineering?
2. What are the common patterns of social engineering in Bangladesh?
3. Can we make a dataset to predict the awareness of social engineering among the people of Bangladesh?
4. Can we determine the awareness level of social engineering among the common people of Bangladesh?

1.5 Expected Output

The expected outcomes of this research are:

- A dataset that may help understanding the pattern of social engineering in Bangladesh as well as may help predict the awareness of social engineering of common people.
- A model that can best fit to predict the awareness of social engineering by using different machine learning classifiers.

1.6 Project Management and Finance

There is no financial back up or funding for this work, though the research is very focused and timely. We ourselves took all the responsibilities to collect the data manually and also by using google form. Later, Google Colab was used for further preprocessing and analyzing the data. However, we would express our heartiest gratitude to Daffodil International University to provide all kinds of support for conducting this research.

1.7 Report Layout

In this report there are seven chapters altogether and which chapter talks about what is mentioned below.

Chapter 1 gives an idea about social engineering and the rationality of conducting a research on social engineering. It also includes research questions and expected outcome of the research.

Chapter 2 talks about the key terminologies of the research as well as justifies the scope of the research by finding the limitations of existing research on social engineering and other cyber threats.

Chapter 3 describes the data collection methodology and the overall methodology of how the research was conducted.

Chapter 4 narrates the findings of the research that were obtained from the model proposed in the research using various machine learning classifiers.

Chapter 5 describes the ethical aspects of the research and also about the social impact of the research.

Finally, chapter 6 concludes the report narrating the outcomes, limitations and future scopes of this research.

CHAPTER 2

BACKGROUND

2.1 Preliminaries/Terminologies

Cyber security: Cyber security involves the study and practice of securing systems, networks, and programs from external attacks. Cyber security is an interconnected security system that protects the internet against malicious cyber-attacks through hardware and software. Experts in cyber security work to protect user data and enterprise sensitive information from unauthorized access and data breaches. A strong cyber security program can also protect a system or device from attacks intended to disable or impair its operation.

Social Engineering: A technique for getting information from people by lying to them. Being a good actor is part of social engineering. The goal of social engineering is to get free stuff. Social engineering is an art of human hacking. When you are vulnerable, you will be lured in by social engineering. Social engineering exploits human weaknesses and vulnerabilities to gain access to personal information and systems. It is the art of manipulating people and preparing for targeted attacks [1],[12], [13], [14].

Phishing: Phishing is a type of online scam. The attackers send people targets via email, phone call, or message, so long as it looks real. Phishing attacks sometimes utilize URL manipulation on popular websites. Current events, charities, financial institutions, and government agencies are common phishing targets. Current events like the COVID-19 pandemic are common phishing targets. The main purpose of phishing attacks is to steal personal information. They can then use that information to access their social media accounts and bank accounts [1], [2].

Spear Phishing: Spear phishing is a highly targeted and well-known information gathering technique. The main target of this type of scam is reputed companies, public figures and other lucrative targets. Spear phishing is similar to regular phishing, but the messages come from trusted sources as well. Such as Google, PayPal, Amazon, Facebook [1], [2].

Vishing: Voice phishing is known as vishing. It's an online scam. An attacker calls you as a bank officer, law enforcement agency, or lucky draw winner. The methods for contacting more people are getting easier. The VoIP technology can be used by scammers to place hundreds of calls simultaneously. The use of VoIP technology makes it more difficult for authorities to locate fraudsters [2].

Baiting: Baiting is called one type of phishing attack. Here victims get attractive offers from the hacker. Firstly, hackers are curious about the targeted person in specific things and also making good relationships. The hackers try to gain the targeted person's faith. They always try to confine the victim in a specific way and take all the vital information or install malware in the system. Sometimes hackers give some link according to the victim's curiosity and run away to the harmful side or download malware infected applications from online [1], [2].

Pretexting: This type of social engineering attack is not commonly used. This type of attack is based on a false story or scenario. Here attackers first find the weakness of the targeted person and then make a faithful false scenario to scare the target and pretend that is a necessity for the target. The attacker also pretends that he/she can solve this problem. By this way the hacker steals all types of information and vital data [1], [2].

Phreaking: It is a technique of attacking through a telephone system. That’s why sometimes it is called phone phreaking. The first case regarding phreaking was noted in 1960. The phreaker uses this technique to make free phone calls or free long distance phone calls or tap any other phone call [24].

Tailgating: Tailgating is physical hacking. This type of hacking is used to gain access to a restricted area. Here hackers target a person who has access to this restricted area or who is able to grant access in this restricted area. Here hackers can take many forms to get access like a food delivery boy, electrician or any relative etc. [1], [3], [4].

Quid pro quo: This technique is a low-level hacking technique. Here hackers do not need high-level equipment. Here the hacker calls in a random number for a technical problem and pretends to him/her as a technical expert or a company servicer and convinces the person to share her/his personal details to solve the problem. That way the hacker takes their personal details or banking information. Sometimes the hacker tries to install malware by providing it in SMS [1].

2.2 Related Works

A growing number of people are adopting technology today. Therefore, our cyberspace is vulnerable to security loopholes. Malware, Ransomware, DDOS, SQL Injection, Phishing, Password Attracting, Cloud vulnerability, Social Engineering are currently among the most dangerous cyber threats in the present age. In cyberspace, a threat is an act aimed at harming data, stealing data, or otherwise disrupting digital life. Social engineering is a most powerful attack. The majority of hacking attacks are performed through social engineering. Almost every attack starts with social engineering.

Conteh and Schmick have worked out types of social engineering attack and how it performs. It also discusses social engineering and its role in cybercrime. It also provides individual guidelines on preventing social engineering. There is an explanation behind data collection results and output motivation behind social engineering [1].

Bansla, Kunwar and Gupta describe the social engineering attack technique and types of social engineering skills in this paper. They focus on how prevention techniques can be applied to train people and create awareness [2].

Breda, Barbosa and Morais defined social engineering and the social engineering approach in this article using Kali Linux operating system. They have described the execution of a simple example of a technical attack and demonstrated its methodology. They used the Social Engineer Toolkit (SET) that comes with Kali Linux pre-installed [3].

Chitrey, Singh and Singh in their paper, discuss the initial approaches to social engineering. Approximately 90 responses were collected via a questionnaire. Different IT domain experts participated in the study. In this paper, the main focus was on India's perspective on social engineering-based attacks [5].

Albladi and Weir analyze the vulnerability of users using the model proposed in the paper. A survey invitation email was sent to the selected experts to ask them to participate. Participants are information security specialists. The survey data collection phase is divided into two phases [6].

Ghafir, et al., have described social engineering attack strategies in their work. Several general categories can be defined based on social engineering techniques. Describe defence mechanisms against social engineering attacks [7].

Salahdine and Kaabouch describe that social engineering attacks can be classified into a number of categories based on several perspectives. It can be classified into two categories depending on the entity involved software or human. In this paper, the authors propose an overview of social engineering attacks, detection techniques, and countermeasures [8].

Junger et al. presented a work based on a survey where a total of 290 people completed the questionnaire. They have also discussed the Phishing attack in detail and how it works. They have also demonstrated how one becomes a prey to spear-phishing by just clicking on an email assuming it has come from a nearby online shop [9].

A. Algarni, Y. Xu, Taizan Chan and Yu-Chu Tian, explain the risks associated with SNSs in terms of social engineering. This paper presents an in-depth analysis of the entities and subentities responsible for social engineering attacks on social networks. The article describes a social engineering attack plan, technique, and a potential method for closing the victim [10].

S. Venkatesha, K. Reddy and B. Chandavarkar, in this paper discuss the impact of the global pandemic on social engineering attacks. A detailed analysis of COVID-19 themed attacks is included in this paper as well. The presentation also discussed targeted attacks such as Phishing attacks, Healthcare fraud, and health history-related attacks [11].

Workman, in his paper describes background and previous research on social engineering attacks. He also describes the threats and how a person falls into a trap in his paper. This paper describes how they attacked common people and also gives the procedure to avoid those things. In this paper also conduct risk analyses for the application of technological defenses [16].

Hernández, Levy and Ramim describe cyberslacking and all about the social engineering threat. This paper showed many cyberslacking activities and item sources. In this section, they describe the impact of frequency and time spent on cyberslacking on the level of ethical severity of such activities [17].

Laribee et. al. describe only how a hacker makes a trust and how to attack the targeted person. In this paper they build 2 types of model: “Trust Model”, “Attack Model”. Here, they describe only one type of attacking technique that Phishing [18].

Shindarev et. al., describe the overview of social engineering attack technique. Here only describe software base attack and here use training data to make analysis and that analysis only on company employee accounts in the website of social network VK.com [20].

Table 2.1 Comparative Analysis and Summary

Reference	**Focus**	**Data collection method**	**Sample size**	**Analysis technique**
Conteh and Schmick	Social engineering types	Primary	**N/A**	Descriptive statistics
Bansla, Kunwar and Gupta	Most fundamental social engineering attacks	Primary	**N/A**	Descriptive statistics
Breda, Barbosa and Morais	Use Kali Linux and perform social engineering attacks	Experimental Method	**N/A**	Experiment
Chitrey, Singh and Singh	India’s perspective of social engineering-based attacks	Primary	**N/A**	Descriptive statistics
Albladi and Weir	User vulnerabilities, Behaviour, Perceptual, Socio-psychological-related attributes and User characteristics framework construction	Primary	**11**	Descriptive statistics
Ghafir, et al	Social engineering attack strategies and different approaches to social engineering	Primary	**N/A**	Descriptive statistics

Salahdine and Kaabouch	Describes social engineering attacks, current detection techniques, and countermeasures.	Primary	**N/A**	Descriptive statistics
Junger et al	Phishing and social engineering	Primary	**256**	Descriptive statistics
Algarni et al.	Phishing attack, social engineer strategy, risk of victim	Primary	**N/A**	Descriptive statistics
S. Venkatesha, K. Reddy and B. Chandavarkar	Social engineering attack during COVID19	Primary	**N/A**	Descriptive and correlation statistics
Workman	Previous research paper and social engineering attack	Primary	**612**	Descriptive and correlation statistics
Hernández, Levy and Ramim	Social engineering threat and cyberslacking	Secondary	**183**	Descriptive and correlation statistics
Laribee, Barnes, Rowe and Martell	Social engineering attack with making trust	Primary	**N/A**	Descriptive statistics
Shindarev et al.	Software base social engineering attack technique	Primary	**700**	Correlation statistics

2.4 Scope of the Problem

After a thorough literature review, it has been observed no work has been done on Social Engineering focusing the people of Bangladesh. Therefore, there lies a huge research scope to observe the trends of Social Engineering attacks in Bangladesh and also the awareness of Social Engineering among the people. Further we tried to find the correlation among awareness and victims.

2.5 Challenges

The main obstacle to conduct this research was to collect data from the users as people of Bangladesh are suspicious about giving data. So, we had to adopt both online and offline data collection methods.

CHAPTER 3

RESEARCH METHODOLOGY

3.1 Research Subject and Instrumentation

Nominal variable: Nominal variables are also known as categorical variables. Nominal variables can have more than one category, and they don't have a natural order. As an example, consider occupation and affiliation to a political party as variables without numerical values. A third concept related to nominal variables is that they are named (nominalis comes from Latin, meaning pertaining to names) [41].

Nominal variables:

- Quantification is not possible. This means you can't use them as part of an arithmetic operation like adding or subtracting, or a logic operation like "equal to" or "greater than".
- Cannot be assigned any order.

Dichotomous variable: Dichotomous variables have two levels or classifications. In what is known as an analysis of variance, different levels and groups are comprised of the same independent variable (see What is Analysis of Variance? for more information on levels and groups) [41].

Dichotomous variables can be considered binary if they have either a 0 or a 1. For example, male (0) or female (1).

In addition to discrete dichotomous variables, continuous dichotomous variables can also be described as dichotomous. In this way, continuous variables and discrete variables can both be compared. There are no possibilities between two discrete variables, nor can there be between two continuous variables.

For determining how strong a correlation is between data, correlation coefficient formulas are used. Each formula returns a value between -1 and 1, where:

A positive relationship indicates a score of 1.

A negative relationship is indicated by -1.

Null results indicate no relationship at all.

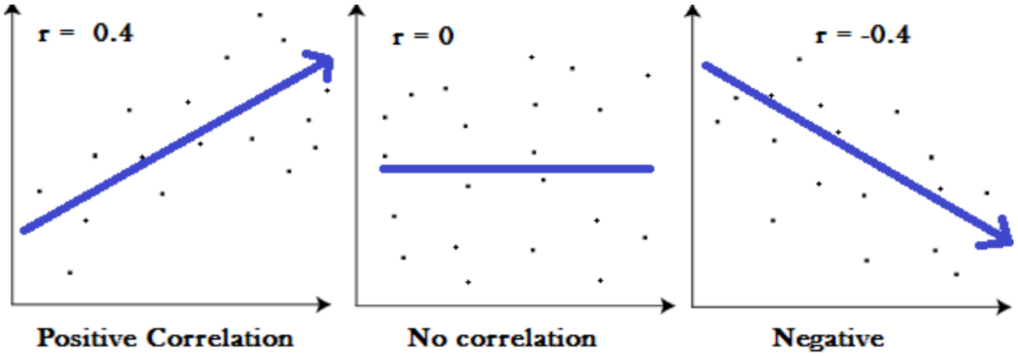


Fig 3.1: Graphs showing correlation of -1, 0 and +1 [41]

If there is a correlation coefficient of 1, then a positive increase of a fixed proportion occurs in the other variable for every positive increase in the first variable. As an example, shoe sizes increase with the length of the foot in (almost) perfect correlation.

A correlation coefficient of -1 signals that with every increase in one variable, there is a decrease in the other by a fixed proportion. As an example, the amount of gas in a tank decrease (almost) perfectly in correlation with speed.

The concept of zero means that for every increase, there is neither a positive nor negative increase. The two are independent of one another.

Relationship strength is determined by the absolute value of the correlation coefficient. The higher the value, the greater the strength of the relationship. For example, |-.75| = .75, which has a stronger relationship than .65.

Phi coefficient: Phi coefficients are measures of the association between two binary variables, also known as mean square contingency coefficients.

For a given 2×2 table for two random variables x and y:

	Y=0	Y=1
X=0	A	B
X=1	C	D

Then, the Phi coefficient can be calculated as:

$$\Phi = \frac{AD - BC}{\sqrt{(A+B)(C+D)(A+C)(B+D)}}$$

Interpreting Phi coefficient:

Phi coefficients take on values between -1 and 1 like Pearson correlation coefficients, where:

The relationship between the two variables is perfectly negative at -1.

No association between the two variables is indicated by 0.

A value of 1 indicates a perfect positive relationship between two variables.

An increasing Phi Coefficient indicates that the relationship between two variables is stronger when it is further away from zero.

Phi Coefficients are a measure of how far from zero a variable is from zero, the more evidence there is for a systematic pattern between the two variables [42].

3.2 Data Collection Procedure

No research has been conducted in Bangladesh on the subject of social engineering. The Covid-19 Situation also made it more difficult to communicate directly with people to collect data. For this reason, data is collected through a Google form. Some of the data was collected in person. Later all these online data and offline data were gathered into one excel file.

3.3 Statistical Analysis

After conducting both online or offline data collection methods we were able to collect 391 data altogether. A few demographic statistics of the dataset are given below.

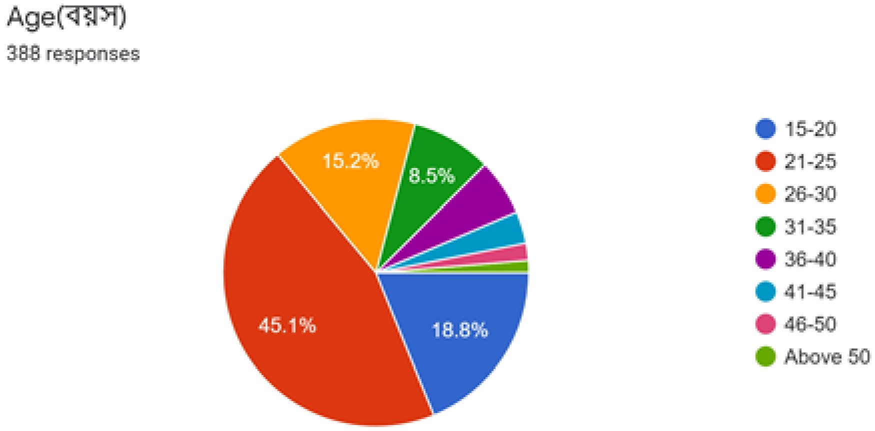


Fig 3.2: Age distribution of the respondents

Among the 391 respondents 388 respondents responded about their age. From the pie chart is easy to understand that majority of these respondents belongs to 21 to 25 age group.

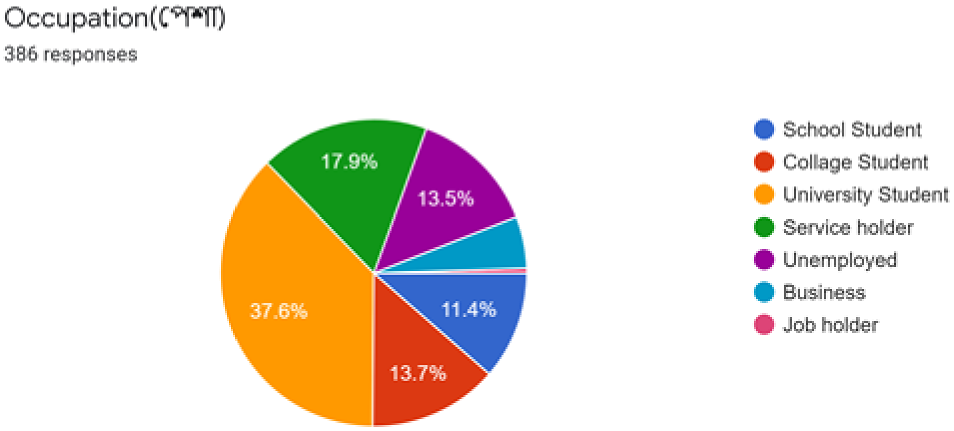


Fig 3.3: Occupation of the respondents

Among the respondents, most of them were students. If mentioned particularly, 62.7% of the respondents were students. However, among the students' majority were university going students. They individually covered 37.6% of the overall sample size.

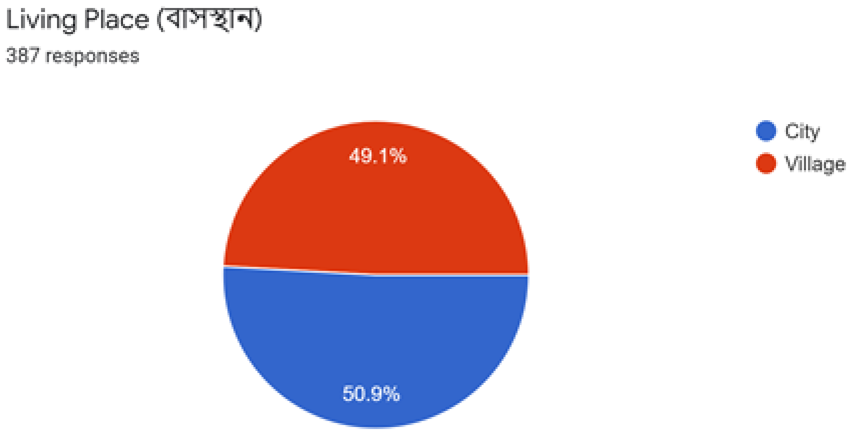


Fig 3.4: Distribution of living places of the respondents

Though data were collected randomly, distribution dwelling places of the respondents were very balanced. 50.9% of the respondents were from city and the rest of the respondents were from villages.

3.4 Proposed Methodology

The overall methodology used to conduct our research is shown in fig 3.5. Later every step of this method is explained for further understanding.

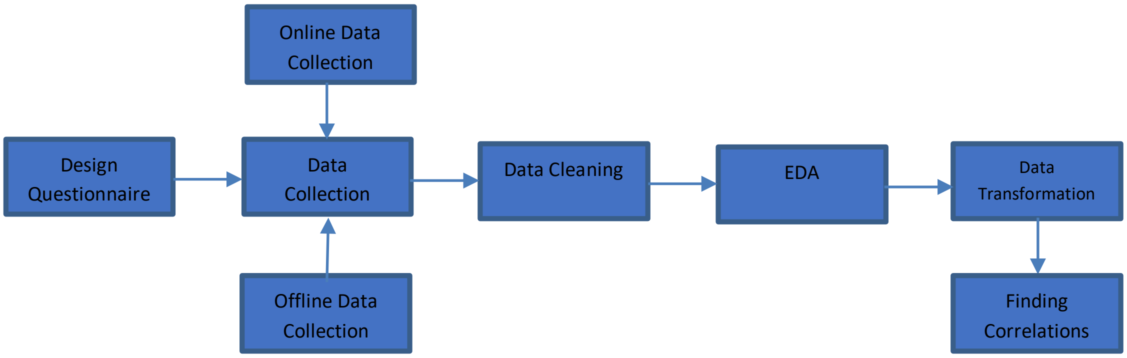


Fig 3.5: Proposed methodology

3.4.1 Design questionnaire

In order to study the social engineering attack methods, we have studied number of literatures and based on those literature we have decided our own variables to conduct our own research. Based on our selected variables we made google form which was shared online and the same form was used to collect data manually also. The questionnaire we used for collecting data is included in the appendix section.

3.4.2 Data collection

We have already mentioned that we have adopted survey method to collect our data. Survey was conducted both online and offline. As a whole we have collected 391 data. Among them 331 data were collected through online and 60 were collected manually.

3.4.3 Data cleaning

Data cleaning is one of the most important task for analyzing data. In our case, while data cleaning we have focused on whether there is any missing values or not. To avoid any kind of biasness from our dataset we have decided to remove all the entries those carries any kind of null values.

3.4.4 Exploratory Data Analysis (EDA)

After removing all the null values from our dataset, we have decided to carry on some exploratory analysis to find the statistical analysis from our dataset.

3.4.5 Data transformation

Once EDA was done, we have further decided to study the correlation among the data in our dataset. In this case, it is mentionable here that the data those were collected to study the correlation were all dichotomous data. Therefore, to conduct the research most of variables were first encoded into a simple name along with their values. We have used One Hot Encoder for this purpose.

3.4.5 Correlation finding

Finally, when all the dataset is ready for the experiment, we have done correlation test between awareness against number of victims.

3.5 Implementation Requirements

For our overall research the following tolls were used:

- Google form
- Google Colaboratory

Google Form

Google form were used to prepare the questionnaire and collecting online data.

Google Colaboratory

Google Colabratory was used to analysis data. In this context the following python libraries were used:

- Pandas
- Numpy
- Seaborn
- Matplotlib
- Sklearn

CHAPTER 4

EXPERIMENTAL RESULTS AND DISCUSSION

4.1 Experimental Setup

Before finding the correlation we have tried to observe responses of the tests' outcomes that we conducted. Finding of those tests are presented sequentially here.

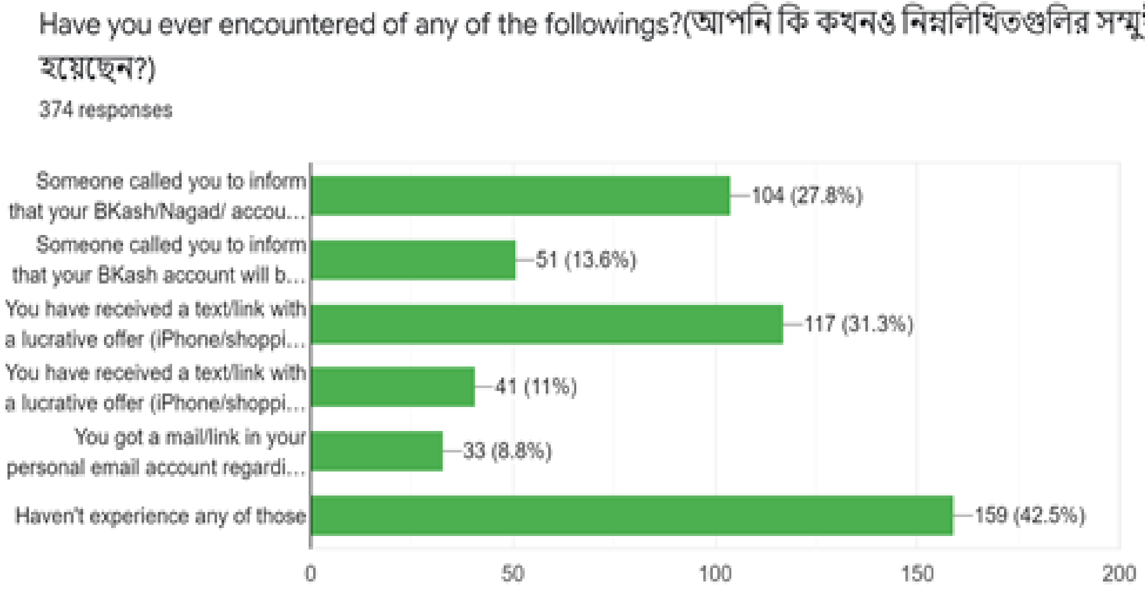


Fig 4.1: Responses to understand the social engineering attacks

Fig 4.1 shows the responses of how the respondents behave against three different types of social attacks. However, around 42.5% of our respondent didn't experience any social engineering threats.

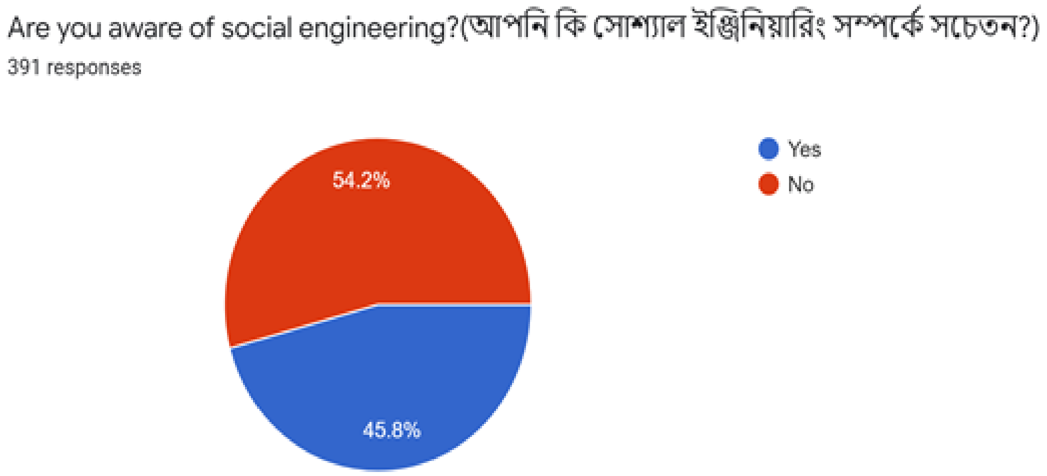


Fig 4.2: Responses to understand the social engineering attacks

Fig 4.2 shows the responses of respondents against the awareness question. However, as per their opinion 54.2% of the respondents are aware about social engineering attacks and the rest are not.

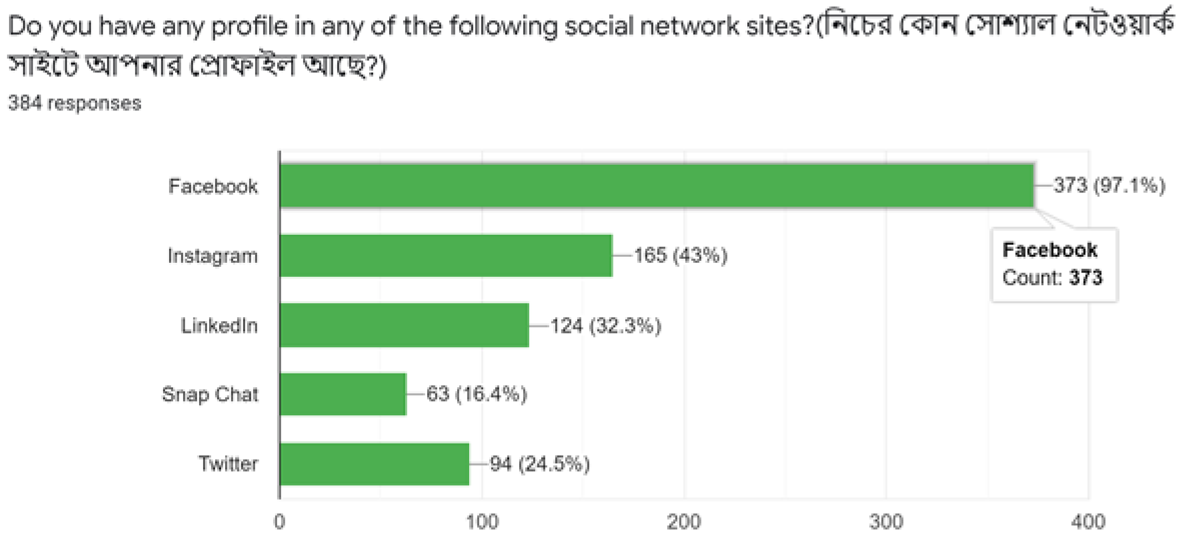


Fig 4.3: Frequency of usage of popular social media in Bangladesh

Fig 4.3 shows the usage frequency of popular social media in Bangladesh. From the graph it is obvious that facebook is by far the most popular social media in Bangladesh. Instagram, Twitter, LinkedIn and Snapchat are next popular social media as per the statistics found from our dataset.

4.2 Experimental Results & Analysis

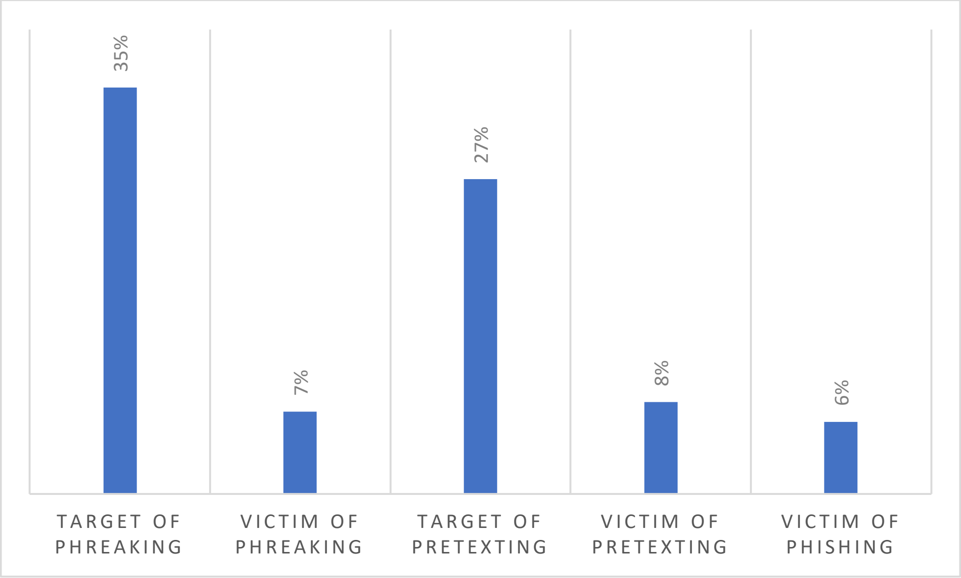


Fig 4.4: frequency distribution of target and victim of various social engineering crimes

This graph shows the percentage of Targets and victims. Target of Phreaking 35% and victim of Phreaking 7%. Target of Pretexting 27% and victim of pretexting 8%. 6% of victims have fallen victim to phishing.

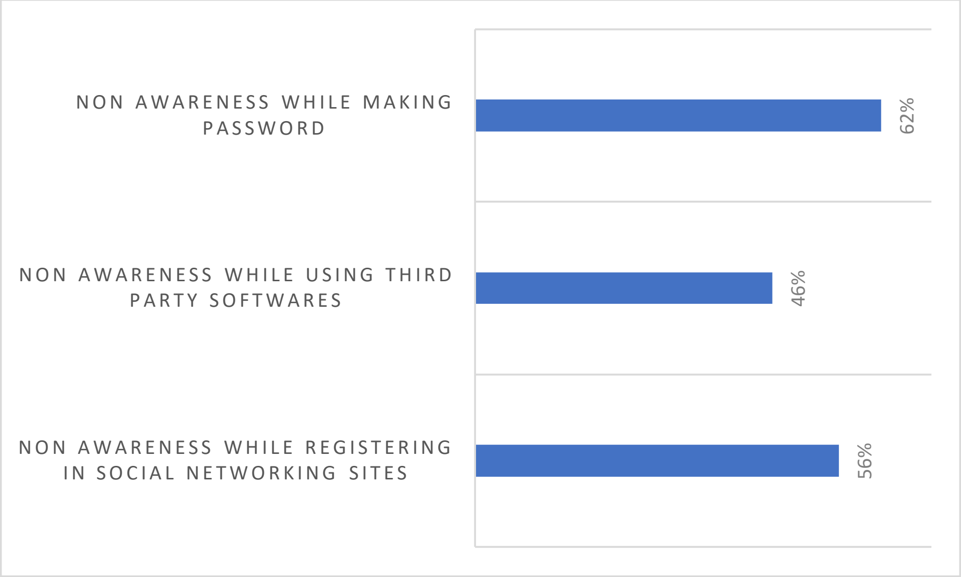


Fig 4.5: Outcome of awareness testing result

Results of non-awareness are displayed in this graph. Non awareness while making password 62%. Non awareness while using third party software 46%. Non awareness while registering on a social networking site 56%.

Table 4.1: claimed case

	Awareness = Yes	Awareness = No
Victim = Yes	28	37
Victim = No	128	160

Therefore, the coefficient calculated here is:

$$\Phi = \frac{28 * 160 - 37 * 128}{\sqrt{(28 + 37)(128 + 160)(28 + 128)(37 + 160)}} = -0.0167$$

This phi coefficient is negative but it is as close as 0. So this phi coefficient is not a perfectly negative relationship. It has a very small amount of negative phi coefficient relationship between awareness and victim of the claimed case.

Table 4.2: test case

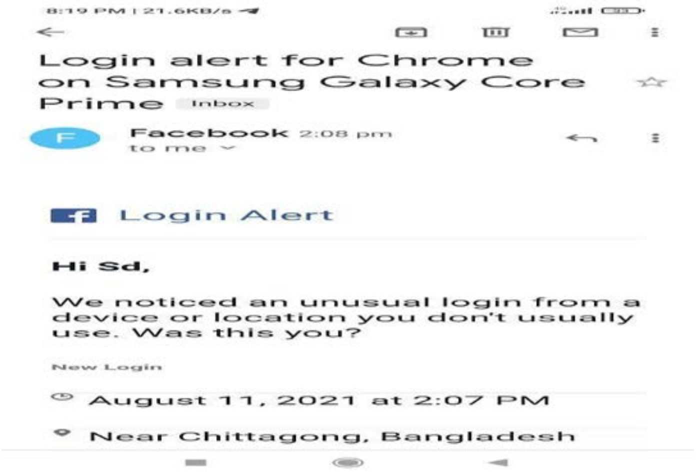
	Awareness = Yes	Awareness = No
Victim = Yes	7	58
Victim = No	28	260

Therefore, the coefficient calculated here is:

$$\Phi = \frac{7 * 260 - 58 * 28}{\sqrt{(7 + 58)(28 + 260)(7 + 28)(58 + 260)}} = 0.013579$$

This phi coefficient is positive but it is as close as 0. So this phi coefficient is not a perfectly positive relationship. It has a very small amount of positive phi coefficient relationship between awareness and the victim of the test case.

4.3 Discussion



Login alert for Chrome on Samsung Galaxy Core Prime Inbox

Facebook 2:08 pm
to me

Login Alert

Hi Sd,

We noticed an unusual login from a device or location you don't usually use. Was this you?

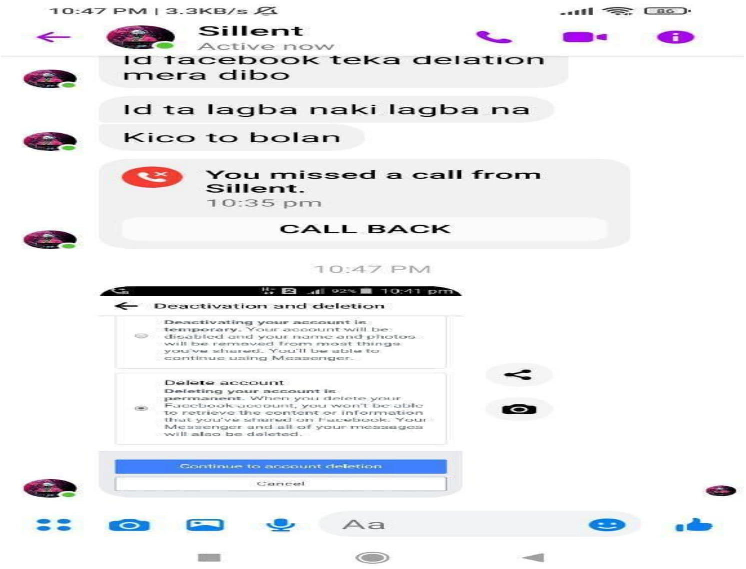
New Login

August 11, 2021 at 2:07 PM

Near Chittagong, Bangladesh

Fig 4.6: a sample case Facebook account hacking

When a hacker or social engineer is logging into his own device. Facebook shows login alerts through email.



Id facebook teka delation mera dibo

Id ta lagba naki lagba na

Kico to bolan

You missed a call from Sillent.
10:35 pm
CALL BACK

10:47 PM

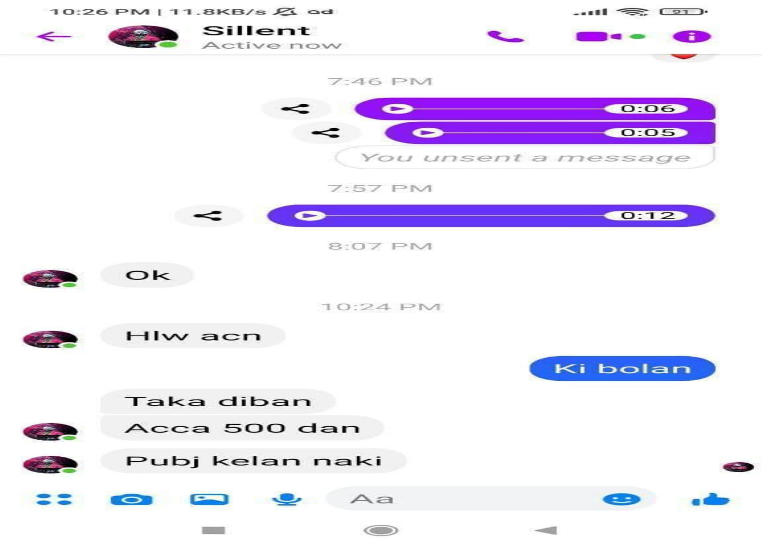
Deactivation and deletion

Deactivating your account is temporary. Your account will be disabled and your name and photos will be removed from most things you've shared. You'll be able to continue using Messenger.

Delete account
Deleting your account is permanent. When you delete your Facebook account, you won't be able to retrieve the content or information that you've shared on Facebook. Your Messenger and all of your messages will also be deleted.

Fig 4.7: Evidence of conversation of threating to account deletion

Conversion between hacker and victim in this case. The hacker scares the victim.



7:46 PM

0:06

0:05

You unsent a message

7:57 PM

0:12

8:07 PM

Ok

10:24 PM

Hlw acn

Ki bolan

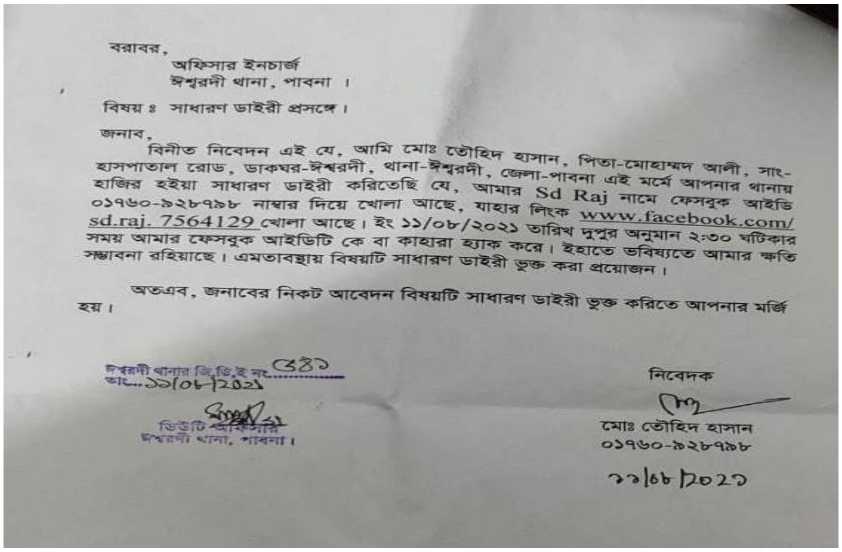
Taka diban

Acca 500 dan

Pubj kelan naki

Fig 4.8: Evidence of conversation for claiming money

In this conversion Hackers try here to scare and take money from their victims.



বরাবর,
অফিসার ইনচার্জ
ঈশ্বরদী থানা, পাবনা ।

বিষয় ঃ সাধারণ ডাইরী প্রসঙ্গে ।

জনাব,

বিনীত নিবেদন এই যে, আমি মোঃ তৌহিদ হাসান, পিতা-মোহাম্মদ আলী, সাং-হাসপাতাল রোড, ডাকঘর-ঈশ্বরদী, থানা-ঈশ্বরদী, জেলা-পাবনা এই মর্মে আপনার থানায় হাজির হইয়া সাধারণ ডাইরী করিতেছি যে, আমার Sd Raj নামে ফেসবুক আইডি ০১৭৬০-৯২৮৭৯৮ নাম্বার দিয়ে খোলা আছে, যাহার লিংক www.facebook.com/sd.raj. 7564129 খোলা আছে। ইং ১১/০৮/২০২১ তারিখ দুপুর অনুমান ২:৩০ ঘটিকার সময় আমার ফেসবুক আইডিটি কে বা কাহারা হ্যাক করে। ইহাতে ভবিষ্যতে আমার ক্ষতি সম্ভাবনা রহিয়াছে। এমতাবস্থায় বিষয়টি সাধারণ ডাইরী ভুক্ত করা প্রয়োজন।

অতএব, জনাবের নিকট আবেদন বিষয়টি সাধারণ ডাইরী ভুক্ত করিতে আপনার মর্জি হয়।

ঈশ্বরদী থানার জি,ডি,ই নং ৫৪১
তাং ১১/০৮/২০২১
ডিউটি অফিসার
ঈশ্বরদী থানা, পাবনা।

নিবেদক
মোঃ তৌহিদ হাসান
০১৭৬০-৯২৮৭৯৮
১১/০৮/২০২১

Fig 4.9: Evidence of a GD by the victim

As a measure of safety, the victim files this diary with the police station. Otherwise, his social media accounts post about crime and illegal activities.

CHAPTER 5

IMPACT ON SOCIETY, ENVIRONMENT AND SUSTAINABLITY

5.1 Impact on Society

Social engineering is very common nowadays. There are concerns that social engineering could have a negative impact on people's jobs and reputations as well as leaking confidential information. People cannot surf social networks safely because of this concern. Social engineering is a bad effect of our daily life. The findings of this study should raise public awareness about privacy and security issues. The research will also raise awareness about social engineering.

5.2 Impact on Environment

In this paper, we focus exclusively on the process of social engineering. Our focus is on software-based social engineering. By our work there is no impact on the environment. Here we only try to make the common people aware of social engineering attacks. There is not a harmful process for the environment. Social engineering attacks can affect both men and the environment. Men who are aware of such attacks can protect their information and property without affecting the environment.

5.3 Ethical Aspects

The purpose of this survey is to learn how aware people are of social engineering. The survey is completely anonymous, and no personal information will be shared. Sole reason of collecting these data is only to conduct research. Keep private and confidential information private and confidential by never divulging it to third parties. Our goal is to not misuse any of the information or privileges you are given as a result of your responsibilities. There are strict guidelines and a code of ethics we follow.

5.4 Sustainability Plan

Identifying and responding to social engineering attacks is one of the best lines of defense against social engineering. Creating user awareness begins with training everyone and continues with security awareness initiatives to keep social engineering defenses fresh in everyone's minds. Align training and awareness with specific security policies.A dedicated security training and awareness program is essential. Every employee's job description should mention information privacy and security tasks and responsibilities.

CHAPTER 6

SUMMARY, CONCLUSION, RECOMMENDATION AND IMPLICATION FOR FUTURE RESEARCH

6.1 Summary of the Study

Social engineering is one of the biggest problems in today's society. Around the world, some people have to deal with various types of social engineering attacks every day. As a small and developing country, Bangladesh is susceptible to these kinds of attacks that could hamper our development. We made this paper to make awareness among the common people. In this paper we discuss many kinds of social engineering techniques that are commonly used. We collect data to make predictions about what the common people think about social engineering. We collect both online and offline data since we gather information from all segments of the population. Using the phi coefficient, we make relationships among the data. The majority of people are not aware of social engineering, according to many coefficient relationships we made. Many of them claimed that they were aware but sometimes they face attacks. A majority of people are unaware of their password when they create it.

6.2 Conclusions

Nowadays, information security is of the most importance to everyone. A number of people lose their personal information through social engineering attacks every day. From a Bangladeshi perspective, it seems that most people don't know about their social media accounts or social engineering. In spite of the fact that social media companies update their security day-after-day, that's not enough for people without any tech education. In our paper, we try to understand the safest way of using computers for educated computer users. To make common people aware of the most basic social engineering techniques, we highlight the following. In particular, this paper will allow Bangladeshi researchers to better understand Bangladeshi people's attitudes toward social engineering.

6.3 Implication for Further Study

To ensure future work can be done as efficiently as possible, we have utilized all preliminary steps of the procedure. The research is focusing on social engineering attacks from the perspective of Bangladesh. Through our work, we demonstrate the awareness of Bangladeshi society to social engineering. We will work on preventing users from falling victim to social engineering in our future work.

Reference

1. N. Conteh and P. Schmick, "Cybersecurity:risks, vulnerabilities and countermeasures to prevent social engineering attacks", *International Journal of Advanced Computer Research*, vol. 6, no. 23, pp. 31-38, 2016. Available: 10.19101/ijacr.2016.623006 [Accessed 21 October 2021].
2. N. Bansla, S. Kunwar and K. Gupta, "Social Engineering: A Technique for Managing Human Behavior", *Journal of Information Technology and Sciences*, vol. 5, no. 1, pp. 18-22, 2019. [Accessed 21 October 2021].
3. F. Breda, H. Barbosa and T. Morais, "SOCIAL ENGINEERING AND CYBER SECURITY", *INTED2017 Proceedings*, 2017. Available: 10.21125/inted.2017.1008 [Accessed 21 October 2021].
4. M. S. Nadeem, "Social Engineering: What is Tailgating?", *Mailfence Blog*, 2021. [Online]. Available: https://blog.mailfence.com/what-is-tailgating/. [Accessed: 21- Oct- 2021].
5. A. Chitrey, D. Singh and V. Singh, "A Comprehensive Study of Social Engineering Based Attacks in India to Develop a Conceptual Model", *International Journal of Information and Network Security (IJINS)*, vol. 1, no. 2, 2012. Available: 10.11591/ijins.v1i2.426.
6. S. Albladi and G. Weir, "User characteristics that influence judgment of social engineering attacks in social networks", *Human-centric Computing and Information Sciences*, vol. 8, no. 1, 2018. Available: 10.1186/s13673-018-0128-7 [Accessed 10 November 2021].
7. I. Ghafir, V. Prenosil, A. Alhejailan and M. Hammoudeh, "Social Engineering Attack Strategies and Defence Approaches", *2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)*, 2016. Available: 10.1109/ficloud.2016.28 [Accessed 10 November 2021].
8. F. Salahdine and N. Kaabouch, "Social Engineering Attacks: A Survey", *Future Internet*, vol. 11, no. 4, p. 89, 2019. Available: 10.3390/fi11040089 [Accessed 10 November 2021].
9. M. Junger, L. Montoya and F. Overink, "Priming and warnings are not effective to prevent social engineering attacks", *Computers in Human Behavior*, vol. 66, pp. 75-87, 2017. Available: 10.1016/j.chb.2016.09.012 [Accessed 10 November 2021].
10. A. Algarni, Y. Xu, Taizan Chan and Yu-Chu Tian, "Social engineering in social networking sites: Affect-based model", *8th International Conference for Internet Technology and Secured Transactions (ICITST-2013)*, 2013. Available: 10.1109/icitst.2013.6750253 [Accessed 10 November 2021].
11. S. Venkatesha, K. Reddy and B. Chandavarkar, "Social Engineering Attacks During the COVID-19 Pandemic", *SN Computer Science*, vol. 2, no. 2, 2021. Available: 10.1007/s42979-020-00443-1 [Accessed 10 November 2021].

12. "The Official Social Engineering Hub - Security Through Education", *Security Through Education*, 2021. [Online]. Available: https://www.social-engineer.org/. [Accessed: 10- Nov- 2021].

13. M. Consulting, "The History of Social Engineering", *Mitnicksecurity.com*, 2021. [Online]. Available: https://www.mitnicksecurity.com/the-history-of-social-engineering. [Accessed: 10- Nov- 2021].

14. C. Hadnagy, *Social engineering*. Indianapolis, IN: John Wiley & Sons, 2018.

15. M. Mattera and M. Chowdhury, "Social Engineering: The Looming Threat", *2021 IEEE International Conference on Electro Information Technology (EIT)*, 2021. Available: 10.1109/eit51626.2021.9491884 [Accessed 10 November 2021].

16. M. Workman, "Gaining Access with Social Engineering: An Empirical Study of the Threat", *Information Systems Security*, vol. 16, no. 6, pp. 315-331, 2007. Available: 10.1080/10658980701788165 [Accessed 10 November 2021].

17. W. Hernández, Y. Levy and M. Ramim, "An empirical assessment of employee cyberslacking in the public sector: The social engineering threat", *Online Journal of Applied Knowledge Management*, vol. 4, no. 2, pp. 93-109, 2016. Available: 10.36965/ojakm.2016.4(2)93-109.

18. L. Laribee, D. Barnes, N. Rowe and C. Martell, "Analysis and Defensive Tools for Social-Engineering Attacks on Computer Systems", *2006 IEEE Information Assurance Workshop*. Available: 10.1109/iaw.2006.1652125 [Accessed 11 November 2021].

19. E. Rabinovitch, "Staying Protected from "Social Engineering"", *IEEE Communications Magazine*, vol. 45, no. 9, pp. 20-21, 2007. Available: 10.1109/mcom.2007.4342845 [Accessed 11 November 2021].

20. N. Shindarev, G. Bagretsov, M. Abramov, T. Tulupyeva and A. Suvorova, "Approach to Identifying of Employees Profiles in Websites of Social Networks Aimed to Analyze Social Engineering Vulnerabilities", *Advances in Intelligent Systems and Computing*, pp. 441-447, 2017. Available: 10.1007/978-3-319-68321-8_45 [Accessed 11 November 2021].

21. D. Irani, M. Balduzzi, D. Balzarotti, E. Kirda and C. Pu, "Reverse Social Engineering Attacks in Online Social Networks", *Detection of Intrusions and Malware, and Vulnerability Assessment*, pp. 55-74, 2011. Available: 10.1007/978-3-642-22424-9_4 [Accessed 11 November 2021].

22. M. Hijji and G. Alam, "A Multivocal Literature Review on Growing Social Engineering Based Cyber-Attacks/Threats During the COVID-19 Pandemic: Challenges and Prospective Solutions", *IEEE Access*, vol. 9, pp. 7152-7169, 2021. Available: 10.1109/access.2020.3048839 [Accessed 11 November 2021].

23. ["Cybersecurity - Attack and Defense Strategies", *O'Reilly Online Learning*, 2021. [Online]. Available: https://www.oreilly.com/library/view/cybersecurity-attack/9781788475297/28c7e948-5460-42b2-8e66-8dc69edd9684.xhtml. [Accessed: 18- Nov- 2021].

24. "phreaking | communications", *Encyclopedia Britannica*, 2021. [Online]. Available: https://www.britannica.com/topic/phreaking. [Accessed: 18- Nov- 2021].

25. "Microsoft Discloses Data Breach: 250 Million Records Exposed", *Fossbytes*, 2021. [Online]. Available: https://fossbytes.com/microsoft-discloses-data-breach-250-million-records-exposed. [Accessed: 18- Nov- 2021].

26. K. Jansson and R. von Solms, "Phishing for phishing awareness", *Behaviour & Information Technology*, vol. 32, no. 6, pp. 584-593, 2013. Available: 10.1080/0144929x.2011.632650 [Accessed 18 November 2021].

27. H. Aldawood and G. Skinner, "Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review", *2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE)*, 2018. Available: 10.1109/tale.2018.8615162 [Accessed 18 November 2021].

28. T. Bakhshi, "Social engineering: Revisiting end-user awareness and susceptibility to classic attack vectors", *2017 13th International Conference on Emerging Technologies (ICET)*, 2017. Available: 10.1109/icet.2017.8281653 [Accessed 18 November 2021].

29. F. Maggi, A. Sisto and S. Zanero, "A social-engineering-centric data collection initiative to study phishing", *Proceedings of the First Workshop on Building Analysis Datasets and Gathering Experience Returns for Security - BADGERS '11*, 2011. Available: 10.1145/1978672.1978687 [Accessed 18 November 2021].

30. D. Twitchell, "Social engineering in information assurance curricula", *Proceedings of the 3rd annual conference on Information security curriculum development - InfoSecCD '06*, 2006. Available: 10.1145/1231047.1231062 [Accessed 18 November 2021].

31. D. Twitchell, "Social Engineering and its Countermeasures", *Handbook of Research on Social and Organizational Liabilities in Information Security*, pp. 228-242, 2009. Available: 10.4018/978-1-60566-132-2.ch014 [Accessed 18 November 2021].

32. M. Masoud, Y. Jaradat and A. Ahmad, "On tackling social engineering web phishing attacks utilizing software defined networks (SDN) approach", *2016 2nd International Conference on Open Source Software Computing (OSSCOM)*, 2016. Available: 10.1109/osscom.2016.7863679 [Accessed 18 November 2021].

33. D. Lee, K. Choi and K. Kim, "Intelligence Report and the Analysis Against the Phishing Attack Which Uses a Social Engineering Technique", *Lecture Notes in Computer Science*, pp. 185-194, 2007. Available: 10.1007/978-3-540-74477-1_19 [Accessed 18 November 2021].

34. M. Khonji, A. Jones and Y. Iraqi, "A novel Phishing classification based on URL features", *2011 IEEE GCC Conference and Exhibition (GCC)*, 2011. Available: 10.1109/ieeegcc.2011.5752505 [Accessed 18 November 2021].

35. R. Brody, W. Brizzee and L. Cano, "Flying under the radar: social engineering", *International Journal of Accounting & Information Management*, vol. 20, no. 4, pp. 335-347, 2012. Available: 10.1108/18347641211272731 [Accessed 18 November 2021].

36. F. Mouton, L. Leenen, M. Malan and H. Venter, "Towards an Ontological Model Defining the Social Engineering Domain", *IFIP Advances in Information and Communication Technology*, pp. 266-279, 2014. Available: 10.1007/978-3-662-44208-1_22 [Accessed 18 November 2021].

37. A. Oest, Y. Safei, A. Doupe, G. Ahn, B. Wardman and G. Warner, "Inside a phisher's mind: Understanding the anti-phishing ecosystem through phishing kit analysis", *2018 APWG Symposium on Electronic Crime Research (eCrime)*, 2018. Available: 10.1109/ecrime.2018.8376206 [Accessed 18 November 2021].

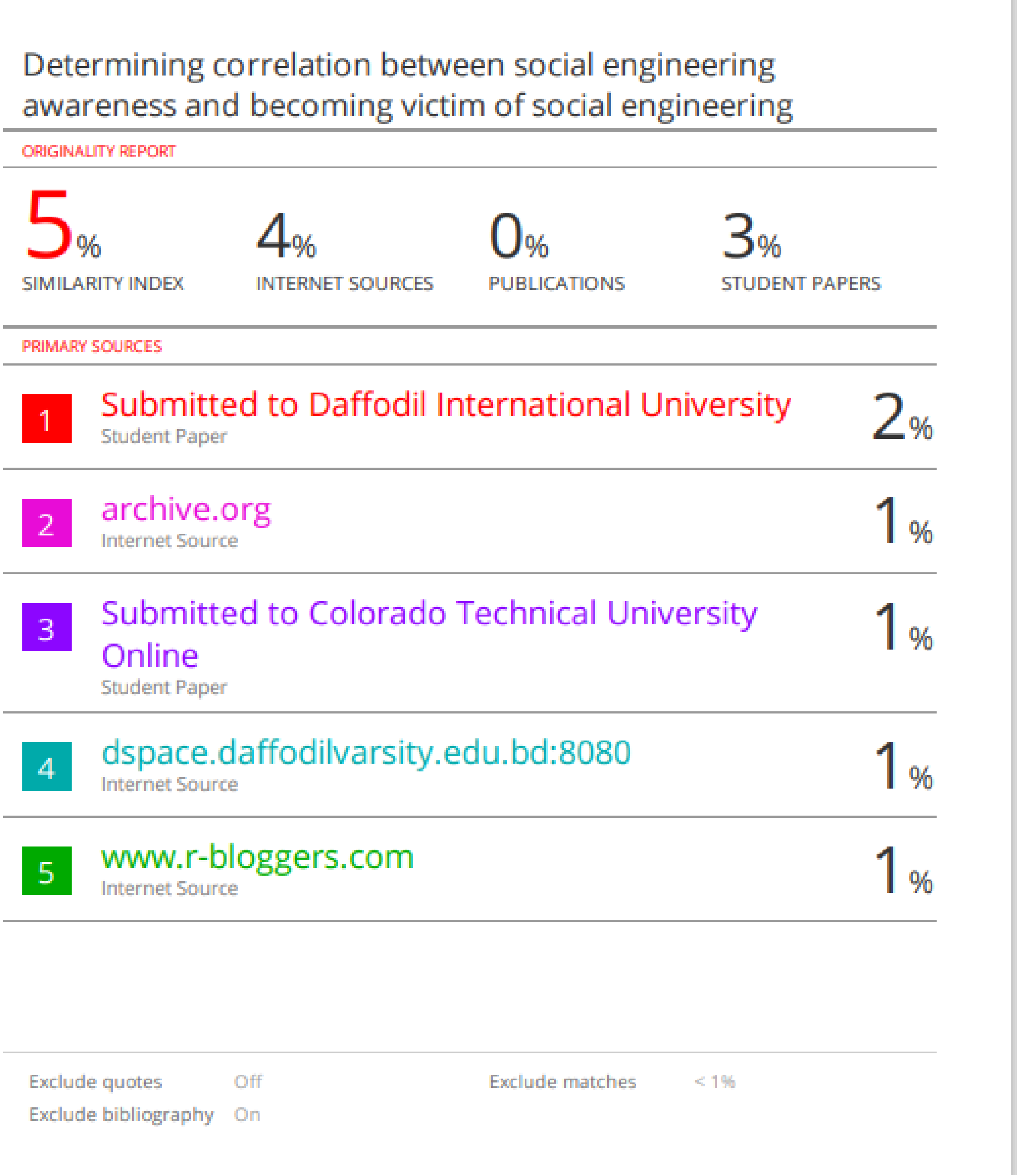
38. S. Senturk, E. Yerli and I. Sogukpinar, "Email phishing detection and prevention by using data mining techniques", *2017 International Conference on Computer Science and Engineering (UBMK)*, 2017. Available: 10.1109/ubmk.2017.8093510 [Accessed 18 November 2021].

39. E. Rabinovitch, "Staying Protected from "Social Engineering"", *IEEE Communications Magazine*, vol. 45, no. 9, pp. 20-21, 2007. Available: 10.1109/mcom.2007.4342845 [Accessed 18 November 2021].

40. H. Sandouka, A. Cullen and I. Mann, "Social Engineering Detection Using Neural Networks", *2009 International Conference on CyberWorlds*, 2009. Available: 10.1109/cw.2009.59 [Accessed 18 November 2021].

41. Stephanie Glen. "Nominal Ordinal Interval Ratio & Cardinal: Examples" From StatisticsHowTo.com: Elementary Statistics for the rest of us! https://www.statisticshowto.com/probability-and-statistics/statistics-definitions/nominal-ordinal-interval-ratio/

Plagiarism report



Determining correlation between social engineering awareness and becoming victim of social engineering

ORIGINALITY REPORT

5%	4%	0%	3%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Daffodil International University Student Paper	2%
2	archive.org Internet Source	1%
3	Submitted to Colorado Technical University Online Student Paper	1%
4	dspace.daffodilvarsity.edu.bd:8080 Internet Source	1%
5	www.r-bloggers.com Internet Source	1%

Exclude quotes Off

Exclude bibliography On

Exclude matches < 1%