IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, June 2025
Impact Factor: 7.67

A Study on Awareness of Social Engineering and the Attacks

Sakthivel[1] and Dr. Arlin Rooshma[2]
B.Com L.L.B.(Hons) 1st Year[1]
Associate Professor[2]
Saveetha School of Law, Saveetha Institute of Medical and Technical Sciences (SIMATS), Chennai

Abstract: *Social engineering has emerged as a serious threat in virtual communities and is an effective means to attack information systems. The services used by today's knowledge workers prepare the ground for sophisticated social engineering attacks. The growing trend towards BYOD (bring your own device) policies and the use of online communication and collaboration tools in private and business environments aggravate the problem. The main objective of this study is to know whether the public is aware of social engineering attacks and whom do they target the most. The researcher has followed empirical research method using convenience sampling method. the sample size is 100.The result observed from the study is that most people are unaware of the attacks of social engineering and most people agrees that the protection given by Indian Legal Framework towards the attacks of social engineers is not enough. And common people are the ones who most often fall prey for these kinds of attacks..*

Keywords: Social engineering, awareness, attacks, victim, cyber security

I. INTRODUCTION

In cyber-security, social engineering refers to the manipulation of individuals in order to induce them to carry out specific actions or to divulge information that can be of use to an attacker. Social engineering in itself does not necessarily require a large amount of technical knowledge in order to be successful. Instead, social engineering preys on common aspects of human psychology such as curiosity, courtesy, gullibility, greed, thoughtlessness, shyness and apathy.

Social engineering techniques are commonly used to deliver malicious software (malware)) but in some cases only form part of an attack, as an enabler to gain additional information, commit fraud or obtain access to secure systems. Social engineering techniques range from indiscriminate wide scale attacks, which are crude and can normally be easily identified, through to sophisticated multi-layered tailored attacks which can be almost indistinguishable from genuine interactions.There are several kinds of theft and crimes that happen online as the technology grows. Indian is one of the most prone areas for Cyber attacks. It stands in the world's 3rd cyber attacks prone area after America and China.India was ranked second globally when it comes to spam and phishing.and it ranks fourth globally with eight per cent of global detections of ransomware (a malicious software which locks computers and demands money to unlock it).

Social engineers are creative, and their tactics can be expected to evolve to take advantage of new technologies and situations. This paper outlines the different kinds of social engineering attacks and their awareness among the peoples.

Objectives :

- To determine whether the public are aware of social engineering attacks
- To determine whether the Indian Legal Framework has enough law to protect the public against the attacks of social engineering.
- To examine the most often targets of social engineers.

DOI: 10.48175/IJARSCT-27667

II. LITERATURE REVIEW

Goodchild (2019) has made a study regarding the most common social engineering tactics used by the hackers. The author has described the tactics they use frequently such as Ten degrees of separation, learning your corporate language. and also given the suitable example which makes it very easy to understand. The author emphasizes being safe from becoming a victim of social engineering.

Bisson (2019) has made a study on 5 most common social engineering methods to watch out for such as Phishing, Pretexting, Baiting. The author has described the common methods and how to escape from being a victim.

Fruhlinger (2019) has made a study on "What is Social engineering". The author has given the appropriate definition and given some examples on which social engineering takes place such as on social media, mail. The author also told about the famous social engineering attacks and also has given tips to defend against it such as train again and again when it comes to security awareness.

Collet (2016) has made a study on the topic "Social engineering tricks and tactics employees still fall for" such as well it looked official, missed a voicemail. The author has said that social engineering scam mail most often comes from official purpose mail than consumer purpose mail.

Irani (2011) has made a study on the topic "Reverse Social Engineering attacks on Social Networks". The author has mentioned that even though social media networks have several merits, when it comes to privacy and security social media fails to be helpful. The author also mentioned different modes of attacks that happen in social media and different kinds of viruses they use such as malware, Trojan horse.

Smith (2013) has made a study on the topic "Improving Awareness of Social Engineering Attacks". The author has mentioned the awareness of social engineering attacks in the society is very low and efforts are required to improve the protection of the user community. He performed experimental trials using 46 participants. and he arrived at the discussion of a new awareness raising website to aid the victims and the user community.

Krombholz (2014) has done a study on "Advanced Social Engineering attacks". The Author says that the use of social media such as linkedin, Skype, Dropbox have led to the increased social engineering attacks. He also says that the recent attacks on NYT and RSA have proved that they will be difficult to defend and they will be a dangerous weapon often used by advanced persistent threats. and he also explained about various attacks of social engineering.

Drew (2016) had done research on Conceptualising Social Engineering Tacticas and its Impacts. The author explains some types of social engineering tactics and concludes the research saying that financial literacy is associated with higher levels of victimisation than the financial Illiterates.

Conheady (2014) has done research on social engineering in IT security. The author says that Social engineering in IT discusses the roots and rise of social engineering.she also said about some specific measures to defend against social engineers. and she also addresses the impact of new and emerging technologies on future trends in social engineering.

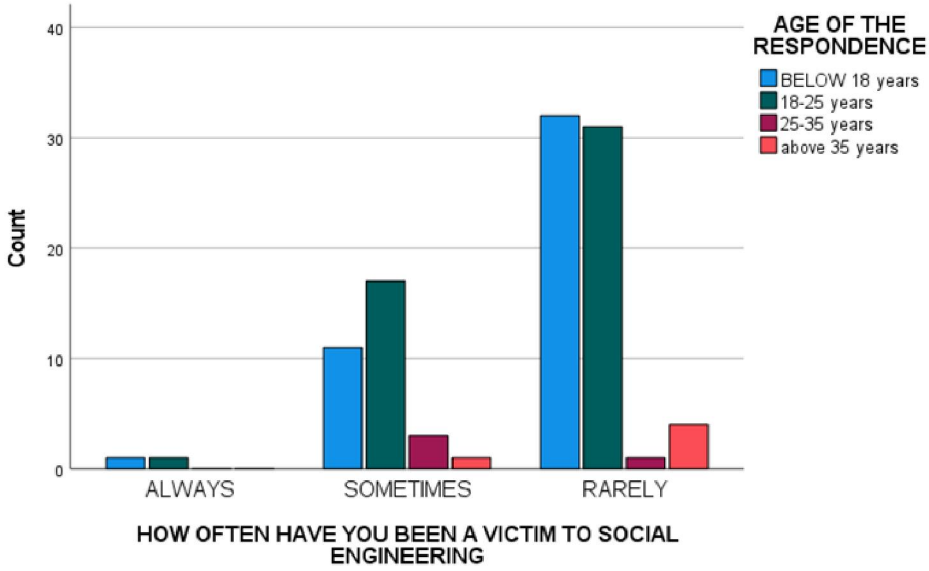
Newbould (2009) has built a game to increase the awareness amongst the people and done the research on the working of the prototype game. The author and his team designed a prototype game which has a set of rules and is simple to play. He had done the research with 21 participants and found that the awareness has been raised to 86 percent which was not even 55 percent earlier.

III. METHODOLOGY

The research method followed here is empirical research. A total of 100 samples have been collected out of which have been collected through a convenience sampling method. The sample frame taken here is in and around puducherry and Tamil Nadu through Google forms. The independent variables are age, gender, educational qualification and marital status. The dependent variables are frequency of social engineering attacks,protection of Indian legal Framework and who has more risk . The statistical tool used here is graphical presentation.

IV. ANALYSIS

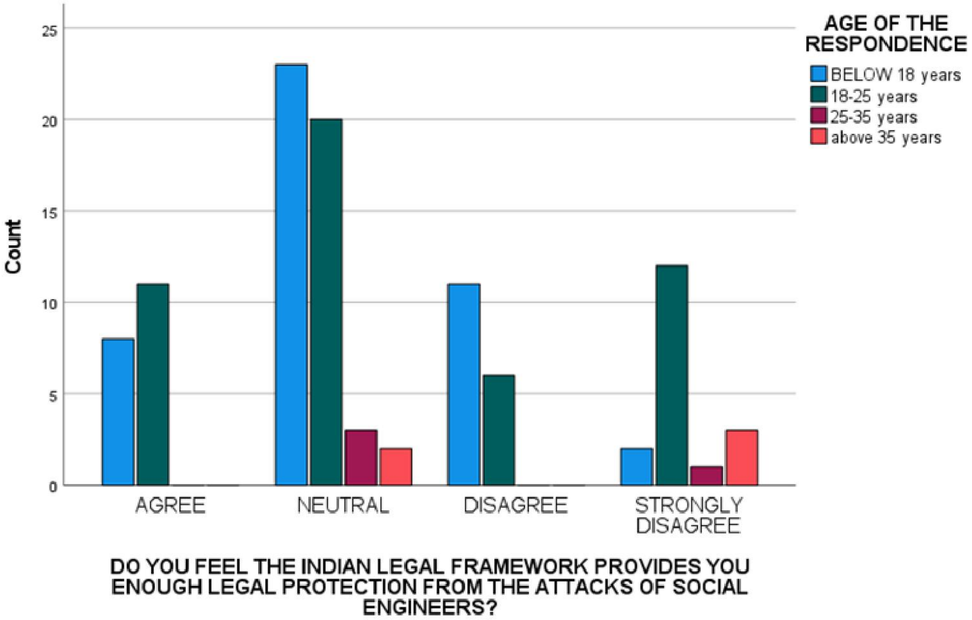
FIGURE 1



LEGEND:

Figure 1 shows the age distribution of the respondents and how often they have been a victim to social engineering.

FIGURE 2

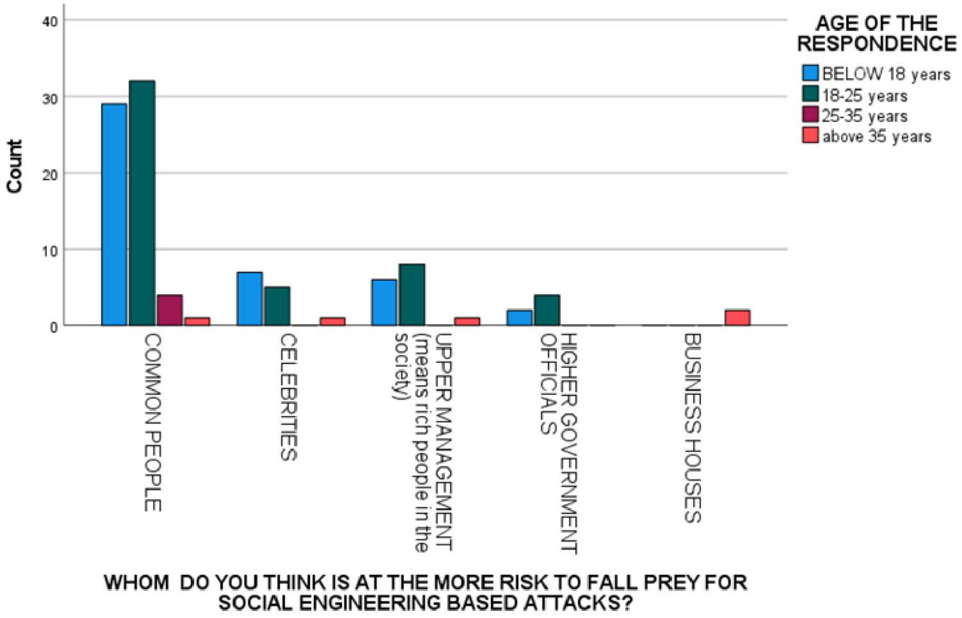


LEGEND:

Figure 2 Shows the age distribution of the respondents and how they feel about indian Legal Framework Providing Legal protection from the attacks of social engineering.

DOI: 10.48175/IJARSCT-27667

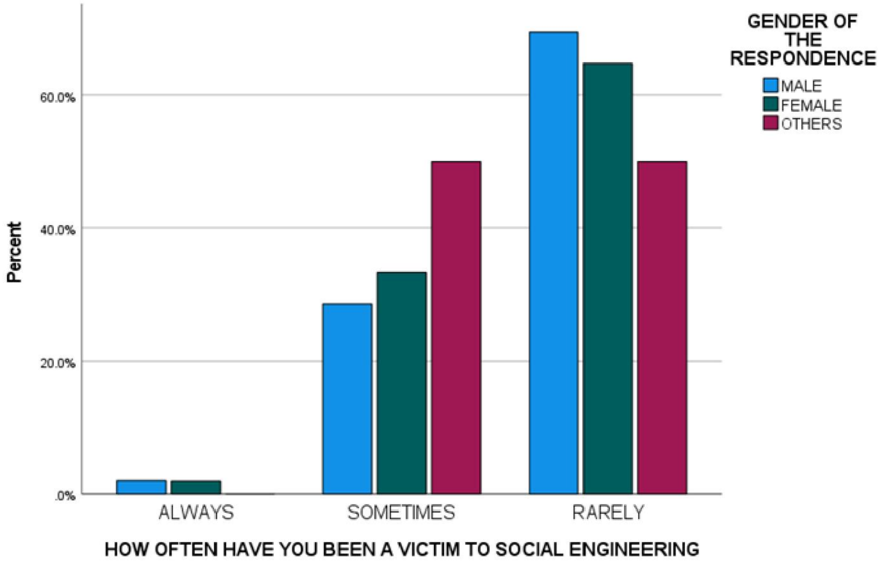
FIGURE 3



LEGEND:

Figure 3 shows the age distribution of the respondents and their opinion about whom the social engineers target

FIGURE 4

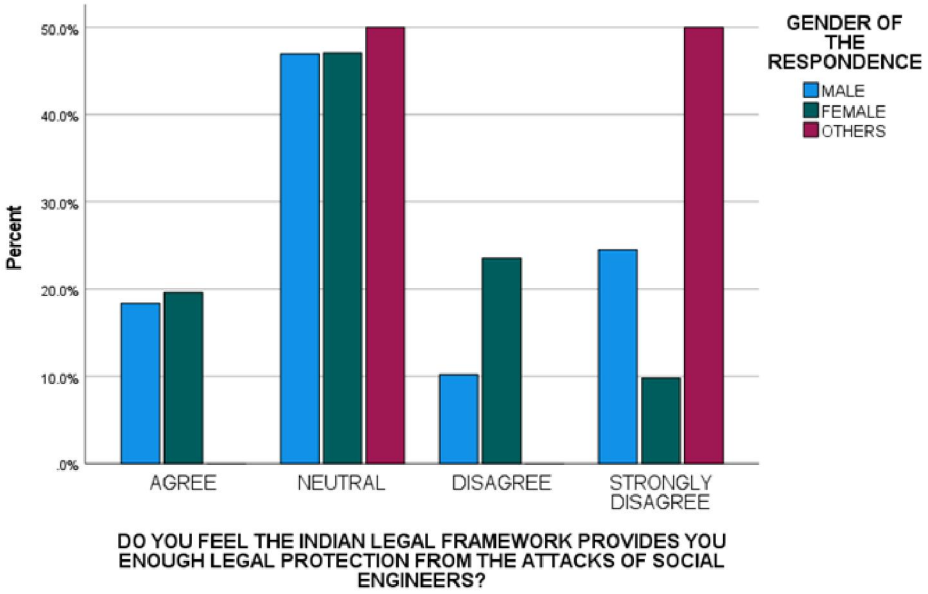


LEGEND:

Figure 4 shows the gender distribution of the respondents and how often they have been victim to social engineering attacks.

DOI: 10.48175/IJARSCT-27667

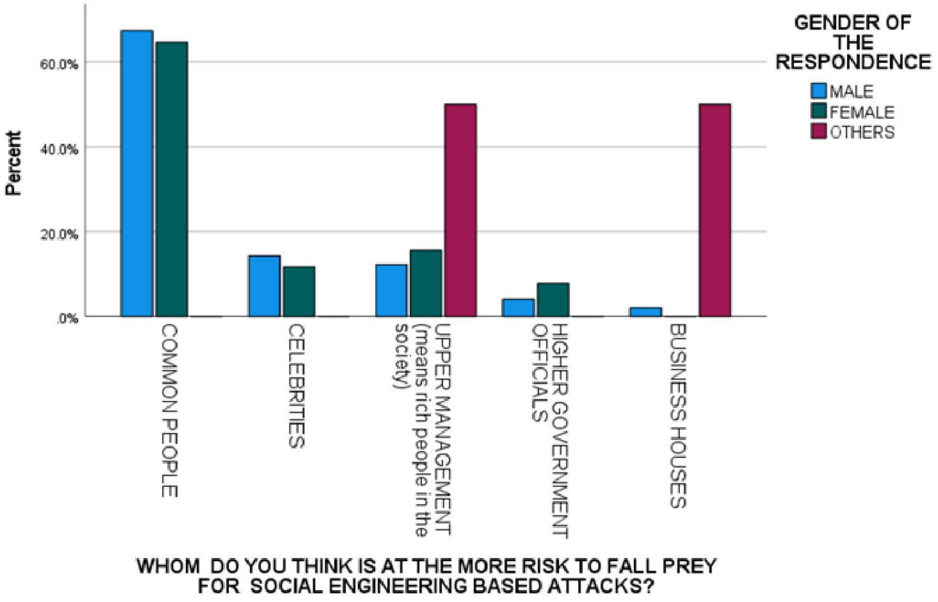
FIGURE 5



LEGEND:

Figure 5 shows the gender distribution of the respondents and how they feel about Indian Legal framework providing legal Protection from the attacks of Social engineering

FIGURE 6

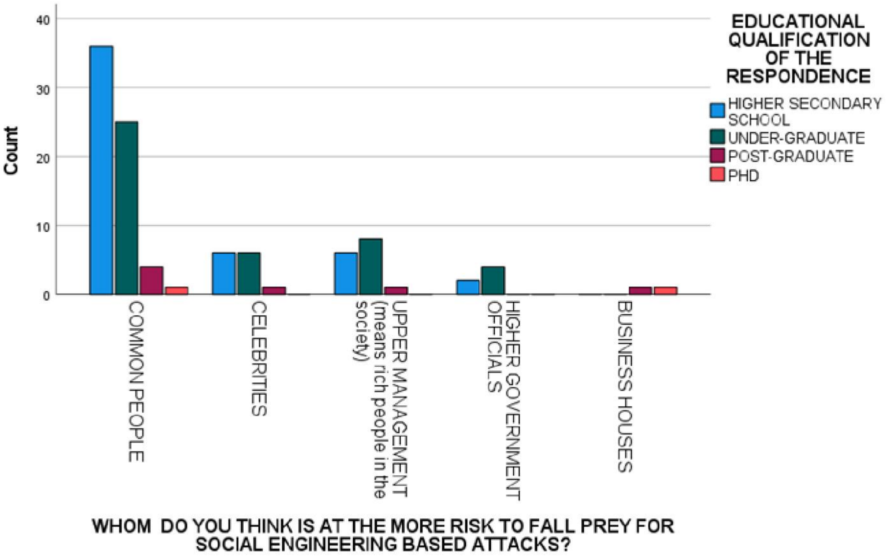


DOI: 10.48175/IJARSCT-27667

LEGEND:

Figure 6 shows the Gender Distribution about the Respondents and whom do they think is at more risk to fall prey for social engineering Attacks.

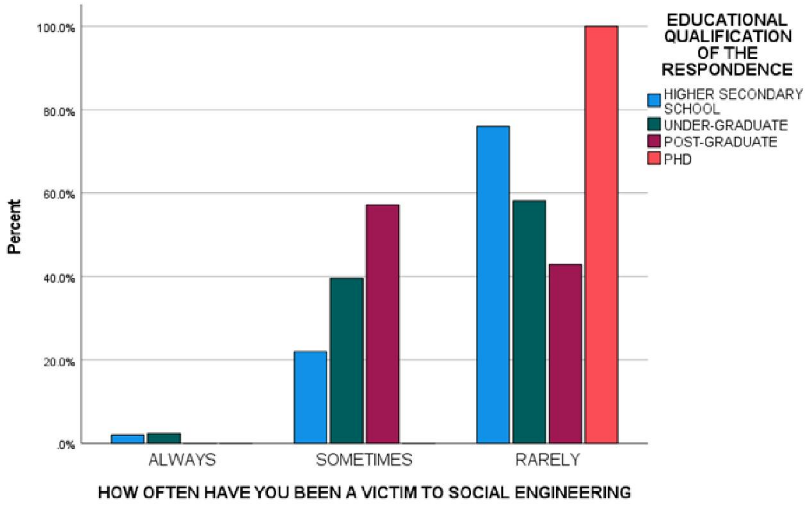
FIGURE 7



LEGEND:

Figure 7 shows the Educational Qualification of and Whom do they think is at more risk to fall Prey for Social Engineering Attacks.

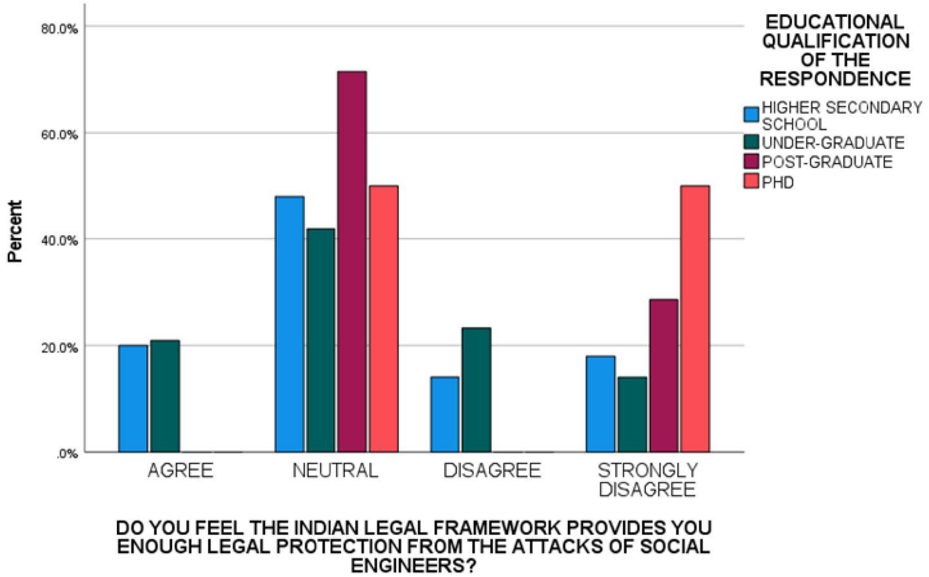
FIGURE 8



LEGEND:

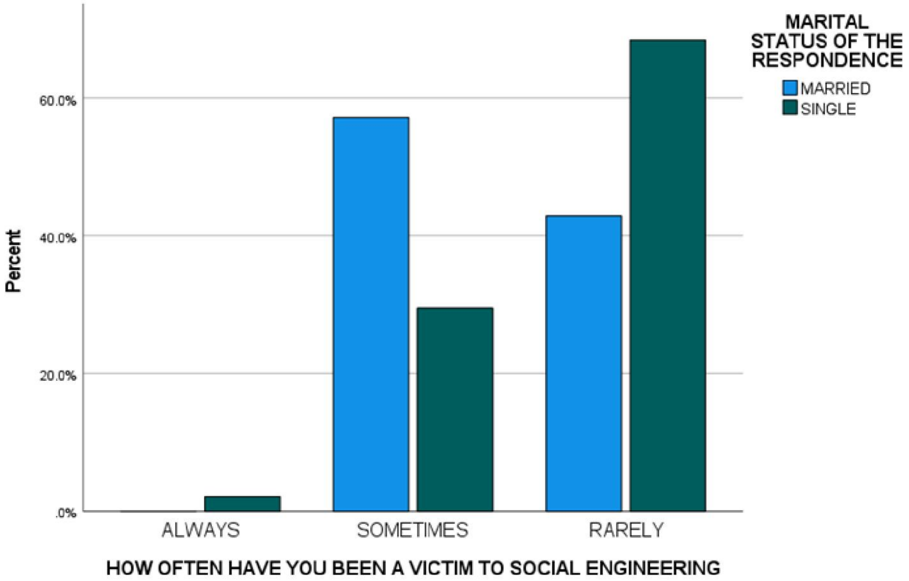
Figure 8 shows the Age Distribution of the Respondents and how often they have been a Victim to Social Engineering Attacks.

FIGURE 9



LEGEND:
Figure 9 shows the Educational Qualification of theRespondents and How they feel about Indian Legal Framework protecting them from the Attacks of Social Engineering.

FIGURE 10



LEGEND:
Figure 10 shows the Marital Status of the Respondents and how often they have been a victim to Social Engineering.

DOI: 10.48175/IJARSCT-27667

V. RESULTS

The Respondents belonging to age group below 18 years are more careful and have rarely faced the attacks of social engineering than the other age groups . (figure 1).

The respondents belonging to the age group 18-25 years strongly disagree saying that the Indian legal framework doesn’t provide us enough legal protections from the attacks of social engineering and very little amount of people agreed while many chose neutral and disagree and no one chose strongly agree (figure 2).

The respondents of every age group mostly agree that the common peoples are the usual victims of social engineers. (figure 3).

The respondents belonging to the male group have been rarely attacked than the other two groups.(figure 4).

The group female disagrees more than the male group and the others group strongly disagrees than the two groups emphasizing that the Indian legal framework should improve its protection towards the attacks of social engineering (figure 5).

The respondents of the group male and female mostly think that the common people are the victims that the social engineers target the most. while the group others mostly think business houses are the target of social engineers (figure 6).

The students of the higher secondary school mostly agree that the common people are the targets of social engineers and also the under- Graduates mostly think that (figure 7).

The respondents of the group PHD have never been a victim to social engineering and the group higher secondary school students have rarely encountered the attacks of social engineers (figure 8).

The respondents of the group higher secondary school and the group under graduates mostly remain neutral while the group PHD strongly disagree saying that the Indian legal framework doesn’t provide enough legal protection (figure 9).

The respondents of the group married have mostly been a victim of social engineering while the group single have rarely been a victim of social engineering (figure 10).

VI. DISCUSSION

Respondents belonging to the age group below 18 years have experienced less attacks than the other age groups .This may be because the students below 18 years group may have not used laptops and systems more often and they may have not been the target of social engineers because they have no access to any financial resources and bank accounts (figure 1)

The respondents belonging to age group 18-25 years strongly disagree saying that the Indian legal framework doesn’t provide us enough legal protections from the attacks of social engineering and no one chose the option “strongly agree” this maybe because people think that the constitution of India was framed before 70 years and the laws framed 70 years ago are outdated cannot control the crimes that happens through the internet nowadays (figure 2)

The respondents of every age group mostly agree that the common peoples are the usual victims of social engineers .They may have thought that because common people are easy targets for the social engineers and attacking them might not create a big problem for the social engineers as compared to other categories (figure 3)

The respondents belonging to the male group have been rarely attacked than the other two groups. This may be because either the male group is more cautious than the other two groups or targeting the female may have been easy for the social engineers. (Figure 4)

The group female disagrees more than the male group and the others group strongly disagrees than the two groups this maybe because that the citizens may have lost their confidence in government protecting them. (Figure 5)

The respondents of the group male and female mostly think that the common people are the victims that the social engineers target the most. This may be because they have heard more common people suffered because of social engineering attacks other than any categories mentioned. (Figure 6)

The students of the higher secondary school mostly agree that the common people are the targets of social engineers and also the under- Graduates mostly think that. This maybe because they have thought that attacking the common people is very easy than any others (Figure 7)

DOI: 10.48175/IJARSCT-27667

The respondents of the group PHD have never been a victim to social engineering and the group higher secondary school students have rarely encountered the attacks of social engineers. This may be because the persons who have completed PHD are smart enough and nowadays teenagers are better informed than the people in their 30's and 40's. (Figure 8)

The respondents of the group higher secondary school and the group under graduates mostly remain neutral while the group PHD strongly disagree saying that the Indian legal framework doesn't provide enough legal protection. This may be because they may think that the Indian legal framework doesn't have enough laws to protect people from social engineering threats. (Figure 9)

The respondents of the group married have mostly been a victim of social engineering while the group single have rarely been a victim of social engineering. This may be because married people are older than the unmarried and the unmarried people may be aware about the social engineering threats while the married doesn't even know its existence. (Figure 10).

Limitation:

One of the major limitations of the Study is the sample frame. There is a major constraint in the sample frame as it is limited to a small area. Thus,it proves to be difficult to conclude the Whole population. Another major Limitation is that the Researcher has acquired a Convenience sampling Method in which we can't expect the result to be 100% perfect.

VII. CONCLUSION

Based on the result of the analysis done, it has been found most of the people aren't aware of the attacks of social engineering and only people below the age of 25 years are well protected from social engineering attacks and every sample has encountered the attack of social engineering at least once in their life. Majority of the samples agrees that the Indian legal framework doesn't provide enough protection from the attacks of social engineers which emphasis the government to improve its protection towards the growing threat of social engineering .And majority of people agrees that the common people are the ones who fall prey to the attacks of social engineering while the other categories have some awareness. This situation emphasis the government of India to take measures to create awareness about the attacks of social engineers and also educate the common people towards protecting themselves from the attacks of social engineering

REFERENCES

[1]. Smith A., Papadaki M., Furnell S.M. (2013) Improving Awareness of Social Engineering Attacks. In: Dodge R.C., Futcher L. (eds) Information Assurance and Security Education and Training. WISE 2013, WISE 2011, WISE 2009. IFIP Advances in Information and Communication Technology, vol 406. Springer, Berlin, Heidelberg.ISBN: 978-3-642-39377-8

[2]. Newbould, M., & Furnell, S. (2009). Playing Safe: A Prototype Game For Raising Awareness of Social Engineering. DOI: https://doi.org/10.4225/75/57b4004e30de7

[3]. Katharina Krombholz, Heidelindel Hobel, Markus Huber, Edgar Weippl,Advanced Social Engineering Attacks.Volume 22, June 2015, Pages 113-122,ISSN: 2249-0559.

[4]. Drew J.M., Cross C. (2016) Fraud and its PREY: Conceptualising Social Engineering Tactics and its Impact on Financial Literacy Outcomes. In: Harrison T. (eds) Financial Literacy and the Limits of Financial Decision-Making.Palgrave Macmillan ISBN:978-3-319-30885-2

[5]. Sharon conheady,Social Engineering in IT Security : Tools,Tactics,Techniques , published in 2014 by McGraw-Hill Education Group,ISBN : 978-0-07-181846-9.

[6]. John Goodchild,Most common Social engineering Tactics by the hackers,2019,Vol 7, issue 1,ISSN : 2320-7132

[7]. Max Bission, Study on Five Most Common Social Engineering Methods,International Journal Of Research Of Research Thoughts,2019,ISSN : 2450-2884

[8]. Stefan Fruhlinger,Mike Ross,What Is social Engineering, 2019,Vol 19,issue 4,May 2019, ISSN: 2349-7568

[9]. Dave Collet, John Reese,Social Engineering Tricks And Tactics employees still fall for,2016,ISSN : 2247-0556

[10]. Karan Irani, Harold Finch, Reverse Social Engineering Attacks On Social Networks, Vol 8,issue 5, August 2011,ISSN : 2237-8451.

DOI: 10.48175/IJARSCT-27667