ESSENTIAL AWARENESS OF SOCIAL ENGINEERING ATTACKS FOR DIGITAL SECURITY

Ms. Tanu Manocha, Ms. Vinita Sharma

New Delhi Institute of Management
E-mail: emailtotanu@gmail.com ; vinitasharma75@gmail.com

Abstract

In the current time of pandemic when almost every next person is working from home by using Internet technologies, so it has become necessary for all organizations to ensure that their employees have a basic knowledge of social engineering along with information security. In current global situation, social engineering is considered to be one of the biggest security threats. They should be aware of the kind of threats emerging from social engineering attacks to save their secret organizational data.

This study is an attempt to check the level of awareness of social engineering attacks among professionals who are working online. A survey of employees, who are working in Delhi NCR in different organizations and industries, was conducted. The results of the survey revealed the fact of awareness employees have for social engineering and protective policies. The study also analyzed the impact of demographic profile of employees based on their age, gender, education and internet usage on social engineering attacks.

Keywords – Social engineering, cyber security, pandemic, COVID 19, Work from home

Introduction

Due to digitization the use of the internet has increased and also the risk associated with that has also increased. In the current scenario, the World Wide Web is dominating in all the spheres of life. But it is inviting a new threat of social engineering each day. Now, the rude act of data theft which was done by attackers has been beautifully swapped by more refined procedures. Irrespective of the types of technology or software used by the company or individuals, such types of manipulative methods help the hackers to get into the information system of the victims. Hence, if we talk about the current scenario of the virtual world, social engineering has become the biggest security threats.

As suggested by Ahmad, (Ahmad, 2017) –social engineering crimes are not only by the use of

technology or the technological knowledge but also by the exploitation of human vulnerabilities. It also indicates that awareness of social engineering attacks, the knowledge and the security practices significantly affects the employees.

It is very clear that it is essential to understand the security practices and policies which can reduce the threats to social engineering. This field is constantly evolving and in such a scenario it becomes crucial to understand the concept of social engineering threats and the practices to reduce these attacks by creating awareness about security protective policies.

The security of data has become a major concern (Ahmad,2017) explain that the cyber-crime attacks which take place on computers were a major threat for individuals and the economy but these attacks have been shifted to social engineering attacks. These attackers are quite knowledgeable about human flaws, how to manipulate people and infect the information systems and steal the credentials and transfer data.

(Aldawood & Skinner, 2018) defined social engineering, a non-technical method, which depends on human interaction, tricking and manipulating people and breaking the normal security procedures. Such kinds of threats are very vulnerable and cause much damage (Daimi,2017)

According to the US department of Justice, –social engineering attacks are considered to be the most dangerous and risky threats all over the world and it highly impacts the worldwide economy.

The use of cutting edge technology and complex functionalities with many more innovative practices has made the networks more vulnerable to various security threats and hacks. (Team,2014) There are various kinds of threat like Phishing, SQL injection, Social Engineering, hacking, spamming, denial of services attack, virus and worm, an endless list.

Social Engineering is a specific form of attack. It is the human who is breaking the integrity which cannot be protected with hardware or software. People with lack of knowledge or awareness are considered to be the weakest link in the security chain. (Algarmi,2107) explained, –an employee gives away the key information on email or telephonically and it is the tact or the trick of gaining sensitive information and exploiting the basic human nature of trust, fear and desire to help. Companies are using the various authentication processes, firewalls, VPN and network monitoring software but are still open to attacks. Eaves-dropping,

dumpster diving, tailgating, Fake- Software and many more.

Classification of Attacks based on Social Engineering

Based on the nature of attacks, social engineering attacks can be classified as below -

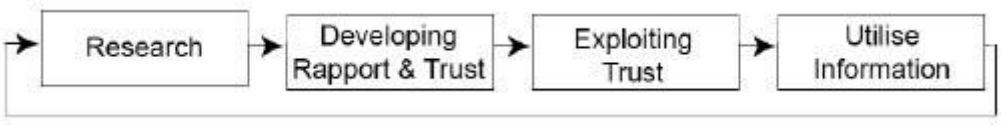
1. Human-based attacks, are possible only when human interaction takes place between the attacker and victims.
2. Technology-based attacks, in which the use of computers is essential to execute the attacks. (Power & Forte, 2006) (Gulati, 2003) explained about human based attacks.
3. Social based social engineering attacks. (Patil & Devale, 2016).

1) Human Based Attacks:

These types of social engineering attacks take place during human interaction when the attacker tries to manipulate the victims to get the secret information of the processes or systems. It may happen through personal meeting or a telephonic conversation. Kevin Mitnick's Social Engineering Attack Cycle identified several approaches which include:

- Impersonation
- Posing as a new employee
- Shoulder Surfing
- Dumpster diving
- Threatening the victim for providing secret information
- Pretexting
- Telephonic Social Engineering Attacks
- Pretending as a partner or client or law enforcement to the victim

According to (Pokrovskaia & Snisarenko, 2017), ‒human based attacks are considered to be the physical actions which are performed by the attacker to collect information about the target. The searching in dumpsters for valuable documents can be considered as an example of such kind of attacks.



Kevin Mitnick's Social Engineering Attack Cycle

Source-
https://www.researchgate.net/publication/263588935_Social_Engineering_Attack_Framework/figures?lo=1

2) **Technology Based Attacks:** It is a kind of social engineering attacks which is most popular and it is a computer –based attacks. These attacks involve phishing emails which target individuals in order to obtain private details such as bank account log-in information.

Various other kinds of social engineering attacks include (Wilcox et al., 2014):

- Falls Message Box for advertising various products or competitions
- Pretexting
- Scareware
- Fraudulent Emails e.g. scam emails
- Viruses through email attachments
- Phishing
- Vishing
- Baiting
- Fake- Software
- Ransomware
- Reverse Social Engineering
- SMSishing

Different kinds of attacks like technical based attacks, human and social base attacks. As explained by (Kalniņš et al., 2017) are those attacks which are conducted through internet via the online services and social networks and websites, and all by using the desired information which is gathered by using passwords, credit cards and security questions.

Another kind of attacks like social based attacks, which are most dangerous attacks and are most successful as they involve human interaction (Patil & Devale, 2016) explains that these attack victims are played in both the ways psychologically as well as emotionally for example baiting and spear phishing. It also includes online Social Engineering.

Since all such attacks are increasing every day with stronger and smarter plans and techniques,

it is therefore essential to be aware of the security protective policies and to minimize the impact of these attacks (Algarmi,2017). Various measures are taken to reduce these impacts as explained (Chan and Mubarak, 2012) use of Firewalls, Installation and updation of Antivirus, Security Practices, Refuse to disclose the sensitive information, use of strong password, Education and many more are to be followed.

Objectives

The main research objective is to provide a survey on employees of various organizations in Delhi and NCR. Expected outcomes include:

- To identify the kind of awareness employees, have for social engineering attacks.
- To identify the awareness level of various practices followed by the respondents to reduce social engineering attacks.
- To identify the effect of demographic profile (based on age, gender, education level and internet usage) on social engineering attacks.

Methodology

In order to achieve the objectives and test the hypothesis a primary study was done using a survey method among the employees working from home in various organizations in Delhi NCR.A close ended online questionnaire was designed to measure the social engineering attacks, security protective practices, use of internet, age, gender and education. The survey was done online through social media platforms. The online questionnaire was sent to 500 employees out of which only 243 responded. The collected data was analyzed with the help of MS Excel and SPSS.

Measurements

Awareness about social engineering attacks was measured using 4 items (Not at all, very less aware, moderately and quite knowledgeable). The different types of social engineering were measured by 15 items and number of attacks were considered. The different kinds of questions for social engineering attacks were measured like have you been the victim of social engineering attack. The responses were measured with 4 options (never, once or twice, 3-5 times, very often). The responses about the security protective policies were included, as the respondents were aware about security protective policies, and were measured by taking two responses (Yes and No). The question regarding security protective policy includes the types

of protective practices followed (like the firewalls, installation and continuous updating of antivirus, knowledge of security practices, refusal to disclose sensitive information, usage of strong password). Table 1 represents the demographic features of the respondents.

Table1: Demographic features (N= 243)

Gender wise Analysis		
Gender	**No. of respondents**	**Percentage**
Female	106	43.6%
Male	137	56.3%
Total	243	
Age wise Analysis		
Age Group	**No. of respondents**	**Percent**
less than 30 years	2	0.8%
31-40 years	64	26.3%
41-50 years	177	72.8%
Total	243	
Educational Qualification wise Analysis		
Qualification	**No. of respondents**	**Percent**
Undergraduate	8	3.2%
Graduate	30	12.3%
Post graduate	205	84.4%
Total	243	
Internet Usage wise Analysis		
Internet Usage	**No. of respondents**	**Percent**
less than 2 hours	9	3.7%
2-5 hours	26	10.7%
6-10 hours	127	52.2%
Almost all the time	81	33.3%
Total	243	

Source: Primary Data

Data Analysis and Hypothesis Testing Hypothesis

A hypothesis was proposed that the individuals who have knowledge of social engineering attacks are using methods to secure themselves and whether it is dependent on the demographic

profile of the respondents or not. Based on this view, following hypotheses were suggested:

Hypothesis 1 (H01): There is no association between Age and Social Awareness attacks
(Ha1): There is an association between Age and Social Awareness attacks

Hypothesis 2 (H02): There is no association between Gender and Social Awareness attacks
(**Ha2**): There is an association between Gender and Social Awareness attacks

Hypothesis 3 (H03): There is no association between Educational qualification and Social Awareness attacks
(**Ha3**): There is an association between Educational qualification and Social Awareness Attacks

Hypothesis 4 (H04): Time of internet usage and Social Engineering Awareness have no association.
(Ha4): Time of internet usage and Social Engineering Awareness have no association.

Data Analysis

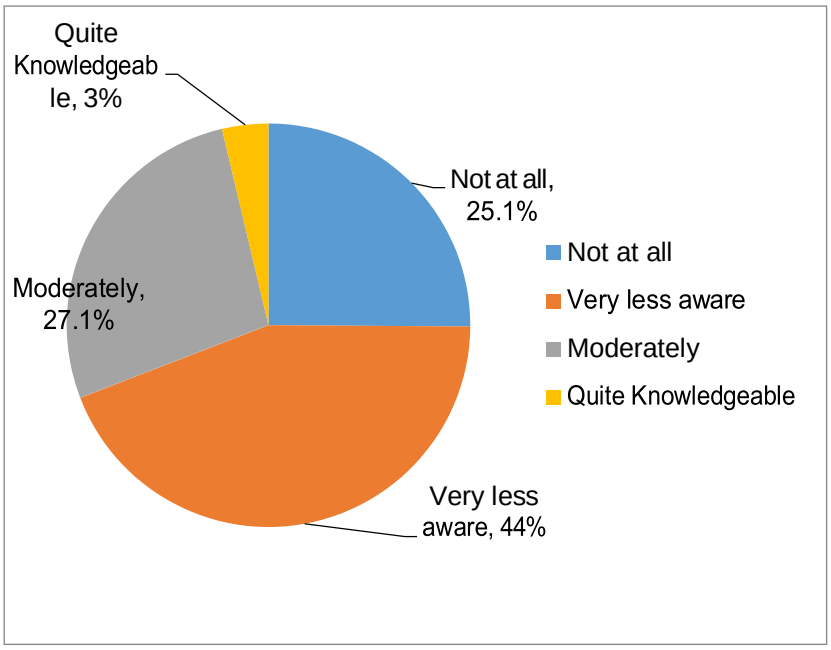
To understand the first objective, we need to identify the level of awareness among the respondents regarding social engineering. Table 2 and Figure 1 clearly show that 25.1% of respondents are not at all aware about the social engineering attacks followed by 44% who are very less aware, 27.1 % are moderately aware and 3.7 % who are quite knowledgeable.

Table 2: Social Engineering – Level of Awareness

Social Engineering – Level of Awareness		
Awareness Level	**No. of respondents**	**Percentage**
Not at all	61	25.1%
Very less aware	107	44%
Moderately	66	27.1%
Quite Knowledgeable	9	3.7%
Total	243	

Source: Primary Source

Fig1: Awareness about Social Engineering Attacks



Source: Primary data

Table 3 and figure 2 indicate different kinds of social engineering attacks with which the respondents are aware of.

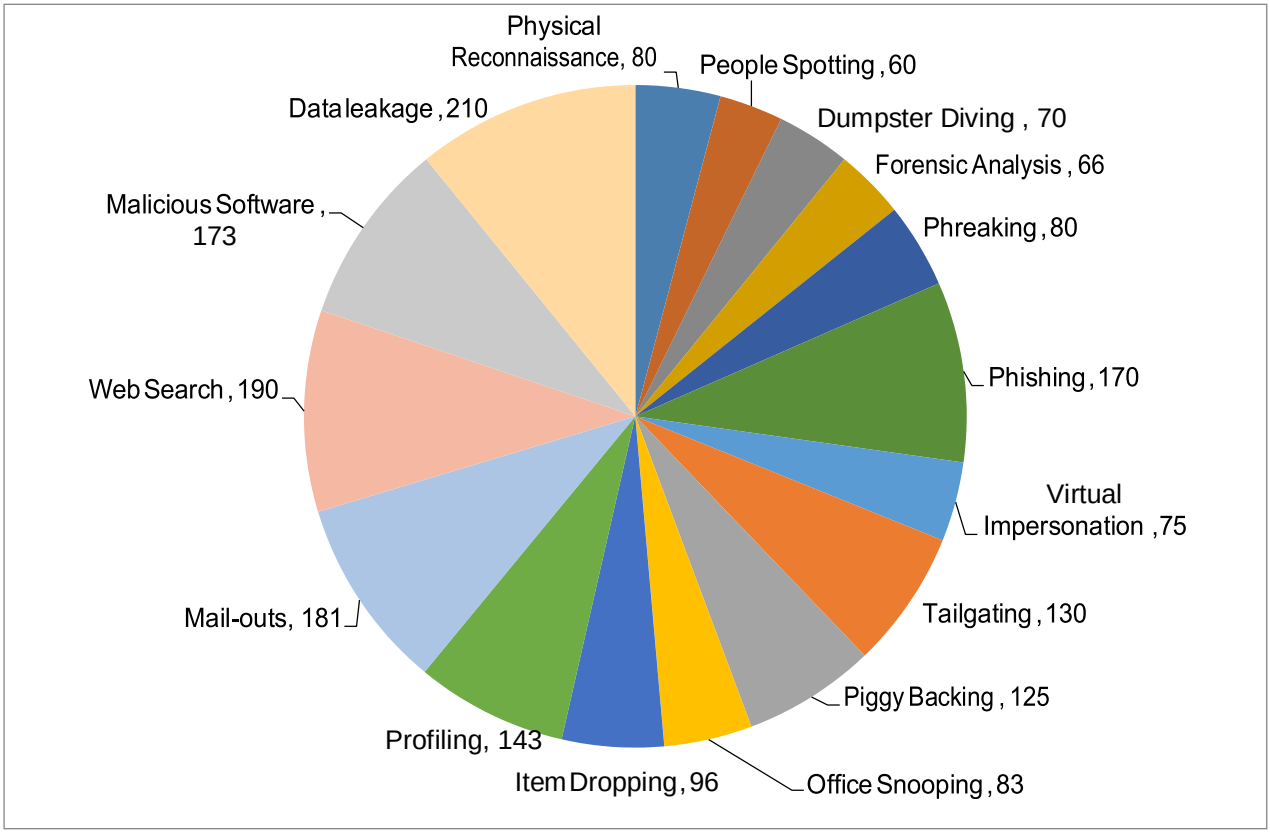
Table 3: Classification of Threats from Social Engineering

Social Engineering Attacks	No. of respondents	Percentage
Physical Reconnaissance	80	32.92%
People Spotting	60	24.69%
Dumpster Diving	70	28.8%
Forensic Analysis	66	27.16%
Phreaking	80	32.92%
Phishing	170	69.95%
Virtual Impersonation	75	30.86%
Tailgating	130	53.49%
Piggy Backing	125	51.44%
Office Snooping	83	34.15%
Item Dropping	96	39.5%
Profiling	143	58.84%
Mail-outs	181	74.48%

Web Search	190	78.18%
Malicious Software	173	71.19%
Data leakage	210	86.4%

Source: Primary Data

Figure 2: Types of Social Engineering Attacks



Source: Primary Data

Table 4 represents whether the respondents have been the victim of any social engineering attack or not. It clearly indicates that 64.1 % of respondents are never hit by any social engineering attack. 34.1 % were experienced only once or twice followed by 0.8 % for 3-5 times and 0.8% very often.

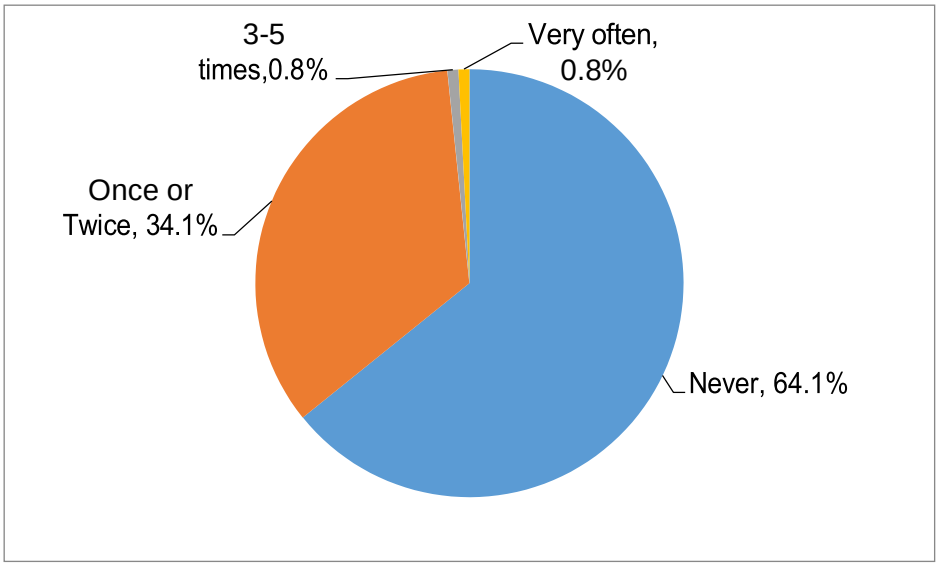
Table 4: Frequency of Victimisation

Frequency of Victimisation		
Victims	**Frequency**	**Percentage**
Never	156	64.1%
Once or Twice	83	34.1%
3-5 times	2	0.8%

Very often	2	0.8%
Total	243	

Source: Primary Data

Figure3: Victim of Social Engineering Attacks



Source: Primary Data

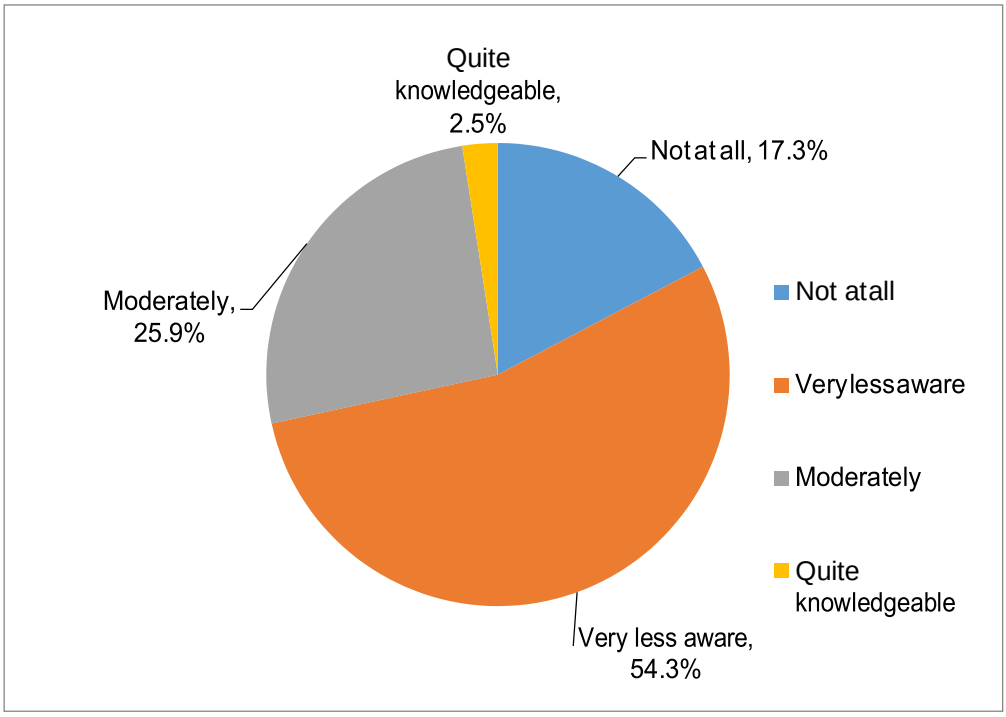
Figure 4 represents the awareness of security protective practices followed, to avoid social engineering attacks. 17.3% of the respondents were not at all aware about the protective practices, 54.3% of the respondents were very less aware and rest 25.9% were moderately aware and very few of them i.e. 2.5% were quite knowledgeable.

Table 5: Awareness Security Protective Practices

Awareness	No. of responses	Percent
Not at all	42	17.3
Very less aware	132	54.3
Moderately	63	25.9
Quite knowledgeable	6	2.5
Total	243	

Source: Primary Data

Figure 4: Awareness about Security Protective Practices



Source: Primary Data

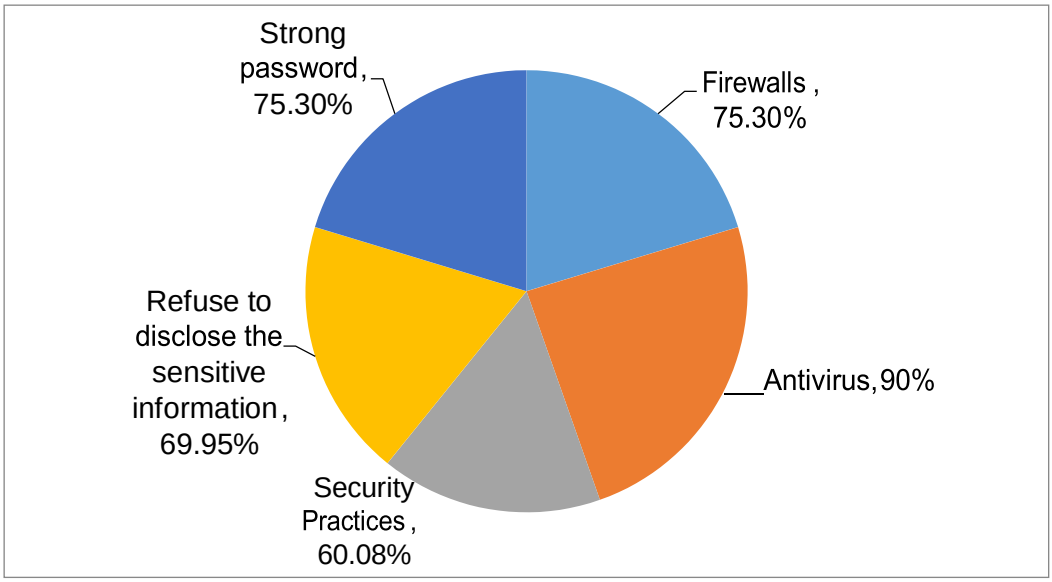
Table 6 and figure 5 indicate about different kinds of social Protective Practices.

Table 6: Types of Social Protective Practices

Social Protective Measures	No. of responses	Percentage
Firewalls	183	75.30%
Antivirus	219	90.12%
Security Practices	146	60.08%
Refuse to disclose the sensitive information	170	69.95%
Strong password	183	75.30%

Source: Primary Data

Figure 5: Types of Social Protective Practices



Source: Primary Data

To test the hypothesis, to study the effect of demographic features (gender, age, educational qualification and usage of internet) on the social engineering attacks, a chi-square test was applied.

Table 7 indicates the key results of age with the social engineering attacks.

Table 7: Age with the Awareness of Social Engineering Attacks

Chi-Square Tests

Test	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	14.496	6	.025
Likelihood Ratio	7.607	6	.268
Linear-by-Linear Association	.592	1	.442
No. of Valid Cases	243		

–a- 5 cells (41.7%) have expected count less than 5. The minimum expected count is .07.

Source: Primary Data

The value of test statistics is 14.496. Hence, in this case, *p= 0.025.*

The value *p* is associated with chi- square value and is less than the significant value (0.05) Hence, the null hypothesis is rejected, which means there is association between age and the awareness of social engineering attacks.

Table 8 indicates the relationship between the genders with the social engineering attacks.

Table 8 – Relationship between Genders and Social Engineering Attacks

Chi-Square Tests			
Test	**Value**	**Df**	**Asymptotic Significance (2-sided)**
Pearson Chi-Square	3.579	3	.311
Likelihood Ratio	3.574	3	.311
Linear-by-Linear Association	.000	1	.996
N of Valid Cases	243		

—a- 1 cells (12.5%) have expected count less than 5. The minimum expected count is 3.93. ‖

Source: Primary Data

The value of test statistics is 3.579. Hence, in this case, *p= 0.311.*

The value *p* is associated with chi- square value and is more than 0.05 (the significant value). Hence, it shows the acceptance to the NULL HYPOTHESIS, which means that there is no association between gender and the awareness of social engineering. Gender is independent of awareness of social engineering.

Table 9 indicates the relationship between the educational qualifications with the social engineering attacks.

Table 9: Relationship between the educational qualifications with the social engineering attacks

Chi-Square Tests			
Test	**Value**	**Df**	**Asymptotic Significance (2-sided)**
Pearson Chi-Square	4.389	6	.624
Likelihood Ratio	4.784	6	.572
Linear-by-Linear Association	.610	1	.435
No. of Valid Cases	243		

–a - 5 cells (41.7%) have expected count less than 5. The minimum expected count is .30. |

Source: Primary data

The value of test statistics is 4.389. Hence, in this case, *p= 0.624.*

The value *p* is associated with chi- square value and is more than 0.05 (the significant value). Hence, it shows the acceptance to the NULL HYPOTHESIS, which means there is no association between educational qualification and the awareness of social engineering attacks. Educational Qualification is independent of social engineering attacks.

Table 10: indicates the relationship between the Usage of Internet with the social engineering attacks

Chi-Square Tests	
Test	**Value**
Pearson Chi-Square	7.502
Likelihood Ratio	7.238
Linear-by-Linear Association	2.303
N of Valid Cases	243

-a- 7 cells (43.8%) have expected count less than 5. The minimum expected count is .33.

Source: Primary data

The value of test statistics is 7.502. Hence, in this case, *p= 0.585.*

The value *p* is associated with chi- square value and is more than 0.05 (the significant value). Hence, it shows the acceptance to the NULL HYPOTHESIS, which means there is no association between Usage of the internet and the awareness of social engineering attacks. Usage of the internet is independent of social engineering attacks.

Conclusion

While working online, one needs to be extra cautious these days as sometimes it is an easier task to save oneself from a hacker but it is very difficult in case of social engineering attacks. With the help of various hypothesis testings through chi square test it can be concluded that –

1. Employees, working in Delhi & NCR are very likely unaware of social engineering attacks. Awareness programs for social engineering are very much recommended for them.

2. Although few employees are a bit aware of social engineering attacks, but these attacks are countable on fingers of which they are aware of. To give such employees more alertness, organizations are required to promote awareness programs from subject experts. That seems the only method to reduce social engineering attacks.

3. The employees who are young were found to be more aware of the social engineering attacks in comparison to senior employees of the organization. Rest of the demographic factors (gender, education level and Internet usage) do not show any specific difference.
   As the social engineering attacks are rising day by day, it is essential for people to get acquainted with these techniques to save themselves. This research work focused on those specific parameters which affect employees' security practices.

   The study revealed that knowledge of safety measures and social engineering attacks, both are required for safety of all employees. Hence, the organizations should make the necessary arrangements to conduct training sessions to increase the awareness of the employees.

   Organizations should arrange interactive executive development programs by experts to increases the awareness of the employees about what all kind of techniques a social engineer may use to befool them. Establishing stronger organizational policies for security also help the organizations to fight against social engineering attacks and save the employees.

References:

1. Aldawood, H. and Skinner, G. Contemporary Cyber Security Social Engineering Solutions, Measures, Policies, Tools and Applications: A Critical Appraisal. International Journal of Security (IJS), 10, 1 (2019), 1.

2. Aldawood, H. and Skinner, G. Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues. Future Internet, 11, 3 (2019), 73.

3. Albladi, S. M. and Weir, G. R. User characteristics that influence judgment of social engineering attacks in social networks. Human-centric Computing and Information Sciences, 8, 1 (2018), 5.

4. Aldawood, H. and Skinner, G. Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review. City, 2018.

5. Airehrour, D., Vasudevan Nair, N. and Madanian, S. Social Engineering Attacks and

Countermeasures in the New Zealand Banking System: Advancing a User-Reflective Mitigation Model. Information, 9, 5 (2018), 110.

6. Ahmad, S. Social Engineering Techniques Contrast Study. International Journal of Engineering, 9, 1 (2017), 105-110.

7. Breda, F., Barbosa, H. and Morais, T. Social engineering and cyber security. City, 2017.

8. C, A., Adesegun, O., Y.A, A. and Oludele, A. Social Engineering Attack Awareness: Case Study of a Private University in Nigeria, 2013.

9. Chan, H. and Mubarak, S. Significance of information security awareness in the higher education sector. International Journal of Computer Applications, 60, 10 (2012).

10. Daimi, K. Computer and Network Security Essentials, 2017.

11. Kumar, A., Chaudhary, M. and Kumar, N. Social engineering threats and awareness: a survey. European Journal of Advances in Engineering and Technology, 2, 11 (2015), 15-19.

12. Salahdine, F. and Kaabouch, N. Social Engineering Attacks: A Survey. Future Internet, 11, 4 (2019), 89.

13. Sharma V., Manocha T. Cyber Crimes- Trends and Awareness: A Study on Youth, International conference ―Managing Business Enterprises: Issues and Challenges", Feb 2020.

14. Snyder, C. Handling human hacking: creating a comprehensive defensive strategy against modern social engineering (2015).

15. Team, C. I. T. Unintentional insider threats: Social engineering. Software Engineering Institute (2014).

16. Yunos, Z., Ab Hamid, R. S. and Ahmad, M. Development of a cyber-security awareness strategy using focus group discussion. IEEE, City, 2016.