THE ASIAN BULLETIN OF BIG DATA MANAGMENT
Vol. 4. Issue 4 (2024)
https://doi.org/ 10.62019/abbdm.v4i4.270

Psychology Behind Social Engineering: Importance of Training/Awareness

Muhammad Sajid Iqbal, Ahthasham Sajid *, Saqib Rasheed, Syed Bilal Ahmed, Muhammad Usman, Hadia Khatoon

Chronicle

Article history
Received: December 1, 2024
Received in the revised format: December 15, 2024
Accepted: December 20, 2024
Available online: December 30, 2025

Muhammad Sajid Iqbal, Dr. Ahthasham Sajid, Saqib Rasheed, Syed Bilal Ahmed, Muhammad Usman & Hadia Khatoon are currently affiliated with the Department of Information Security and Data Science, Riphah Institute of Systems Engineering, Rpihah International University, Islamabad, Pakistan.
Email: sajidiqbal5106@gmail.com
Email:ahthasham.sajid@riphah.edu.pk
Email: caqib14@gmail.com
Email:itssyedbilalahmed@gmail.com
Email: usman.s@outlook.com
Email: hadiakhokher421@gmail.com

Corresponding author*:
ahthasham.sajid@riphah.edu.pk

Keywords: Education, Social Engineering, NIST.

Abstract

The article analyses social engineering attacks, considering legitimate approaches to them. As a form of survey method, user strategies to combat social engineering were evaluated. Along with the above, users' trust in the estimation of potentially hazardous situations and the degree of persuasion targeted by attackers who make use of social engineering were also measured. It was found among the most critical aspects that trust, greed, empathy and feeling in haste are effective tactics whilst many people simply delete or do not care to verify unsolicited emails. This study adopted a mixed-methods attempt to explore the psychology behind social engineering and the importance of training and awareness across various professions and demographic levels. The primary aim is to identify which professions and age groups are more susceptible to social engineering attacks.The need for adequate education, policies, and technologies to combat social engineering is recommended. Besides, the importance of cyberpsychology in developing cyberspace security strategies in businesses is highlighted, which makes them more immune to increasing social engineering attacks.

INTRODUCTION

The global society is transforming into a digital society because human dependency on technologies and dependency of technology and humans on IT is constantly multiplying. This dependency is adding a flavour of ease and facility in human life but at the same time, the same technology and easy access to it have increased threats of privacy breaches, loss, and leakage of sensitive pieces of information. Information Security as a discipline devise and educates such procedures and pieces of knowledge that can be effective in making the world of information sciences more secure. NIST defines Information Security as "protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to violate integrity, confidentiality, and availability" (NIST, n.d.). The custodians and owners of information try to keep it safe from unauthorized access and unauthorized alteration and they also try to ensure its availability when required. But sometimes they may fail in their objectives and efforts to keep the data and information safer because of the malicious actors. The malicious actors or the attackers make use of several techniques, tactics, and technologies to exploit the information systems. Most information systems make use of software that cannot be

perfectly safe from all vulnerabilities. However, another weaker aspect of information systems is the humans who can be exploited by malicious actors, even humans are considered "the weakest link in any organization's cybersecurity chain" (Mifsud, n.d.). Humans in information systems can be exploited through social engineering. IBM defines social engineering in the following words, "Social engineering attacks manipulate people into sharing information that they shouldn't share, downloading software that they shouldn't download, visiting websites they shouldn't visit, sending money to criminals or making other mistakes that compromise their personal or organizational security" (IBM, n.d.). The baseline of social engineering is human psychology as human instincts, motivations, needs, fears, etc. are the vectors through which exploiters succeed in cracking the human firewall. Therefore, while attempting to secure individuals as well as organizations in terms of data and sensitive information it is necessary to train and educate humans to make them foolproof to the maximum level. "Implementing regular training programs and simulated attacks can enhance employee awareness and resilience against social engineering threats" (Ruoslahti, 2024).The primary objective of this research is to explore psychological factors that are exploited by malicious actors while they try to target sensitive information including personal data, authentication credentials, and financial information. The research will explore the most exploited cognitive triggers and the strategies of the exploiters. The research will also investigate the specific conditions like awareness, training, specific professions, and specific age groups when the chances of such exploitation are more likely to succeed. Based on the research the best practices will be sought out and suggested to make the organizations and individuals immunized against the attacks of social engineering.

Scope and Significance

There are more than several important facets of this research. Firstly, it is a multidisciplinary approach as it involves cybersecurity, psychology, sociology and organizational behaviors which may mitigate the chances and resultant consequences of social engineering attacks. The study will consider the effect of professional background on being resistant to social engineering. Demographic segmentation will also be considered to find if people of certain age groups are more resistant or more susceptible to social engineering. The research is significant in the sense that the findings of the study may help policy developers and security in-charges enhance the security posture of their organizations and their employees. The study will also help improve the security culture across the organizations by exploring the value of training and awareness plans. Based on the research the training programs can be tailored and improved to enhance their effectiveness.

LITERATURE REVIEW

The landscape of cybersecurity is expanding as speedily as the dependency of machines, humans, and organizations is increasing on internet-based systems. The world of the internet is susceptible to several threats of which social engineering is of prominent weight as it involves the weakest segment in cybersecurity i.e. humans. As human psychology is exploited in social engineering, therefore, theories related to psychology and social psychology will also be referred to and analyzed for a better understanding of social engineering.

Overview of Social Engineering

Social engineering as a term was first mentioned in 1894 by an industrialist named J.C. Van Marken who was of Dutch origin. When he suggested that just like handling technical challenges; specialists are required to handle human-related challenges (CompTia, n.d.). However, some scholars trace the origin of social engineering far back in history as they consider the incident of the Trojan Horse gifted to the people of Troy as an example of the first recorded example of social engineering that took place in 1184 B.C. (Mitnicksecurity, n.d.). Apart from the debate of tracing its first instance; no doubt in various forms it " has existed throughout history and will continue to exist" (Zuoguang Wang, Limin Sun & Hongsong Zhu, 2020). In social engineering attacks, the attackers target to manipulate humans, in other words it is like hacking humans through various ways. The most common of such attacks are phishing attacks (Kaabouch, 2019). Through these tactics, the targets are deceived to reveal information that they would not and should not. The attackers may use links sent through phishing emails to achieve the desired objectives. The process can be easily understood with the following graphic sketch.

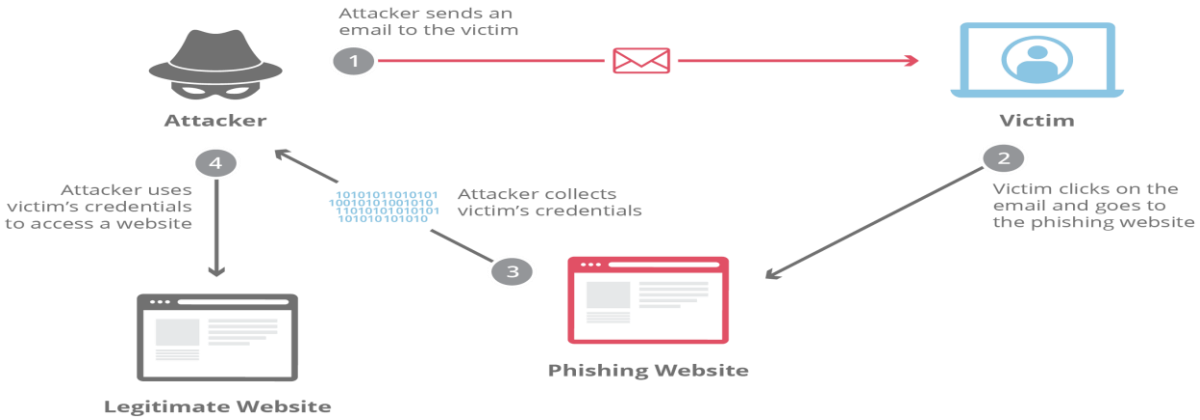

Figure 1.
Phishing Attack: ***(CLOUDFLARE, n.d.)***

Another very common attack is pretexting where fake scenarios are created through which the victims are attracted and made to reveal sensitive information. An example of pretexting is creating fake job offers; the attackers may advertise attractive packages with minimum requirements of qualification and experience and the applicants easily reveal their PII to the attackers. The baiting attacks are performed through free gift offers and the victims click the links. Removable media like USBs are also used in these techniques and any victim who plugs in the compromised USB into the computer may result in compromising the computer or system and sometimes the whole network too.

Psychological Theories Relevant to Social Engineering

In social psychology, persuasion is a process in which one person or a group tries to change the behaviour and or belief of a person or a group of people. The Encyclopedia Britannica mentions that in persuasion, people are influenced through communication without using force. According to Elliot Arranson and others: "one person intentionally attempts to alter another person's behaviour or attitude" (E. Aronson, D. Wilson, M. Akert & R. Sommers, 2016).The current era is an age of mass and social communication, which makes persuasion easier and more widespread as more and more individuals can be targeted through the use of social media tools. The theorists working in the field of Social Psychologists have explored the psychology behind persuasion. Understanding these concepts will help understand which

psychological aspects make people fall victim to social engineering. For example, Richard Petty and John Cacioppo proposed ELM i.e. Elaboration Likelihood Model, in which arguments and evidence are used to make others do something desirable. Emotional appeal, attractiveness and credibility are also used to convince others. The ELM is a very effective tool in understanding the process of an individual's attitude changes (Pei Liu, Michelle Segovia, Eliza Ching-Yick Tse & Rodolfo M. Nayga, September 2022). To change someone's behaviour, social proof is another psychological tool. The concept was proposed by Robert Cialdini, who said that people get influenced when they observe others doing something they will try to follow others, especially when they are in a mental condition of uncertainty. "Social proof in social engineering, particularly during vishing attacks, involves leveraging the behaviour or opinions of others to influence victims." (Keith S. Jones, Miriam E. Armstrong, McKenna K. Tornblad, Akbar Siami Namin, 7 December 2020).

A research conducted by Rosana Montañez et al emphasized the importance of cognitive bias in social engineering. Cognitive bias is deviation from normal behavior as a result of systematic thought processes when an individual starts creating his/her own reality which is mostly subjective and originates from specific inputs which can be deliberate in the part of cyber attackers. The researchers argued that factors like workload, stress and constant condition of vigilance can influence the cognitive patterns of humans and consequently can influence the decision-making of the targets as desired by the attacker because in a stressful situation, the individual will drift to a decision which may bring gratification instead of the final outcome. Culture and especially workplace culture can also enhance the feasibility of attacks in such conditions (Rosana Montanez, Edward Golob & Shouhuai Xu, 2020). Along with cognitive bias people may also get victim of authority bias. Authority bias is a situation in which people do undesirable actions because the opinion of an authority is supposed to be more accurate then their own. And such tendency makes people do something without critically evaluating the opinions of the authorities. The article "A Novel Hybrid Approach of SVM Combined with NLP and Probabilistic Neural Network for Email Phishing" presents a comprehensive study on enhancing phishing detection methods using a hybrid model that integrates Support Vector Machine (SVM), Natural Language Processing (NLP), and Probabilistic Neural Networks (PNN). This study conducted a quantitative research on the topic and concluded that it is hard to find what are the real causes behind the impact of phishing attacks on individuals may be because it is very subjective matter "the exact job of different message-explicit elements, including how and why they impact individuals' decisions and choices, stays hazy" (Abhishek Kumar, Jyotir Moy Chatterjee & Vicente García Díaz, 2019).

Xuan Liu et al also worked objective on the topic of social engineering, they researchers worked on a dataset of emails comprising of 1,705 emails was used for training and testing, of which 1,291were legitimate emails and 404 had phishing intents. Detecting such content in the emails is not quite easy as strategies of the attacks are always changing and current detection systems have inherent limitations, detecting phishing emails poses a number of important obstacles because of the use of the new IT technologies like generative AI in creating phishing emails. Along with phishing email there are phishing websites as well which also pose a significant threat to the vulnerable targets and this aspect of social engineering is crucial too because "phishing websites are common entry points of online social engineering attacks, including numerous frauds on the websites" (Abdul Basit, Maham Zafar, Xuan Liu, Abdul Rehman Javed, Zunera Jalil & Kashif Kifayat, 2021).

Ahmed Baiomy et al in a research mentioned that financial sectors, retails and cloud computing are the targets of social engineering with a view to steal critical credentials. They found that previously, the emails were the major source of disseminating phishing URLs but currently other social media platforms have made the targets more accessible to the attackers so they use Facebook and Twitter etc. to send malicious links. This research like the current study also the students of various age groups as a sample for studying the level or demographic group of the respondents and their ability to find notice phishing intent of the sender. In this study the respondents were trained with the help of certain games which increased their understanding of the phishing contents. The results of the study indicated that awareness training through games was effective. Following is the table compiled by this study:

Table 1.
Tests results classified by participants' demographics

	Pre-test					Post-test				
	Minimum	Maximum	Average	STDV	Average confidence	Minimum	Maximum	Average	STDV	Average confidence
Gender										
Male	5.5	8.5	6.91	0.81	3.68	7.5	10.0	8.79	0.70	4.54
Female	5.0	8.5	6.89	0.90	3.63	7.0	10.0	8.75	0.69	4.51
Education and age										
High School (15–18)	6.0	8.0	7.00	0.71	3.76	8.5	9.5	9.07	0.47	4.63
College under grade (19–23)	5.5	7.5	6.57	0.65	3.79	7.5	9.5	8.57	0.65	4.46
Post graduate (24–30)	7.0	8.5	7.79	0.47	3.93	8.0	10.0	9.14	0.60	4.72
Employee (>30)	5.0	7.0	6.25	0.67	3.15	7.0	9.0	8.29	0.67	4.32

The results of the study indicated that awareness training (Ahmed Baiomy, Mahmoud Mostafa & Alyaa Youssif, 2019)

This study elaborated the impact of training on various age groups however, it lacked the psychological factors which may influence how the targets become susceptible to the attackers. The study titled: Anti-Phishing Techniques – A Review of Cyber Defense Mechanisms, ppostulates an overview of diverse anti-phishing approaches and their efficacy in preventing phishing attacks, which have been on the rise due to increasing cyber threats and user vulnerabilities. This work highlighted that phishing attacks get successful largely because of the target's not being well aware of the skills to recognize the malicious contents of the email or messages. The study comprehensively discussed two types of the phishing that is email phishing and spear phishing. For both types, the researchers emphasized on the importance of education and training for making people more protected against the social engineering attacks. Despite the broader overview of the topic, there are several gaps as well. Like the individuals' behavior concerning phishing awareness needs more in-depth investigation. AI is also changing the basic concepts of attacks and preventive measures. "The analysis presented, therefore, concludes with anti-phishing AI techniques being more effective in detecting phishing attacks" (Glăvan, 2020). S. Hawa Apandi et al in a study investigated the topic by segmenting it into two distinct

sectors that phishing prevention and phishing detection, however the study lacked on detailed strategies for ant-phishing solutions. Therefore they suggested that "we can do more research on the academic phishing detection / classification schemes that utilize deep learning to see its potential of accuracy to detect phishing websites" (S. Hawa Apandi, J. Sallim and R. Mohd Sidek,, 2020). Bhagya Bajanthri and Mr. Sayeesh studied the use of redirecting URLs in phishing attacks. The URLS seem to be legitimate but such fabricated and embedded links which may compromise whoever clicks. There are also websites which seem very closes to the legitimate and popular platforms. The victims upload their sensitive credentials on such websites and thus become easier victims of the attackers. The study emphasized that lexical analysis should be done before clicking any link because the malicious URLs cannot be the exact copy of those platform which they are framing. This study also lacked exploration of the user's knowledge/awareness and his/her response when they are asked to click certain URLs. However, it has in-depth study of link-manipulation and site-forgery; "Most methods of Phishing use some form of technical deception designed to make a link in an email appear to belong to the spoofed organization. Misspelled URLs or the use of subdomains arc common tricks used by Phishers" (Sayeesh, 2022).

Durga Parsada in a study noted that The realm of cybersecurity is a hotbed of activity which makes it more interesting because of the more aggressive and advanced threats that already exist. In the research work, the authors attempt to resolve some of these issues associated with advanced persistent threats, so to say, by facilitating the transition from threat detection to automatic responses with the use of artificial intelligence. Their paper revolves around removing the curtain on how organisations can transform their security infrastructure with the use of AI technologies like AI-based detection, advanced threat analytics and the introduction of autonomous response systems. However, the paper has the limitation as it did not mention the drawback of data dependency in the functioning of AI. The effectiveness of AI-based threat detection and responses will depend on the quality of the data on which the AI model for such detections and responses was trained "The rising level of threat posed by cyber adversaries and the relative weakness of conventional safeguards raises great urgency surrounding security needs. This context is affected by evolution of technological advancements, the invention of the internet, and the large-scale distribution of internet-connected devices which have brought in additional weaknesses" (Sanagana, 2024).

Zainab Alkhalil, et al in a research considered the demographic factors like age and awareness level and their influence in being susceptible to the phishing attacks. They found that the impact of different variables on vulnerability to phishing attacks like age, gender, education level, as well as knowledge of the scam. It has been established that older students possess better skills in distinguishing emails that are hoaxes, while students from engineering and IT departments exercise more restraint when it comes to clicking links in unsolicited emails. Additionally, psychological factors such as curiosity and promptness affect how a person interacts with a phisher, as most of the time, a decision is made without proper judgement. Many people possess computers and therefore are able to gain more advanced knowledge with ease. But ironically, those who possess more knowledge about phishing are actually more likely to be attacked; this is primarily due to an overinflated self-perception. Some of the limitations related to the research were the assumptions on which the hypothesis was based. For instance, the students had very limited demographics, thereby reducing

the generalisability of the research. Self-reported phishing knowledge, which was implicit, was also a limitation in the research.

Ultimately, the short existence of phishing websites reduces the effectiveness of all the detection techniques considered in this research. The study also notes that women might stand a higher chance of falling for phishing scams than their male counterparts due to their weaker technological abilities; however, men are more prone to mobile phishing targeting banks. Overall, the results highlight the importance of training and sensitisation programmes for the prevention of phishing attacks. Overall the findings point to the significance of training and sensitization programmes in addressing phishing attacks. (Zainab Alkhalil, Chaminda Hewage, Liqaa Nawaf & Imtiaz Khan, 2021)

Research Methodology

This study adopted a mixed-methods attempt to explore the psychology behind social engineering and the importance of training and awareness across various professions and demographic levels. The primary aim is to identify which professions and age groups are more susceptible to social engineering attacks. A combination of qualitative and quantitative methods was employed to ensure comprehensive analysis and reliable findings.A structured survey was designed to collect quantitative data on the vulnerability of different professions and age groups to social engineering attacks. The survey consisted of:

i. **Demographic Questions:** To gather information on respondents' age, gender, profession, and educational background.

ii. **Knowledge Assessment Questions:** To assess respondents' understanding of social engineering techniques and related cybersecurity concepts.

iii. **Behavioral Questions:** To evaluate the likelihood of respondents falling victim to various types of social engineering attacks (e.g., phishing, pretexting, baiting).

Target Population

The target population for the survey included individuals with an IT background, as they are more likely to encounter social engineering attacks in professional settings sometimes for protecting their organizations and sometimes to protect themselves. Respondents were selected from diverse professions, including IT support, software development, cybersecurity, management roles or at least studying in related fields.

Sampling Technique

A purposive sampling method was employed to ensure the participation of individuals who have the requisite IT knowledge. The survey was distributed through professional networks, email invitations, and social media platforms targeting IT professionals.

Data Collection

Data was collected using a Google Form survey, which was distributed over a four-week period. Participation was voluntary, and anonymity was maintained to encourage honest responses.

Literature Review Methodology

The literature review was conducted to provide a theoretical foundation for the study and to contextualize the survey findings. The following steps were undertaken:

1. **Database Search:** Academic databases such as IEEE Xplore, PubMed, and Google Scholar were used to search for relevant literature.

2. **Inclusion Criteria:** Articles published within the last five years, focusing on social engineering, psychology, and cybersecurity training, were included.

3. **Critical Analysis:** Selected articles were critically analyzed to identify recurring themes, gaps in research, and practical implications for various professions and demographics.

To keep the analysis apprised with the newest tendencies and requirements only the works issued after 2019 were considered. The table below carries a summary of spme of the works that were studied for this study:

Topics	Writers
Exploiting the Human Factor: Social Engineering Attacks on Cryptocurrency Users	Kristin Weber, Andreas E. Schütz, Tobias Fertig and Nicholas H. Müller
Phishing Attacks: A Recent Comprehensive Study and a New Anatomy	Zainab Alkhalil, Chaminda Hewage, Liqaa Nawaf and Imtiaz Khan
Cybersecurity: Risks, vulnerabilities and countermeasures to prevent social engineering attacks	Nabie Y. Conteh and Paul J. Schmick
ExplainableAImethodsincyberriskmanagement	PaoloGiudici EmanuelaRaffinetti
Phishing Attacks Survey: Types, Vectors, and Technical Approaches	Rana Alabdan
Harnessingh AI for Evolving Threats: From detection to Automated Response	Durga Prasada Rao Sanagana
The evolving techniques of the social engineering of extraction	Judith Verweijen and Alexander Dunlap
A comprehensive survey of AI-enabled phishing attacks detection techniques	Abdul Basit, Maham Zafar and Xuan Liu2
Anti-Phishing Techniques -A Review of Cyber Defense Mechanisms	Pawankumar Sharma, Bibhu Dash, Meraj Farheen Ansari

DATA ANALYSIS

The survey form was circulated online and103 individuals responded by filling that form. A descriptive analysis of the data collected through the survey is presented with the help of charts and graphs. The analysis and statistics of the collected data are as follows: Various age groups participated in the survey. Participation of various age groups helped in understanding that the attack and the importance of awareness training is not limited to any specific age group, rather everyone who is online and using any connected gadget can be the target and victim of the social engineering attacks.

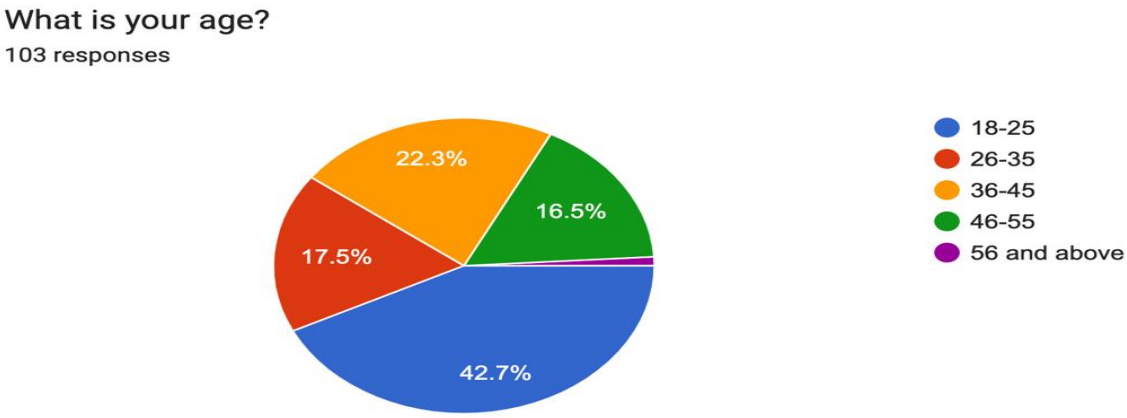

Figure 2.
Age groups of the Respondents

The responses collected were also inquired about their education levels. The responses returned from various qualification levels maintained that like for different age groups, the vulnerabilities for educated people and the need of training for them is same.

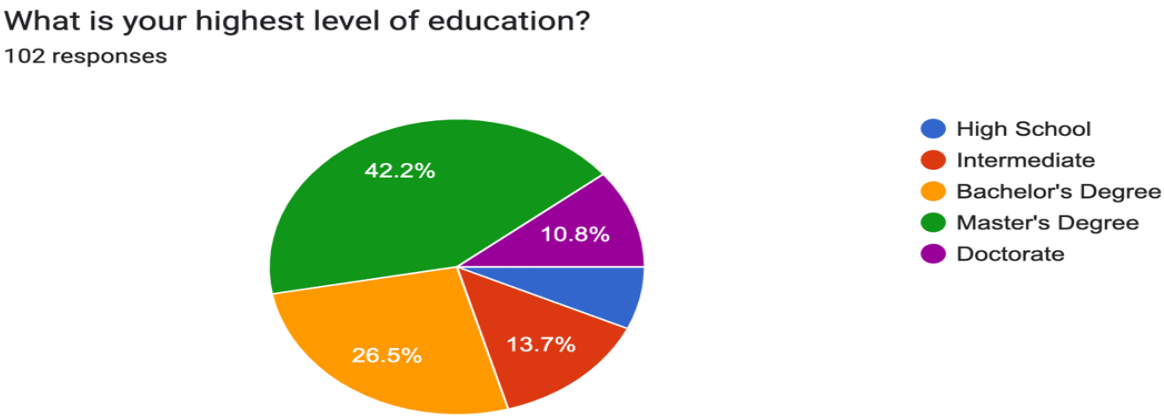

Figure 3.
Qualification Levels of the respondents

As shown in the below figure, apart from various education levels, the responses from various professionals related to IT were also collected. If the respondents were not doing some job related to IT, they were at least studying information technology or information security. The responses from such professionals also indicated that the awareness and training programs were equally valuable and necessary for them to keep them safer in their individual as well as professional lives.

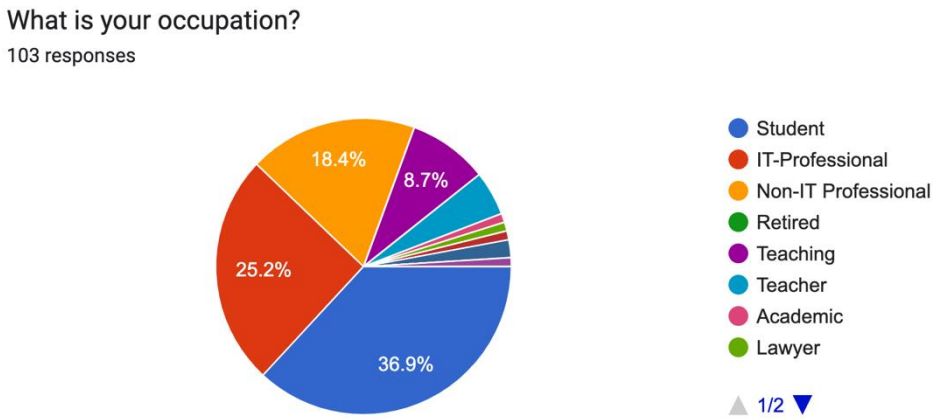

Figure 4.
Occupations of the Respondents

The given below graph is the calculation of the connected devices world-wide. Just with in 10 years the number doubled. However, as evident from the graph, the speedof this growth also increased in 2018 and onwards. The number of online connected devices is constantly on the increase. Various platforms show that there are about 30 billion devices connected to the internet and this number will rise up to 34.2 billion in the year 2025 and number of internet user all over the world are calculated in 2024 to be about 5.52 billion (Oberlo, n.d.).

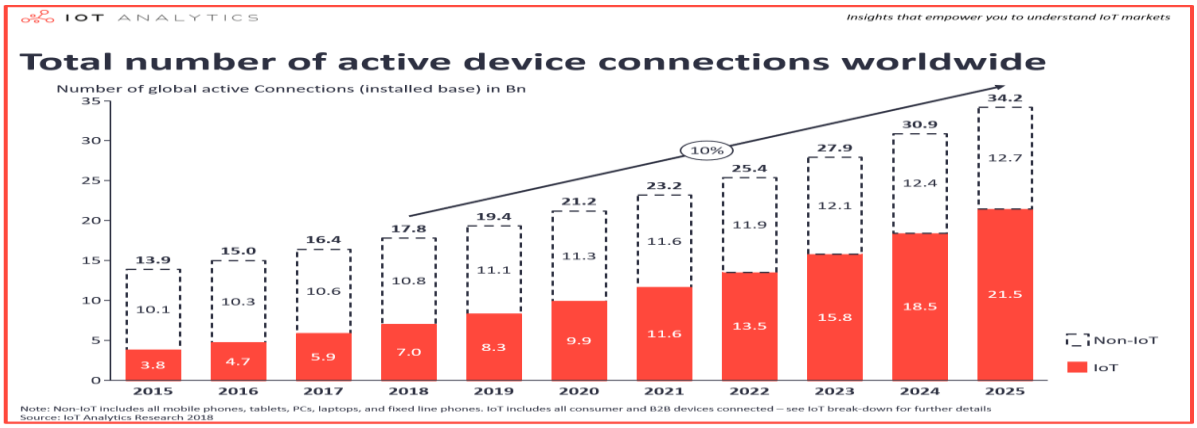

Figure 5.
Total number of connected devices (Analytics, n.d.)

The number of connected devices and user is constantly multiplying however awareness about online security is not as coomon. The rresulst of the sury as shown with the help of the Figure no. 06 indicate that amongst this huge number of direct and indirect users of internet, only 10 per cent of people are well aware of the online security issues. Fifteen per cent of people admitted that they had no idea of such issues. 33 per cent of respondents claimed that they were slightly aware of cyber security while 39 per cent claimed that they were familiar with such issues to a considerable extent.

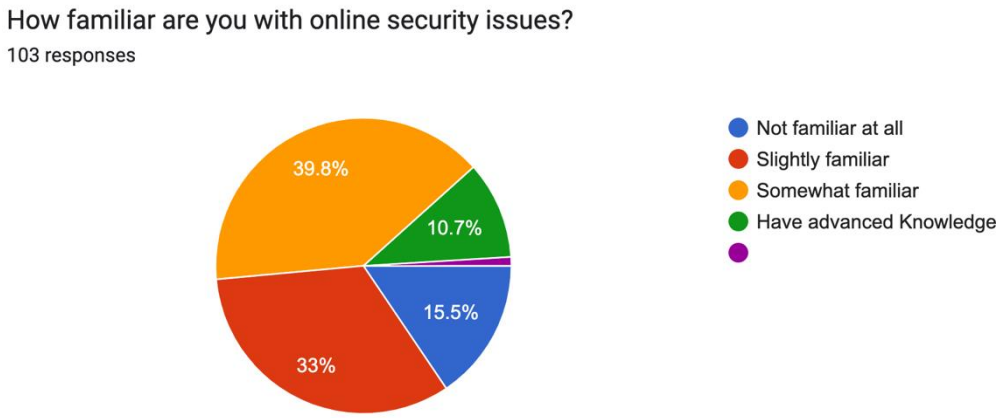

Fig 6 Familiarity with Online Security Issues

While only 10.7 percent people claimed that they had advance knowledge of online security issues, according to the survey as shown in the given below figure no 7, only 23.3 per cent acknowledged that they had gone under awareness/training sessions but mor than 76 per cent people did not receive any such training. This number again emphasises that there is an immense need to arrange training and awareness sessions for the people working in various organizations. Apart from the workers, there is a large number of people who do not work in any organisation still they are the heavy users of the internet and connected devices.

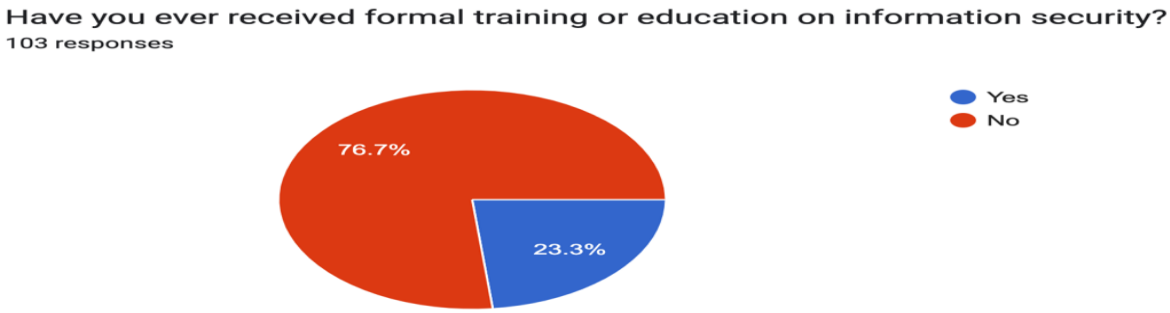

Figure 7.
Ratio of Formally Trained and Untrained Respondents

According to the obtained survey results, close to half of the interviewed persons (48.5%) have been victims of social engineering or online fraud schemes including phishing or baiting. This shows that phishing and baiting are very common and stresses the need for strong security measures and education. On the other hand, 51.5% declared that they had never been the targets of such attacks, this claim might have been due to lesser exposure or being unaware of having been a target. The results indicated below also emphaise the dire need for preparedness, education and alertness so that the people become more aware and trained to deal with the evolving online frauds.

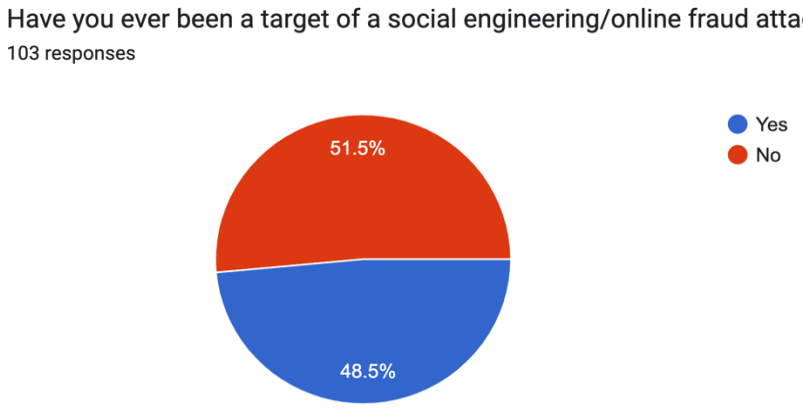

Fig 8 Respondents who admitted to be the target of cyber attacks

This study especially recorded the responses of the common on what kind of attacks do they commonly come across. There are various tactics applied by the attackers to succeed in their malicious designs of deceiving the people e.g. the targets may receive phishing emails or messages. They may be targeted through false identity. Gifts and surprisingly low prices for valuable things or services are also offered. The below chart Figure no 9, graphically indicates the most common types of tactics utilized by the attackers. According to the survey the most respondents (about 37 percent) revealed that were targeted through fishing emails 35 per cent mentioned that they were offered gifts while a considerable number were also targeted through pretexting ie false identity.

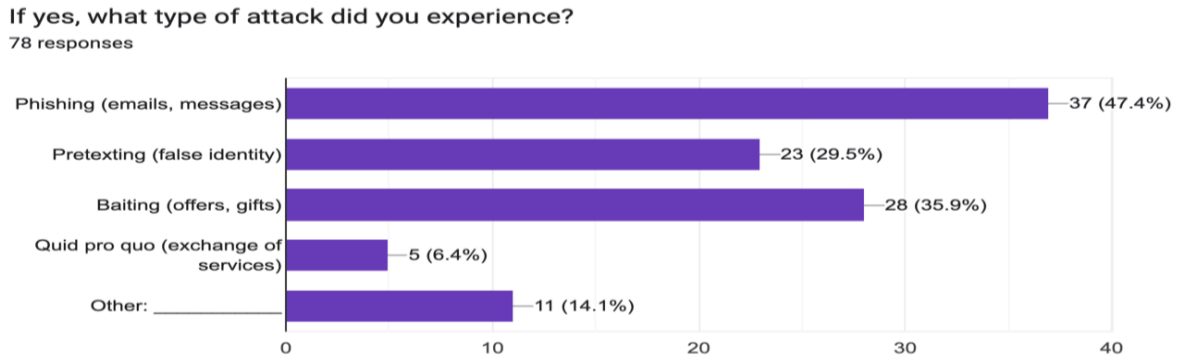

Figure 9.
Methods applied by the Cyber Attackers

Social engineering is part of social interactions and carries out those actions. But, more than half of the respondents, as much as 53.1 percent, simply did not respond to the attack. This could indicate that the victims have no perception of any potential threats, or that the fact of the violence itself does not matter to them. Nevertheless, 32.7 percent of the respondents on the other hand self-reported the violence, which is quite reassuring in terms of the willingness of these actors to take proactive response and seek preventive measures against such incidents. In the same vein, 5.1 percent of the victims of this type of assault note that such people should enhance their knowledge and readiness to confront social engineers' tactics. Such data also serve as the grounds for the active defense approach – a willingness to take actions to

prevent such aggressions and ensure the occurrence of reporting on such aggressions.

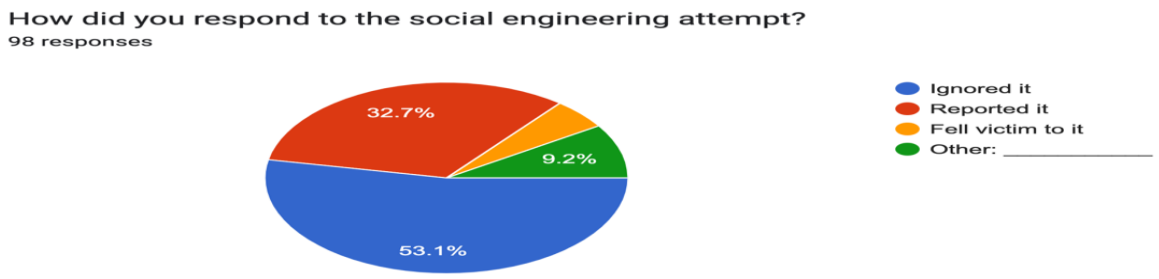

Figure 10.
How do People Respond to Cyber Attacks

The research on the confidence of self-identified social engineers and online fraudsters demonstrates a rich diversity in how the participants assessed their abilities. However, 7.1% pledged to full disheartenment, stating it qualifies to a level of 1, emphasising an inability. A further 13.6% planned to rise above the self-esteem gauge but could manage to sit at a level of 2. Most prominently, the major group resting at a level of 3, constituting a large 34% range, are those quite optimistic about their skills to begin with, however sitting at a dormant stage of potential waiting to be triggered. The combined population rate shrinking to 44.7% of the inhibition elbow, showing greater confidence levels perhaps resting at 4 or 5 on the gauge. These results showcase the importance of higher education and ongoing training for those inclined to be on the lower end of the scale of confidence and augmenting the skill set for those who appear to be fairly confident.

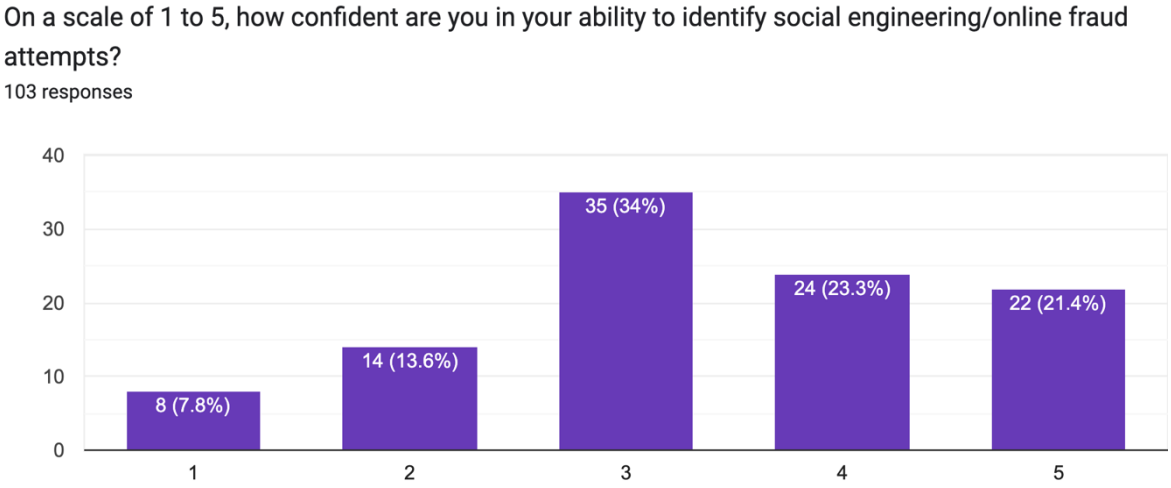

Figure 11.
Awareness Level of online Security Issues

The results of the poll indicate that Trust and Empathy (50.5%) are regarded as the most effective psychological weapons in social engineering attacks, thus demonstrating the extent of emotional manipulation in reducing the ability to defend oneself. Greed and Curiosity (44.7%) and Fear and Urgency (35.9%) are also high, suggesting that human instinct as well as fear can be used to manipulate behaviour.

Social Proof (39.8%) and Authority (32%) further show the role of social proof and authority respectively in shaping the behaviour of the victim. Commitment and Consistency (18.4%) and Reciprocity (10.7%), among others, are less potent but nevertheless strengthen one's innate predisposition to meet obligations to do so or to do something in return. These insights emphasise the need for specific awareness and education in order to counter such many and very effective psychological employs.

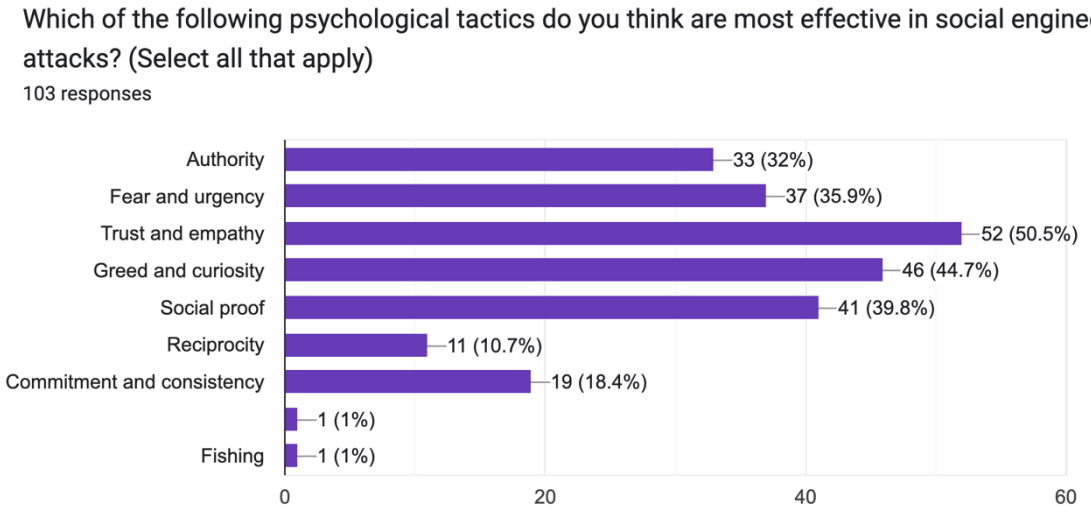

Figure 12.
Psychological Tactics Used for Manipulation

As shown in the below figure (no.13) the respondents answered questions in a way that shows that nearly 44% of people only check the email address or phone number of the recipient of an unwanted message as a way of verifying the identity and authenticity of the sender while 33.7% simply do not respond to the notice. It should be noted, however, that only 10.9% of individuals actually bother to ring the organisation or the sender; this is highly advisable but much less practised. While analyzing the fake emails it was noted that such emails may have linguistics errors and generic addressees. "Studies show that phishing emails frequently contain errors in capitalization, punctuation, and word forms, with 100% of analyzed Philippine phishing emails exhibiting such mistakes" (Cardona, 2024). Surprisingly, 7.9% think bad spelling in a message probably means it is fake, and this can be easier but still helpful. The 4 per cent answering Other have this idea in mind as well and are assumed to have various unreported strategies. All these examples point to the conclusion that there has to be proper guidance so that social engineering attacks could be better dealt with. "Social engineers often utilize principles such as reciprocity, commitment, and social proof to influence targets" (Lance, 2022). Some researchers emphasized the role of greed in being the target of social engineering attacks, "Attackers leverage traits like naivety, greed, and curiosity to manipulate individuals into divulging sensitive information" (Ganchenko, 2022). An other researcher asl concluded similar results when he found that "Scam emails often include misspellings and poor formatting, contrasting with the polished presentation of legitimate emails" (Sophomore T. Vacalares, Brian Paul E. Sta. Ana, Daryl Q. Dranto & Jinky S. Gallano, 2024).

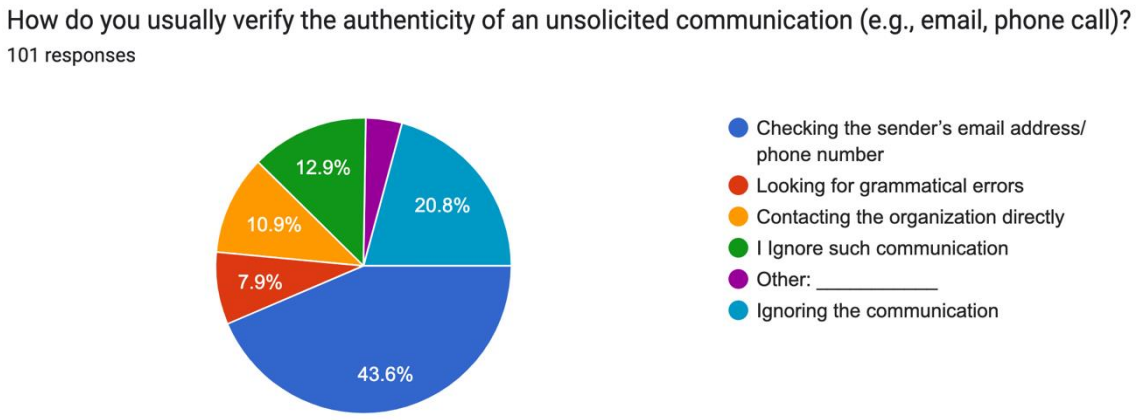

Figure 13.
How do people Respond to Phishing Attacks

The adherence rates to the security policies as well as the support that is extended to these policies, have been found to be on some level in conflict as shown in the below chart by the survey findings. 23.3% in total, which combines roughly 5.8% of the Very Unlikely Sample and 17.5% of the Unlikely Sample, do add to the statistic of employees who do not engage in these practices or do not have faith in their importance. It is quite shocking that 29.1% of the respondents in the survey believe that guidelines for security have not been issued irrespective of the organisation's purpose; this indicates a serious flaw in the overall cybersecurity culture and training of the organisation. But on the bright side; 37.9% of the respondents opined that they are likely to adhere to the guidelines, hinting at the fact that not all organisations that do not give proper understanding are out of compliance. The results of the survey indicate that companies and organizations should form and outline the policies alongside implementing them such that greater improvement is made on the security of the organisation.

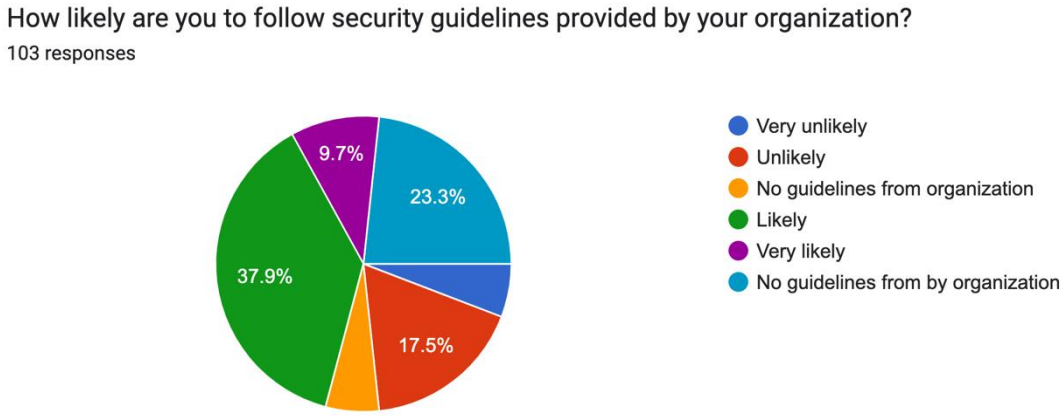

Figure 14.
Do People Follow Security Guidelines?

The survey responses regarding the measures to increase protection from online security breaches especially when humans are the target of such attacks through

social engineering, display a fair perspective of both human and technological measures. More Security policies (28.4%) are among the most effective undertakings, which implies that there is an understanding of the importance of having strong frameworks to ensure that safe behaviours are followed. Better technological solutions (23.5%) equally rank well, underscoring the need to incorporate sophisticated technologies in mitigating social engineering attacks. Increased awareness campaigns (25.5%) mean that there is a need for ongoing education and appropriate awareness sessions to be arranged in order to create a more alert and safer population. More frequent sessions for refresher training (20.6%) point out the significance of hands-on experience learning that reinforces ideal practices. These findings suggest that a multi-level approach that includes policy, education, and advanced technology is critical in reducing the risk of social engineering. "Understanding the psychological tactics used in social engineering is crucial for developing effective countermeasures" (Siddiqi, 2022).

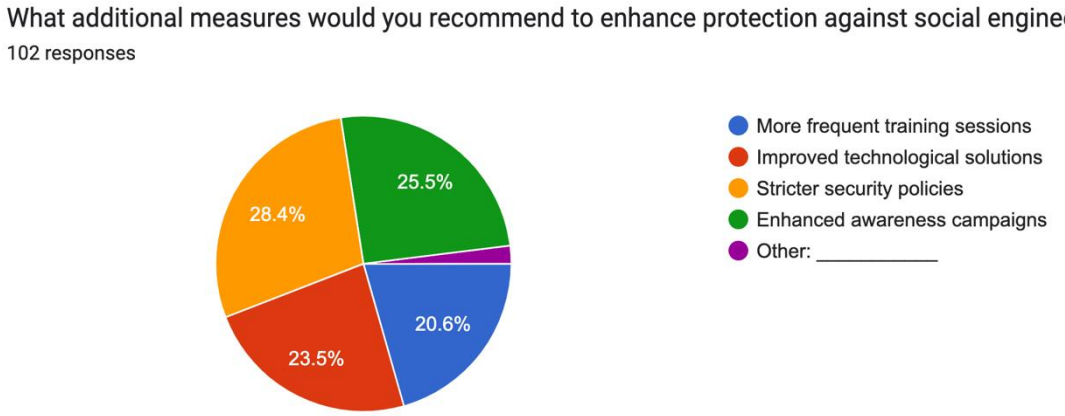

Figure 15.
Additional Measures Suggested by the People

Figure no 16 as shown below speaks of the importance of understanding psychological vulnerabilities.

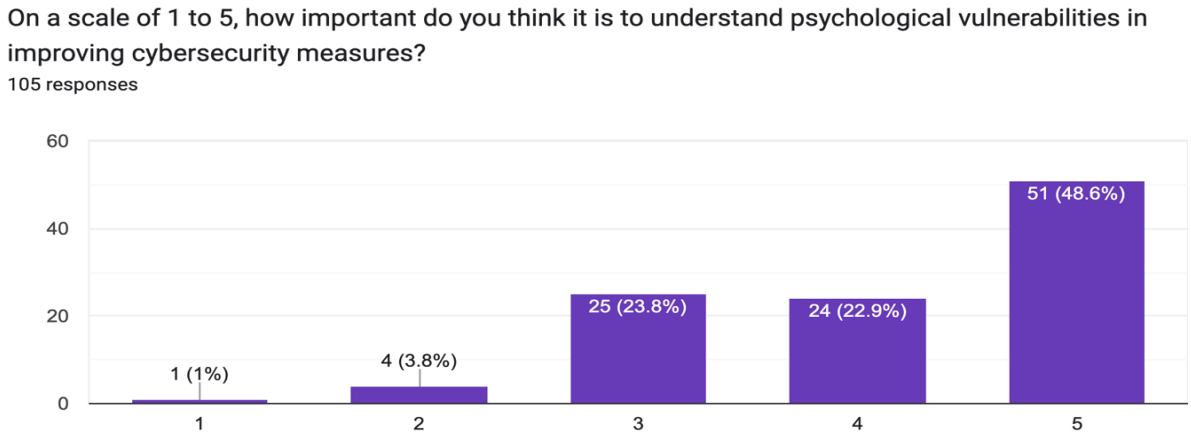

Fig 16.
Importance of Understanding Psychological Vulnerabilities

The survey shows that the majority of the participants are in agreement on the necessity to address psychological factors in order to enhance cybersecurity measures. A major portion of the respondents i.e. 48.6% of the sampled, rated this understanding as 5 on the importance scale (zero to 5), which is evidentially wide support for the overwhelming significance that psychological considerations have for cybersecurity. At the same time, 22.9% rated it as 4, which once again highlights its significance. A large 23.8% and 3.8% rated it as 3 and 2 respectively, insinuating that the understanding is of moderate to low importance to some people. A mere 1% rated it as 1, signifying minuscule importance. These results indicate very explicitly that most of the respondents are aware of and seek solutions for psychological vulnerabilities as a requisite for enhancing overall cybersecurity. Understanding social engineering is crucial in strengthening organizational cybersecurity and protecting sensitive data. Social engineering exploits human weaknesses which means that employees need to be able to identify and respond to potential threats. The following sections outline the importance of awareness in countering social engineering attacks. "Targeted awareness training significantly improves employees' ability to identify phishing attempts and other social engineering tactics, particularly in high-risk sectors like finance" (Ayoola, 2024).

CONCLUSION

The results of this survey assist in enhancing the understanding of the relation between psychological tactics used and the social engineering aspects which can be improved, so as to strengthen the control measures for abuse of the system. As Social Engineering attackers are actively developing means of social engineering attacks, participants in the survey were deliberately chosen from different age, educational and occupational backgrounds, which emphasized the ubiquitous nature of the problem and the ways of dealing with it. What caught the attention the most, was the difference between participants' degree of knowledge of subjects such as social engineering along with familiarity of other security concepts. While some said they understood social engineering, quite a number of them said they knew nothing of it. This clearly underscores the need for campaigns targeted at education and training, especially among the younger generation and non-IT workers who stand to be more vulnerable because of inadequate exposure to these ideas.

The survey also found that many of the respondents encountered social engineering, with phishing or baiting being the most common method of attack. Trust, greed, empathy, fear and authority were among the most effective psychological aspects recognised in the attacks, revealing the complexity of the strategies used by the attackers. This suggests the need for two things: educating individuals about such tactics at the individual level and incorporating such psychological aspects relative to the intended audience while developing training sessions for organisational purposes. During the study, it was also noticed that the targets of such attacks mostly ignore such attempts while their reporting could help others recognize such attempts. There also some respondents who claimed to report such interactions as spam.

Despite the fact that several responses have been provided, the differences in these responses highlight the need for standard policies and sound approaches to incident reporting. Furthermore, while some of the respondents believed that they would be able to detect the cases of fraud undertaken against them, this could not be said to be the case, especially where there is no relevant practice. The data also

underscored the importance of institutions in enabling a safe working space. Respondents viewed organizational training programs as fair but, they think, there is scope for improvement. More frequent and scenario-based training sessions as well as awareness campaigns were the proposed solutions to the issues. These measures, together with the instilling of a security culture will provide individuals with the ability to make the right decisions as well as weaken the chances of them being victims of cyber fraud attempts. Another major point from the study that was emphasised is the recognition of psychological vulnerabilities as an essential aspect in relation to social engineering risks and their mitigation. It is essential to understand how and why an attacker targets feelings, cognitive aspects, and psychological weaknesses. In this case, the knowledge should be incorporated into the behaviour of people and into the policies of an organisation in order to develop a framework that is not just technologically comprehensive but also deals with practical issues in relation to cybersecurity. Working in this space reconfirms the claim that there is a need for a comprehensive and psychological approach to tackling social engineering. In the future, attention should be turned towards creating customized training courses, promoting collaboration between psychologists and cyber security specialists, and conducting studies on the prognosis of these measures over time. By doing this, it is expected that there will be substantial improvement in the general capacity of people as well as organizational resistance against advanced persistent threats through social engineering.

DECLARATIONS

Acknowledgement: We appreciate the generous support from all the supervisors and their different affiliations.

Funding: No funding body in the public, private, or nonprofit sectors provided a particular grant for this research.

Availability of data and material: In the approach, the data sources for the variables are stated.

Authors' contributions: Each author participated equally to the creation of this work.

Conflicts of Interests: The authors declare no conflict of interest.

Consent to Participate: Yes

Consent for publication and Ethical approval: Because this study does not include human or animal data, ethical approval is not required for publication. All authors have given their consent.

REFERENCES

CSRC Content Editor. (n.d.). information security - Glossary | CSRC. https://csrc.nist.gov/glossary/term/information_security

Mifsud, F. (2022, September 20). The weakest link in any organisation's cybersecurity chain is employees. Cybergate - Your Cyber Security Partner. https://cybergateinternational.com/blog/the-weakest-link-in-any-organisations-cybersecurity-chain-is-employees/

Ibm. (2025, January 10). What is social engineering?. IBM. https://www.ibm.com/topics/social-engineering

What is social engineering - the human element in the technology Scam| Cybersecurity | CompTIA. (n.d.). CompTIA. https://www.comptia.org/content/articles/what-is-social-engineering

Mitnick Security Consulting. (n.d.). The history of social engineering. https://www.mitnicksecurity.com/the-history-of-social-engineering#chapter-2

Zuoguang Wang, Limin Sun & Hongsong Zhu. (2020). Defining Social Engineering in Cybersecurity. IEEE Access, 08, 85094-85115.

Kaabouch, F. S. (2019). Social Engineering Attacks: A Survey. Future Internet, 11(4).

CLOUDFLARE. (n.d.). What is a phishing attack? Retrieved 07 06, 2024, from https://www.cloudflare.com/learning/access-management/phishing-attack/

E. Aronson, D. Wilson, M. Akert & R. Sommers. (2016). Social Psychology. Boston: Pearson.

Pei Liu, Michelle Segovia, Eliza Ching-Yick Tse & Rodolfo M. Nayga. (September 2022). Become an environmentally responsible customer by choosing low-carbon footprint products at restaurants: Integrating the elaboration likelihood model (ELM) and the theory of planned behavior (TPB). Journal of Hospitality and Tourism Management, Volume 52, Pages 346-355.

Keith S. Jones, Miriam E. Armstrong, McKenna K. Tornblad, Akbar Siami Namin. (7 December 2020). How Social Engineers Use Persuasion Principles During Vishing Attacks. Information and Computer Security, Vol. 29 (No. 2), 314-331.

Rosana Montanez, Edward Golob & Shouhuai Xu. (2020). Human Cognition Through the Lens of Social Engineering Cyberattacks. Frontiers in Psychology, 11.

Abhishek Kumar, Jyotir Moy Chatterjee & Vicente García Díaz. (2019). A novel hybrid approach of SVM combined with NLP and probabilistic neural network for email phishing. International Journal of Electrical and Computer Engineering, Vol. 10(No. 1), 486-493.

Abdul Basit, Maham Zafar, Xuan Liu, Abdul Rehman Javed, Zunera Jalil & Kashif Kifayat. (2021). A comprehensive survey of AI-enabled phishing attacks detection techniques. Systems, 76, 139-154.

Ahmed Baiomy, Mahmoud Mostafa & Alyaa Youssif. (2019). Anti-Phishing Game Framework to Educate Arabic Users: Avoidance of URLs Phishing Attacks. Indian Journal of Science and Technology, 12(44).

Glăvan, D. (2020). Detection of phishing attacks using the anti-phishing framework . Scientific Bulletin of Naval Academy, 1, 208-212.

S. Hawa Apandi, J. Sallim and R. Mohd Sidek,. (2020). Types of anti-phishing solutions for phishing attack. IOP Conference Series: Materials Science and Engineering, , 769(1), 012072.

Sayeesh, B. B. (2022). A Study on Various Phishing Techniques and Recent Phishing Attacks. International Journal of Advanced Research in Science, Communication and Technology, 2(2), 296-302.

Analytics, I. (n.d.). Global number of Connected Devices. (IOT Analytics) Retrieved December 22, 2024, from https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/

Oberlo. (n.d.). How Many People Use Internet. (Oberlo) Retrieved December 22, 2024, from https://www.oberlo.com/statistics/how-many-people-use-internet

Sanagana, D. P. (2024). HARNESSING AI FOR EVOLVING THREATS: FROM DETECTION TO AUTOMATED RESPONSE. Journal of Science Technology and Research (JSTAR), 5(1), 91-97.

Zainab Alkhalil, Chaminda Hewage, Liqaa Nawaf & Imtiaz Khan. (2021). Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. Frontiers in Computer Science, 3.

Lance, W. (2022). Social engineering and the use of persuasion to commit cyber fraud. Cyber Security: A Peer-Reviewed Journal, 6(2), 102-110.

Ganchenko, M. I. (2022). Human psychological and biometric factor in the development and use of social engineering methods in peacetime and wartime. Sučasnij zahist ìnformacìï, 1(49).

Siddiqi, M. A. (2022). A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures. Applied Sciences, 12(12), 6042-6042.

Ayoola, V. B. (2024). Effectiveness of social engineering awareness training in mitigating spear phishing risks in financial institutions from a cybersecurity perspective. Global Journal of Engineering and Technology Advances, 20(3), 94–117.

Ruoslahti, I. T. (2024). Human Factors Make or Break Cybersecurity! Information & Security, 55(3), 245-259.

Cardona, J. (2024). Grammatical Deviations in Philippine Phishing Emails. International Journal of English Language Studies, 124-129.

Sophomore T. Vacalares, Brian Paul E. Sta. Ana, Daryl Q. Dranto & Jinky S. Gallano. (2024). Bank Emails: The Language of Legit and Scam. International Journal of Research and Review, 192-203.