International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 06 | June - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

From Offer to Breach: The Empirical Study on Quid Pro Quo Cyber Attack

Kamalesh S,
Project Guide: Venketesh R,
Msc Criminology and Forensic Science,
Dr.MGR Educational and Research Institute

ABSTRACT

Quid pro quo attacks are a sophisticated form of insider threat where malicious individuals exploit the human element within an organization to gain sensitive information or unauthorized access. Unlike traditional cyberattacks that focus on technical system flaws, these attacks rely on social engineering techniques to deceive people. Attackers often use ransomware, encrypting a victim's data and demanding payment, typically in cryptocurrency, for the decryption key. The term "quid pro quo" highlights the exchange involved, indicating that the attacker seeks something in return for stopping their harmful actions.

To effectively understand and defend against quid pro quo attacks, a comprehensive approach is necessary. The primary goal of this research is to examine how these attacks operate and to propose effective solutions and preventive measures. This will be achieved by studying incidents involving affected victims. The research aims to identify the specific methods used in these attacks, analyze the vulnerabilities that allow them to succeed, and offer practical recommendations for improving cybersecurity defenses. By learning from the experiences of past victims, this research seeks to provide valuable insights that can be used to develop proactive strategies and security protocols to prevent or mitigate the impact of quid pro quo attacks in the future.

CHAPTER 1: INTRODUCTION

1.1 Origin:
Cybercrime traces back to the 1970s with hacking evolving from curiosity to exploitation of computer systems. The 1980s saw the rise of viruses and malware, while the 1990s brought phishing and identity theft as the internet expanded.

1.2 Definition:
Cybercrime encompasses unlawful activities involving computers or networks, including hacking, identity theft, fraud, and malware.

1.3 Law:
In India, cybercrime is defined by the Information Technology Act, 2000, covering hacking, identity theft, phishing, and online fraud. Internationally, frameworks like the Budapest Convention address cybercrime.

1.4 Types:
Cybercrimes target individuals, organizations, and governments, including identity theft, data breaches, cyber espionage, and cyber terrorism.

1.5 Classification:
Cybercrimes can be categorized by nature, target, method, or motive, including computer-enabled crimes, material-related crimes, and cyber terrorism.

1.6 Online Platforms:
Various online platforms facilitate communication, commerce, gaming, education, and collaboration,

such as social media, e-commerce, and educational platforms.

1.7 Cyberspace:
Cyberspace refers to the interconnected digital world where people engage in activities like communication, commerce, and information sharing.

1.8 Cyberattack:
Cyberattacks aim to disrupt or gain unauthorized access to digital networks or systems through malware, phishing, denial-of-service attacks, and insider threats.

1.9 Social Engineering:
Social engineering involves deceiving individuals or groups into divulging sensitive information or granting access through techniques like phishing, pretexting, and tailgating.

1.10 Quid Pro Quo Attack:
Quid pro quo attacks exploit human trust within organizations to gain access to sensitive data or systems. Unlike traditional cyberattacks, these rely on social engineering tactics. Awareness campaigns and training can help employees recognize and prevent such manipulation.

1.11 Cybercrime Statistics in Chennai:
India, like many nations, has seen a surge in cybercrime, with Chennai accounting for a significant portion. The number of recorded cybercrimes has increased, with a notable rise during the pandemic.

1.12 Causes of Cybercrime:
Cybercrime stems from various factors, including financial gain, anonymity, technological advancements, globalization, lack of cybersecurity awareness, legal loopholes, social motives, organized crime, and access to technology and skills.

1.13 Impact of Cybercrime:
Cybercrime leads to financial losses, data breaches, disruption of operations, reputational harm, identity theft, cyber espionage, vulnerabilities in critical infrastructure, psychological distress, legal implications, erosion of trust in digital technologies, and regulatory challenges.

1.14 Limitations of Cybercrime:
Challenges in combating cybercrime include technological complexity, global reach, anonymity, resource constraints, data privacy concerns, underreporting, encryption, sophistication of attacks, legal and regulatory hurdles, and the rapidly evolving threat landscape.

1.15 Precautions:
Protecting against cybercrime involves education, strong passwords, two-factor authentication, software updates, caution with emails, secure networks, regular data backups, security policies, monitoring financial accounts, investing in cybersecurity products, and fostering a culture of security.

1.6 Aim of the Study:
The study aims to quantify incidents of quid pro quo attacks through surveys conducted online, utilizing a random sampling approach to gather data from victims.

CHAPTER-2
LITERATURE REVIEW

 Protection from Social Engineering Attacks (2015):

- Provides an overview of social engineering, emphasizing psychological manipulation in attacks.
- Urges prompt detection and mitigation, stressing the need for preventive measures and education.

 Social Engineering Attacks on Social Networks (2022):

- Examines attacks on social media, advocating for heightened cybersecurity awareness.
- Highlights emotional and financial impacts, emphasizing the importance of safeguarding information.

Social Engineering Attack Classifications (2023):

- Introduces SEAD pipeline for defense against social media attacks.
- Leverages sentiment analysis and source screening for SEA identification.

Study on Social Engineering Attacks (2016):

- Stresses the importance of cybersecurity training and establishing a culture of security awareness.
- Recommends educating users about hacker-friendly resources for better defense.

Social Engineering Attack Examples (2016):

- Presents ten unique social engineering assault templates for awareness and testing.
- Highlights the value of templates in creating scenarios and detecting assault algorithms.

Survey on Social Engineering Attacks (2019):

- Advocates for creative detection methods, defense mechanisms, and cybersecurity education.
- Calls for large investments in cybersecurity education by governments.

Social Engineering Attack Framework (2014):

- Proposes a comprehensive framework for analyzing and comparing social engineering attacks.
- Integrates temporal data to map historical events and scenarios.

Social Engineering Attack Detection Model (2018):

- Initially focused on detection but shifted to encouraging individual alertness.
- Explores various aspects within the field of social engineering.

Employee Awareness Model (2021):

- Aims to enhance awareness of social engineering threats in the Saudi public sector.
- Emphasizes the importance of a supported information security framework.

Social Engineering Attacks in E-Government Systems (2022):

- Advocates for national education and training initiatives to increase public knowledge.
- Recommends research on technology utilizing Natural Language Processing for detection.

CHAPTER-3
METHODOLOGY

This chapter discusses the methodology embraced by the researcher conducting the study. The present chapter discusses about aim, objectives and purpose of the study, Universe, Material and approaches, statistical analysis and tools and tactics.

3.1 Aim:

The aim of the study is to enlighten individuals who frequently work in cyberspace.

3.2 Objectives:

- A social engineering attack depends on countermeasures rather than having a specialized defense mechanism. Not everyone is aware of these countermeasures, but we may be able to change that by raising awareness.

- To examine how attackers use the emotions of their victims as leverage when committing crimes.
- To understand the psychological effects that Cybercrime has on its victims.

3.3 Purpose of the study:

The purpose of this study is to assess the awareness of Cyberattacks among the general civilian population, evaluating their comprehension of such incidents and their knowledge regarding preventive measures.

3.4 Independent variable:

- Age
- Gender

3.5 Dependent variable:

Responses from general civilian about awareness of Cyberattack in google forms.

3.6 Universe:

The data for the study was gathered from individuals who are actively engaged in cyberspace activities on a regular basis in Chennai.

3.7 Data processing and Analysis:

A statistical tool serves as a pivotal instrument for interpreting and analyzing data, facilitating a scientific comprehension of the issue across its multiple dimensions.

3.8 Sample of the study:

- Data of the study was collected from general people whom frequently works in cyberspace.
- There are totally 80 responses were collected for the study.

3.9 Research tools and Techniques:

We used Google forms to collect their response from Online.

3.10 Statistical analysis:

Statistical analysis was performed employing Microsoft Excel for the generation of a Pie chart. Google forms is used for collecting data.

3.11 Need for study:

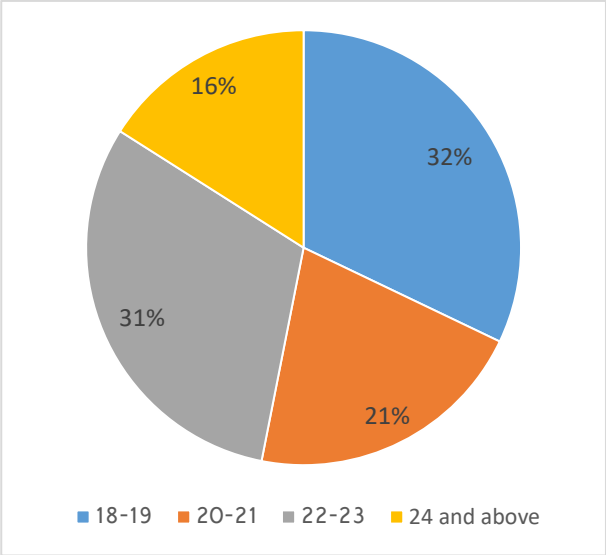
Overall, this research survey aims to assess the general public's knowledge of quid pro quo attacks. The findings will help educate them on how to prevent future cyberattacks.

3.12 Limitation:

- Difficulty in collection of survey from the IT sector people.
- Due to lack of time limit I had to collect the survey via online platform (google form).
- The authenticity of the data is questionable due to the use of Google Forms.
- Respondents may be hesitant to provide honest answers due to concerns about data privacy, especially if the survey collects sensitive information.
- Ensuring the quality and validity of responses can be challenging due to limited tools for verifying respondent identity and preventing multiple submissions from the same individual.

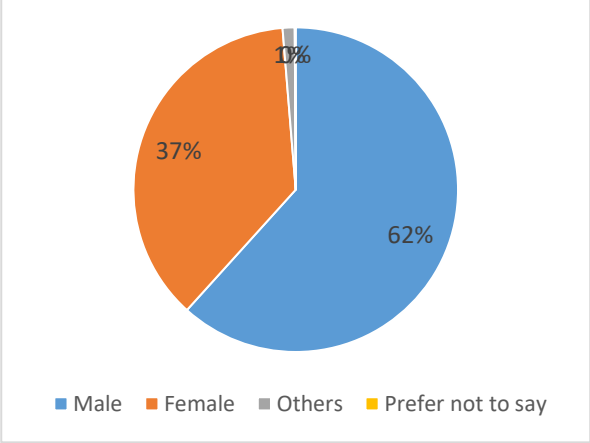
CHAPTER-4
DATA ANALYSIS

Pie chart 1.. Shows the age distribution of the responder.



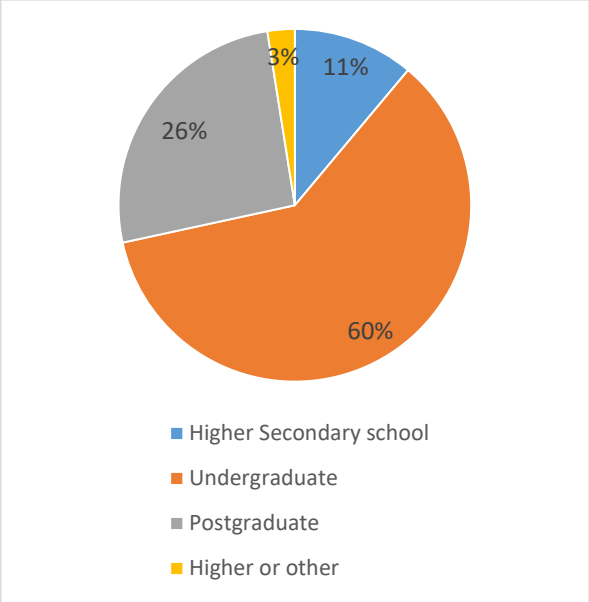
According to this study, in this research, the age distribution of the 80 respondents reveals a predominant concentration within the 18-19 and 22-23 age brackets. Conversely, the 20-21 and 24-and-above age cohorts are notably underrepresented in comparison to the aforementioned groups.

Pie chart 2.. Shows the gender distribution of the responder.



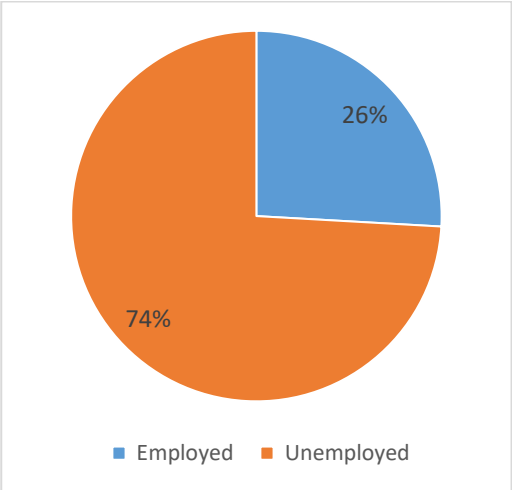
In this study, a notable disparity is observed in the gender distribution of respondents, with a higher representation of male participants in comparison to female respondents. Additionally, individuals identifying with other genders contributed to the survey, albeit with a considerably smaller response rate.

Pie chart 3.. Shows the education qualification of the responder.



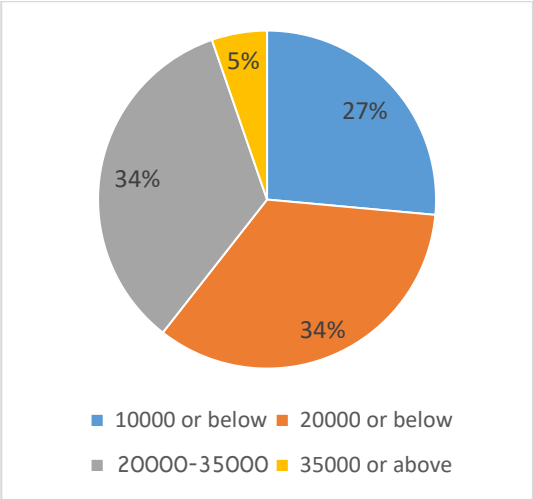
According to this study, the primary demographic of respondents in this survey comprises undergraduates, with postgraduates representing the second largest cohort. Furthermore, there is a presence of respondents from high school and diverse educational backgrounds.

Pie chart 4.. Shows the occupation of the responder.



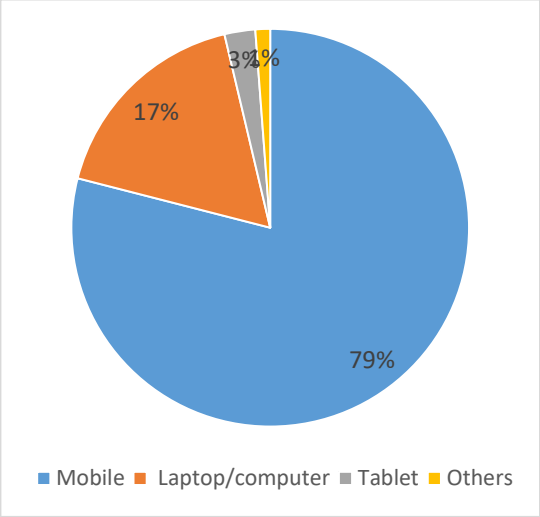
According to this study, The survey garnered a larger response from unemployed individuals in comparison to employed respondents. This trend can be attributed to the propensity of unemployed individuals to allocate more time to online activities, thus increasing their likelihood of participating in surveys conducted through digital platforms.

Pie chart 5.. Shows the income of the employed responder.



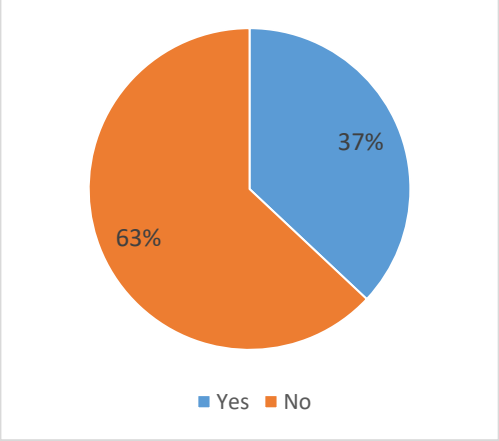
According to this study, within the survey, a specific inquiry was directed towards the payroll of employed individuals, particularly focusing on two income brackets: those earning below 20,000 and those earning between 20,000 and 35,000 per month.

Pie chart 6.. Shows the device usage of the responders.



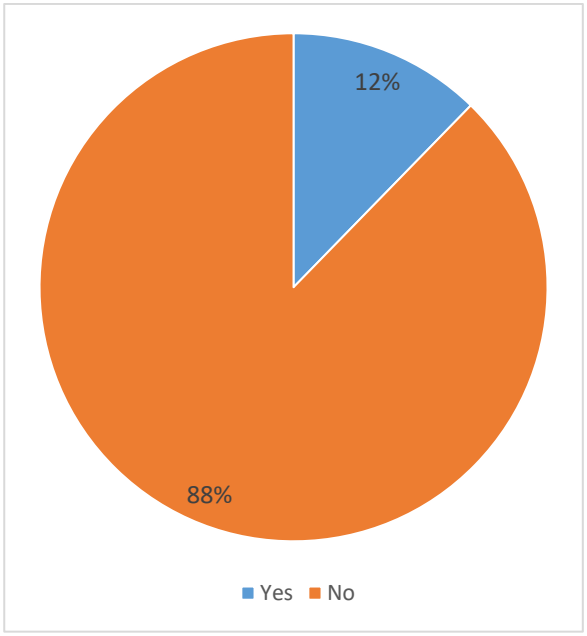
According to this study, among respondents, the mobile device emerged as the most prevalent electronic device in use, with laptops and personal computers (PCs) exhibiting comparatively lower rates of utilization.

Pie chart 7.. Shows that how many of them aware of Quid pro quo attack.



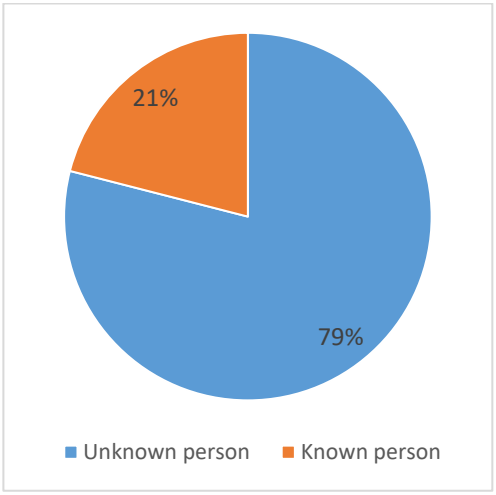
According to this study, in our survey, participants were queried regarding their familiarity with Quid pro quo attacks. The findings revealed that a significant majority, comprising 63% of respondents, were unaware of this specific type of cyberattack. Conversely, 37% of participants indicated possessing knowledge about Quid pro quo attacks.

Pie chart 8.. Shows that the respondent have ever been affected by quid pro quo attack.



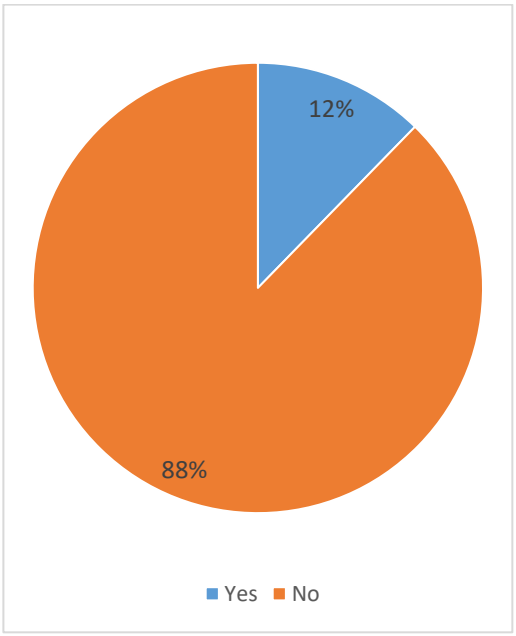
According to this study, when queried about encounters with Quid pro quo attacks, a segment of respondents provided insights into their experiences. Specifically, 12% of participants, comprising 10 individuals, disclosed instances of being victimized by this particular form of cyberattack. Conversely, the vast majority, totalling 88% of respondents (70 individuals), recounted being affected by alternative types of cyber threats.

Pie chart 9.. Shows the responder victimized by known or unknow person.



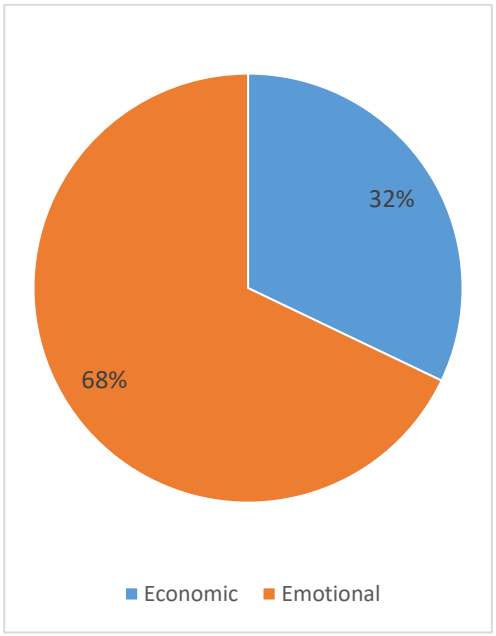
According to this study, in response to inquiries regarding the source of the cyberattacks, a substantial majority of respondents, accounting for 79% of the surveyed population, indicated that they were impacted by actions initiated by unknown individuals or entities.

Pie chart 10.. Shows that the attack takes place on you by your own knowledge.



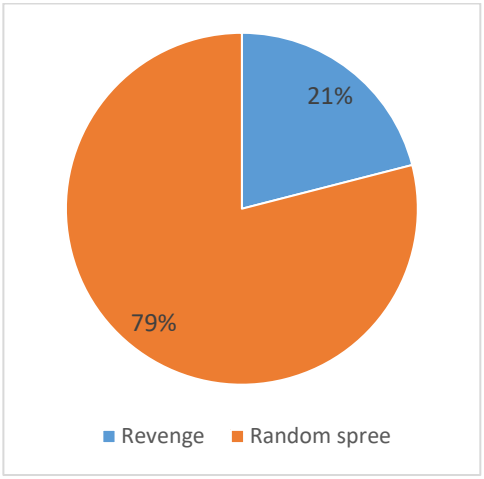
According to this study; in a significant majority of cases, approximately 88% of individuals have experienced victimization through Quid pro quo attacks without prior awareness or recognition of the tactic's existence. Conversely, a distinct minority, constituting roughly 12% of the population, possess knowledge pertaining to Quid pro quo maneuvers.

Pie chart 11.. Shows that the responder loss on economic or emotional.



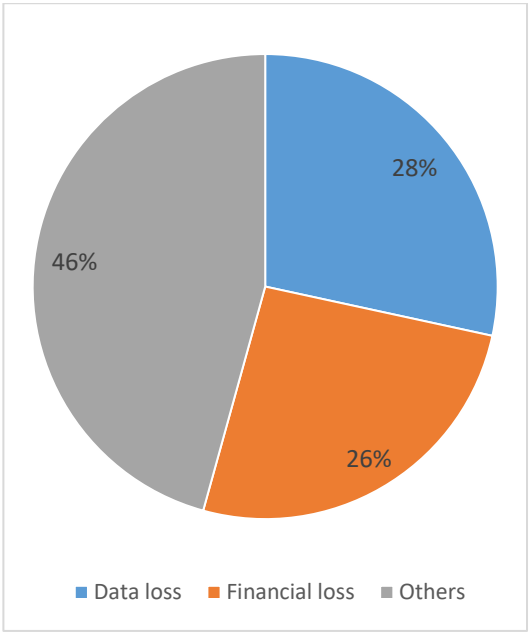
According to this study; a notable trend emerges wherein 68% of individuals report experiencing emotional setbacks rather than economic ramifications. Conversely, 32% of the population encountered economic losses as a result of adverse circumstances.

Pie chart 12.. Shows that the attack takes place on respondent as revenge or random spree.



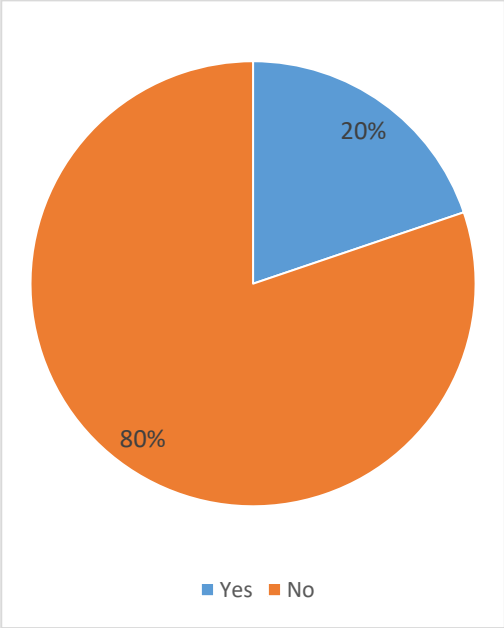
According to this study, a minority segment, comprising 21% of respondents, attributed cyberattacks to motives of revenge, particularly among those aged 17. Conversely, a significant majority, constituting 79% of participants, expressed the belief that such attacks were indiscriminate acts, with 63% specifically characterizing them as random sprees.

Pie chart 13.. Shows what was stolen from the respondent.



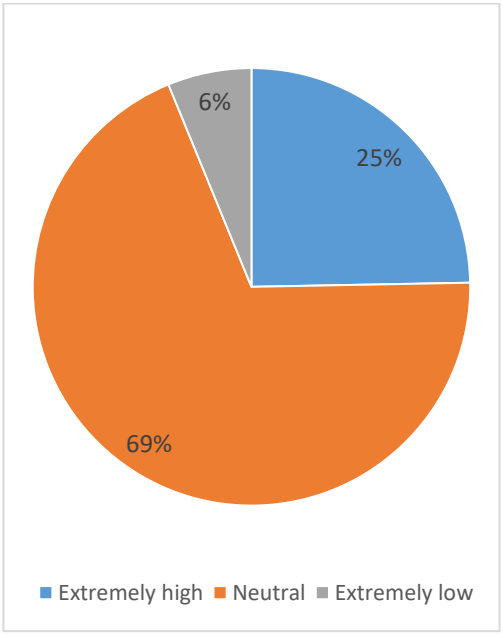
According to this study, a plurality of respondents, representing 46% of the surveyed population, reported experiencing losses categorized as "other," distinct from financial or data-related losses. Within the subset specifying financial losses, 26% of participants indicated such impacts. Meanwhile, 28% of respondents identified data loss as the primary consequence. Among the "other" losses cited, instances of reputation damage, identity theft, and time theft were notably prevalent.

Pie chart 14.. Show that the responder fellow family members or friends have been affected by the Quid pro quo attack.



According to this study, in the survey, respondents were queried regarding the impact of cyberattacks on their extended network, including friends and family. A significant majority, comprising 80% of participants, reported that their acquaintances had not been affected by such incidents. Conversely, 20% of respondents acknowledged that cyberattacks had indeed affected individuals within their personal circles.

Pie chart 15.. Shows how much this cyberattack affects you mentally in scale.



According to this study, a predominant sentiment among respondents indicates a relatively low perception of the severity of cyberattacks, with the majority of participants not considering them a significant issue. Specifically, only a marginal proportion, constituting 6% of the surveyed population, reported being directly affected by cyberattacks.

CHAPTER-5
RESULT AND DISCUSSION

Result

The research survey indicates that the majority of the general public is unaware of quid pro quo attacks. Out of 80 participants, only 30 individuals (37%) were aware of what a quid pro quo attack entails, while the remaining 50 participants (63%) lacked this knowledge. This survey concludes that, until this research, the general public was largely uninformed about quid pro quo attacks and the measures to prevent them. Participants in this survey have subsequently learned about this type of cyberattack and the precautions needed to defend against it.

Through training and increased awareness, it is possible to effectively defend against quid pro quo attacks.

Discussion

A research survey was conducted among the general public to establish an understanding of quid pro quo attacks through a detailed study. This survey was administered via questionnaires using Google Forms, and the data was collected accordingly. The results indicate that the public has insufficient knowledge about quid pro quo attacks and their significance in data and financial loss, despite some awareness of this social engineering attack. The survey targeted individuals aged 18 and above, with a total of 80 respondents. The age group most affected was 18 to 19-year-olds, who are particularly vulnerable due to their limited knowledge of cyberspace and the potential consequences. These individuals are easily manipulated by attackers, making their security vulnerable and enabling attackers to achieve their malicious objectives. Many respondents were deceived through social media platforms, enticed by offers of exciting deals, free products, and discounts. Some attackers made false promises, exploiting victims' desires for economic gain, leading them to compromise their security and disclose sensitive information about themselves or their workplaces. Many victims were unaware of the compromise until they noticed irregularities in their transaction statements or were informed by others. The survey reveals that beyond economic loss, victims often suffer emotional distress, which can be difficult to overcome. These attacks are typically random rather than motivated by revenge. Respondents reported that in addition to data and financial loss, other consequences included reputational damage, wasted time, and identity theft. Preventing quid pro quo attacks relies more on experience and knowledge rather than specific preventive tools, according to respondents. Additionally, many participants were unaware of the Cybercrime Wing, which can assist victims in recovering their losses. The cybercrime helpline is 1930. The motivation for focusing on quid pro quo attacks in this study stems from my own experience as a victim. By sharing the lessons I have learned, I aim to help prevent future incidents and protect others from becoming victims.

CHAPTER-6
CONCLUSION

This study was undertaken to examine the experiences of individuals engaged in social media who have encountered quid pro quo attacks. The analysis indicates that individuals aged 18-19 and 22-23 are more prone to encountering such attacks on social media platforms. Respondents reported that the majority of these attacks were characterized as random spree attacks rather than acts of revenge. These findings suggest a pervasive threat that exploits the broad and often indiscriminate nature of social media interactions. Furthermore, the study reveals that individuals experience more significant impacts in terms of time theft, intellectual property loss, reputation damage, and psychological distress, rather than direct financial loss or data compromise. This underscores the multifaceted nature of these attacks, highlighting how they extend beyond economic implications to affect personal and professional lives profoundly. The psychological and emotional toll of quid pro quo attacks emerged as a critical concern, with victims reporting significant stress, anxiety, and a sense of violation. Additionally, a noteworthy finding is that many of these events occur without the victims' knowledge or awareness. This highlights a crucial vulnerability: the lack of awareness and understanding of quid pro quo tactics among social media users, making them easy targets for such deceptive practices. Increased awareness and education are therefore vital in mitigating these risks. The study underscores the detrimental effects of quid pro quo attacks on individuals engaged in social media activities, emphasizing the need for robust preventative measures and support systems. It also highlights an increasing awareness of this phenomenon among the affected population, suggesting a positive trend towards better recognition and reporting of these incidents. Overall, the study's

analysis provides comprehensive insights into the nature and impact of quid pro quo attacks on social media users, yielding satisfactory results. The findings call for enhanced education and awareness campaigns, as well as the development of strategic interventions to protect vulnerable age groups and mitigate the emotional and psychological impacts of such attacks.

REFERENCE

1. Protection of Computer Networks from the Social Engineering Attacks (2015) Hardik K. Molia and Hardik A Gohel
2. Overview of Social Engineering Attacks on Social Networks (2022) Kaouthar Chetiouia , Birom Baha , Abderrahim Ouali Alamia and Ayoub Bahnasseb
3. Social Engineering Attack Classifications on Social Media Using Deep Learning (2023) Yichiet Aun1, Ming-Lee Gan, Nur Haliza Binti Abdul Wahab2 and Goh Hock Guan
4. A Study on Social Engineering Attacks and Defence Mechanisms (2016) Mukesh Chinta, Jitendra Alaparthi, and Eswar Kodali
5. Social engineering attack examples, templates and scenarios (2016) Francois Mouton, Louise Leenen and H.S. Venter
6. Social Engineering Attacks: A Survey (2019) Fatima Salahdine and Naima Kaabouch
7. Social Engineering Attack Framework (2014) Francois Mouton , Mercia M. Malan , Louise Leenen and H.S. Venter
8. Social engineering attack detection model (2018) Francois Mouton
9. Employee Awareness Model to Enhance Awareness of Social Engineering Threats in the Saudi Public Sector (2021) Mohammed Fahad Alghenaim, Nur Azaliah Abu Bakar, Rasimah Che Mohd Yusoff, Noor Hafizah Hassan and Hasimi Sallehudin
10. Social Engineering Attacks in E-Government System: Detection and Prevention (2022) Musa Midila Ahmed
11. Social Engineering Attacks Prevention: A Systematic Literature Review (2022)Wenni Syafitri, Zarina Shukur, Umi Asma Mokhtar, Rossilawati Sulaiman and Muhammad Azwan Ibrahim
12. Mitigating the risk of social engineering attacks (2011) Matthew Spinapolice
13. Social Engineering Attacks: A Clearer Perspective (2022) Samuel Adu-Gyimah, George Asante and Oliver Kufuor Boansi
14. Implementation of Social Engineering Attack at Institution of Higher Education (2019) Zhengbing Hu, Volodymyr Buriachok and Volodymyr Sokolov
15. Social engineering against security policy (2019) Miika Sillanpää
16. A survey of social engineering attacks: Detection and prevention tools (2021) Noor Ammar Odeh, Derar Eleyan and Amna Eleyan
17. Efficacious Tactics, Mechanics and Heuristics for Progressive Social Engineering (2021) Ujas Dhami
18. A Preliminary Propagation Tool in Social Engineering Attacks (2021) Peggy Hoong
19. A Taxonomy for Social Engineering attacks (2011) Koteswara Ivaturi and Lech Janczewski
20. Social Engineering: I-E based Model of Human Weakness for Attack and Defense Investigations (2017) Wenjun Fan, Kevin Lwakatare and Rong Rong
21. The human layer of cybersecurity – the art of social engineering Elisa Norvanto
22. Social engineering and real-world measures employed in defense of them (2019) Mason Carnes, Jonah Oliver and Kelly Woodworth
23. Research of Social Engineering Mechanisms and Analysis of Counteraction Methods (2021) Vyacheslav Yu. Evglevsky , Michael M. Putyato and Alexander S. Makaryan

24. Analysis and classification of chosen social engineering methods in cybersecurity (2021) Monika Olchowik
25. Contribution of Open-Source Intelligence to Social Engineering Cyberattacks (2022) Kim Rosengren

APPENDIX

Questionnaire

1) Age
2) Gender
3) Education qualification
4) Occupation
5) If working, what is your income per month?
6)Which kind of device do you prefer to use the internet?
7) Are you aware of quid pro quo attack?
8) Have you been affected by it?
9) If yes, please describe your experience.
10) From whom you've been victimized?
11) Does it happen, according to your knowledge??
12) If yes, please describe your experience.
13) How did you found out that you victimized?
14) How did you come up with to determine that this is a quid pro quo attack?
15) What was your major loss in this?
16) What is your assumption of this attack takes place on you?
17) What was stolen from you?
18) How did you overcome from it?
19) Is there any prevention technique from it, which help others.
20) Not just you, your friends or family affected by this attack?
21) How did they overcome it?
How does this cyberattack affects you mentally, please describe it.