10TH INTERNATIONAL CONFERENCE ON
CYBERSYCHOLOGY AND MENTAL HEALTH:
CHALLENGES, TRENDS, AND SOLUTIONS

SCIENTIFIC -E- RESEARCH POSTER
SUBMISSION ID: 35

"HUMAN HACKING: UNRAVELING THE PSYCHOLOGICAL TRIGGERS BEHIND SOCIAL ENGINEERING"

AUTHORS AND AFFILIATIONS

1. **Samreen Arshad** (*Corresponding Author*)
Samrinarshad@yahoo.com
Department of Psychology
Government College University, Lahore.

2. Sheheryar Pirzada K163941@nu.edu.pk
Senior Software Engineer at Q Solutions
Karachi.

ABSTRACT

Background: Human factors play a crucial role in how individuals fall victim to social engineering attacks. Understanding these factors is vital for strengthening defenses against such attacks. **Objectives:** This study investigates how various human factors specifically trust, commitment, obedience, threat severity and subjective behaviors affect susceptibility to social engineering. By analyzing these factors, the research aims to provide clear insights into how social engineers exploit these vulnerabilities and offer practical recommendations to enhance cyber security. **Method:** A correlational research design was used. Data were collected from 488 participants using a scale developed by Workman (2007) to assess human factors linked to social engineering susceptibility. **Results:** The analysis included a graphical interpretation of survey results. The study reveals significant correlations between trust, commitment, obedience, and threat severity with subjective behaviors linked to social engineering attacks. The scale's psychometric properties were assessed, confirming its effectiveness in measuring these factors. The descriptive analysis highlights critical vulnerabilities that are frequently exploited by social engineers. **Conclusion:** The findings underscore the need to address specific human factors in cyber-security training and awareness programs to understand the influence of trust, commitment, obedience, and threat severity on susceptibility can pave the way for developing more effective strategies to combat social engineering attacks.

Keywords: human factors, trust, commitment, obedience, threat severity, social engineering, cyber security.

INTRODUCTION

In the digital age, cyber attacks increasingly target psychological vulnerabilities alongside technological ones. Social engineering, or "human hacking," exploits cognitive biases and behavioral tendencies to bypass technical safeguards, manipulating individuals into compromising sensitive information or security systems. Key psychological triggers such as trust, obedience, commitment, and perceived threat severity play a critical role in these attacks. Research indicates that over 90% of successful cyber attacks stem from human error or manipulation rather than technical flaws (Verizon Data Breach Investigations Report, 2024). Despite this, limited research systematically examines the interplay of psychological traits with susceptibility to social engineering attacks (Workman, 2007; Alharthi & Regan, 2020). With the rising prevalence of tactics like phishing, baiting, and pretexting, there is an urgent need to understand how these psychological triggers are exploited.

This study seeks to address this gap by exploring the role of human vulnerabilities in social engineering attacks, providing actionable insights to enhance cyber security awareness and develop tailored defense strategies. By integrating psychological perspectives with cyber security practices, this research aims to strengthen individual and organizational resilience against such threats.

METHOD

OBJECTIVES

The primary objective of this study was to investigate the relationship between psychological vulnerabilities (trust, commitment, obedience, and threat severity) and subjective behavior susceptibility to social engineering attacks. The study also aimed to assess how these vulnerabilities can be mitigated to enhance cyber security awareness and defenses.

HYPOTHESES

H1: Higher levels of trust are positively correlated with subjective behavior susceptibility to social engineering attacks.
H2: Greater commitment to interpersonal relationships increases susceptibility to social engineering.
H3: Higher levels of obedience to authority figures are positively correlated with susceptibility to social engineering.
H4: Increased threat severity is negatively correlated with susceptibility to social engineering.

SAMPLE

- ***Participants:*** The study included 488 participants (52.1% female and 47.9% male) recruited through simple random sampling.
- ***Inclusion Criteria:*** Participants with regular internet use and basic familiarity with online communication channels were included.

INSTRUMENTS

Gaining Access with Social Engineering Scale (Workman, 2007)

- A validated scale designed to assess psychological factors, including trust, vulnerability, commitment, obedience, reactance, threat severity and subjective behaviors.
- The scale includes Likert-type items.
- ***Reliability:*** Cronbach's alpha for the scale was reported as 0.89.

Demographic Information Form

- Collected data on age, gender, educational background, and internet usage and occupational roles, ensuring variability in demographic profiles.

PROCEDURE

1. ***Data Collection***

- Participants were invited to complete an online survey distributed through email and social media platforms.
- Informed consent was obtained electronically before participants accessed the survey.

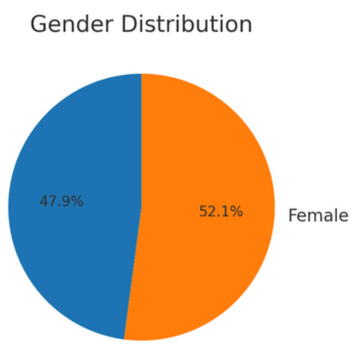
2. ***Survey Administration***

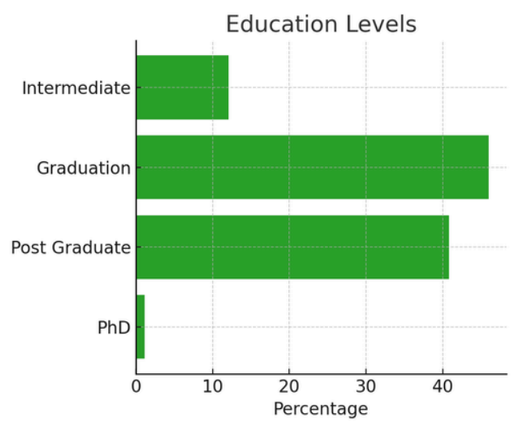
- The survey consisted of two sections: demographic information and the *Gaining Access with Social Engineering Scale (Workman, 2007)*.

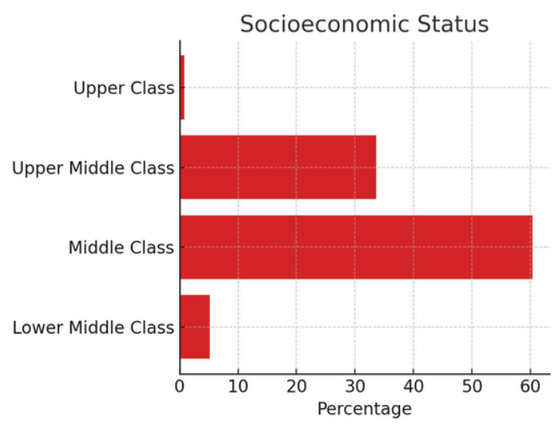
3. ***Ethical Considerations***

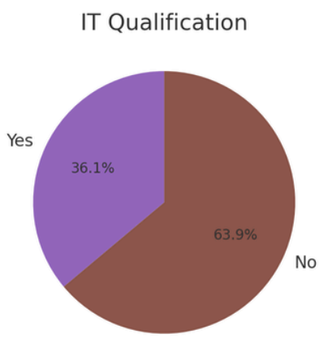
- Consent was obtained, and measures were implemented to ensure confidentiality and anonymity throughout the research process. Participants were informed of their right to withdraw from the study at any point without facing any consequences

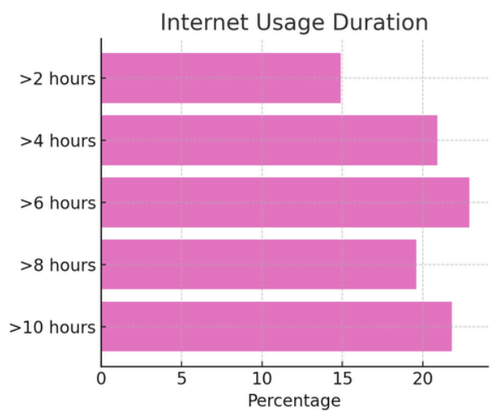
RESULTS AND DISCUSSION

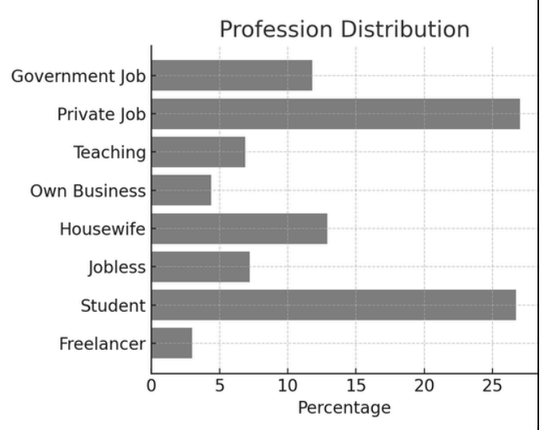












Reliability, Mean, Standard Deviation and Correlation analysis of study variables (N=488)

Variables	M	SD	α	1	2	3	4	5	6	7	8	9
1. Threat Severity	13.65	2.78	0.75	-	-0.42**	-0.36**	-0.29**	-0.31**	-0.33**	-0.30**	-0.32**	-0.35**
2. Vulnerability	12.89	3.12	0.76	-	-	0.41**	0.37**	0.35**	0.38**	0.40**	0.34**	0.39
3. Normative Commitment	14.01	3.04	0.78	-	-	-	0.39**	0.38**	0.37**	0.36**	0.32**	0.31**
4. Continuance Commitment	13.72	3.08	0.72	-	-	-	-	0.40**	0.42**	0.39**	0.37**	0.33**
5. Affective Commitment	13.95	3.19	0.77	-	-	-	-	-	0.41**	0.38**	0.39**	0.36**
6. Trust	14.34	3.01	0.81	-	-	-	-	-	-	0.42**	0.39**	0.37**
7. Obedience	14.12	3.06	0.79	-	-	-	-	-	-	-	0.43**	0.40**
8. Reactance	13.85	3.22	0.73	-	-	-	-	-	-	-	-	0.38
9. Subjective Behavior	14.56	3.14	0.85	-	-	-	-	-	-	-	-	-

* .05 level (2-tailed). **.01 level (2-tailed).

This study revealed significant correlations between key psychological vulnerabilities (trust, commitment, obedience, and perception of threat severity) and subjective behavior susceptibility to social engineering attacks. The results indicate that:

1. ***Trust:*** Participants with higher levels of trust were more likely to fall victim to social engineering attacks, especially phishing and pretexting.
2. ***Commitment:*** Strong personal or organizational commitments were found to increase susceptibility, as individuals showed a higher tendency to comply with requests from trusted sources.
3. ***Obedience:*** Those who exhibited higher levels of obedience to authority figures displayed greater vulnerability to social engineering tactics, particularly those involving manipulation by figures of authority.
4. ***Threat severity:*** Interestingly, higher threat perception was found to be inversely related to susceptibility. Participants who perceived a higher level of threat to their information security were less likely to be manipulated by social engineers.

These findings underscore the need to focus on these psychological factors in cyber security training programs to reduce vulnerability to social engineering attacks.

PRACTICAL IMPLICATIONS

Understanding how trust, commitment, and vulnerability influence susceptibility to social engineering attacks can help cyber security training and defense strategies. For instance, targeting vulnerable individuals with educational interventions that enhance trust in security protocols and reduce reactance might be key to improving overall defenses against cyber threats. Further, tailoring interventions based on individuals' commitment levels could be a strategy to foster stronger defenses and adherence to security protocols.

LIMITATIONS AND SUGGESTIONS

1. ***Limitations:***

- The participants were primarily from urban areas, limiting the generalizability of the findings to rural populations.

2. ***Suggestions:***

- Future research should explore additional psychological vulnerabilities, such cognitive load, to better understand their role in social engineering.
- Studies should also investigate the role of training interventions targeting specific psychological vulnerabilities and measure their effectiveness in reducing social engineering incidents.

REFERENCES

1. Alharthi, M. K., & Regan, P. M. (2020). Psychological vulnerabilities in social engineering: A study of cyber threats and human behavior. Journal of Cybersecurity and Human Factors, 15(3), 205-222. https://doi.org/10.1016/j.cyber.2020.01.005
2. Verizon. (2024). Verizon data breach investigations report 2024. https://www.verizon.com/business/resources/reports/dbir/
3. Workman, M. (2007). The role of psychological factors in social engineering attacks: Trust, commitment, and threat perception. Journal of Information Security, 9(2), 175-193. https://doi.org/10.1016/j.jinfosec.2007.03.002