IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

An Empirical Study On Social Engineering Attack Awareness Among University Students In India

1Mr.Jithesh Kumar A H, 2Ms.Shrinidhi Kharvi, 3Mr.Shreekanth, 4Mr.Yogesh Devappa Mestha, 5Ms.Nagalaxmi

1Assistant Professor, 2Assistant Professor, 3Assistant Professor, 4Assistant Professor, 5Assistant Professor

1IMJ Institute of Science and Commerce Moodlakatte,Kundapura,

2IMJ Institute of Science and Commerce Moodlakatte,Kundapura,

3Dr.BB Hegde College Kundapurs,

4IMJ Institute of Science and Commerce Moodlakatte,Kundapura,

5MJ Institute of Science and Commerce Moodlakatte,Kundapura

Abstract

The rapid expansion of digital technologies has increased exposure to cyber threats, particularly those targeting human vulnerabilities. Social engineering attacks exploit psychological manipulation to deceive users into revealing sensitive information. This paper presents an empirical study evaluating awareness levels among university students using a structured survey of 182 respondents. The analysis examines awareness, behavioral tendencies, and susceptibility to phishing and related attacks. Results indicate that while 64% of respondents are aware of phishing, over 41% still engage in risky behaviors such as clicking unknown links and password reuse. The study highlights a gap between awareness and secure practices and proposes targeted awareness programs and curriculum integration to mitigate risks.

Index Terms— Cybersecurity, social engineering, phishing, awareness, human factors.

I. INTRODUCTION

The increasing reliance on digital platforms has significantly amplified cybersecurity risks. Among various threats, social engineering remains highly effective due to its focus on human psychology rather than system vulnerabilities. Attackers commonly use phishing emails, fake websites, and impersonation techniques to gain unauthorized access to sensitive information.

Despite advancements in security technologies, human error continues to be a major contributor to security breaches. University students are particularly vulnerable due to frequent internet usage and limited awareness of evolving threats.

This study aims to evaluate awareness levels and behavioral patterns related to social engineering attacks among students and to propose strategies for improving cybersecurity awareness.

II. LITERATURE REVIEW

Existing research highlights the growing impact of social engineering attacks and the importance of user awareness in preventing them. Studies indicate that phishing remains one of the most common attack vectors due to its simplicity and effectiveness.

Prior work also emphasizes that technical solutions alone are insufficient, and user education plays a crucial role in mitigating risks. However, limited research focuses specifically on awareness levels among university students in developing regions, which this study addresses.

III. METHODOLOGY

A. Data Collection

A structured survey was conducted using Google Forms. A total of 182 respondents participated, including undergraduate students, postgraduate students, and faculty members.

B. Questionnaire Design

The questionnaire consisted of:

- **Awareness-based questions**
- **Behavior-based questions**
- **Scenario-based decision-making questions**

C. Analysis Method

The collected data was analyzed using:

- **Percentage analysis**
- **Awareness scoring model**
- **Comparative analysis between IT and non-IT students**

IV. RESULTS

A. Awareness of Phishing

- **64% of respondents are aware of phishing attacks**
- **36% are unaware**

B. Risky Behaviors

- **41% click unknown links**
- **52% reuse passwords**
- **33% do not verify email authenticity**

C. Comparative Analysis

- **IT students awareness: 72%**
- **Non-IT students awareness: 55%**

D. Awareness Level Distribution

- **High awareness: 28%**
- **Medium awareness: 46%**
- **Low awareness: 26%**

Fig. 1. Awareness of phishing attacks

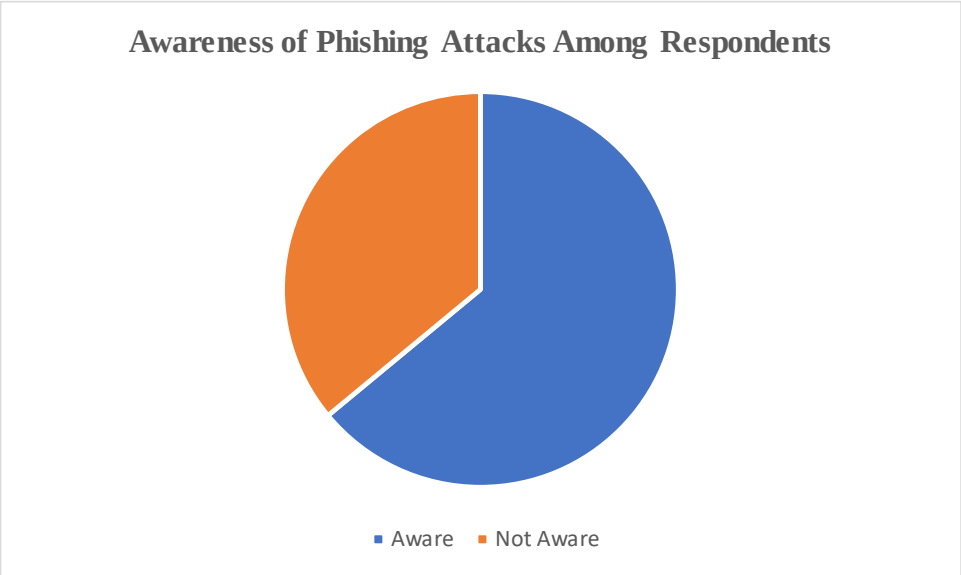


Fig. 2. Risky online behaviors

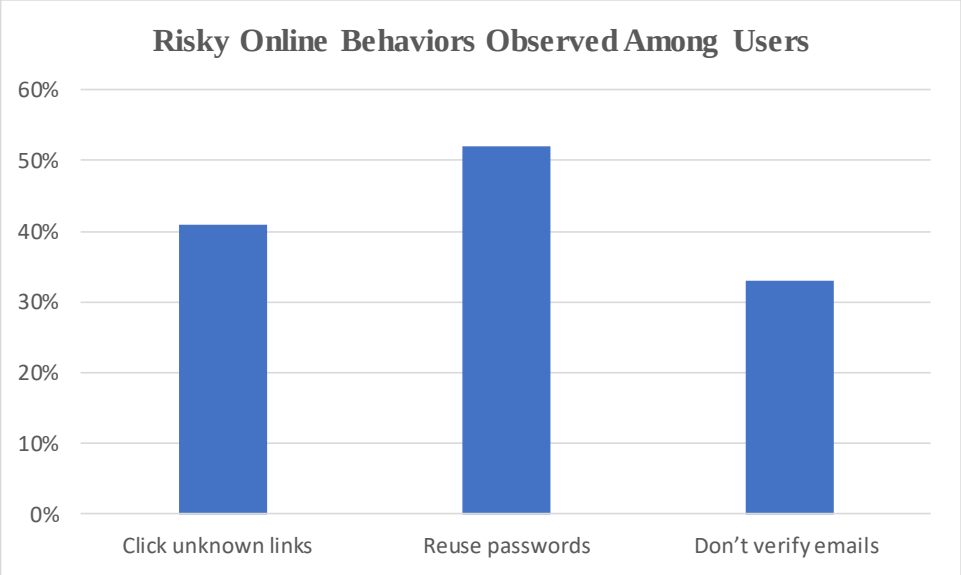


Fig. 3. IT vs Non-IT comparison

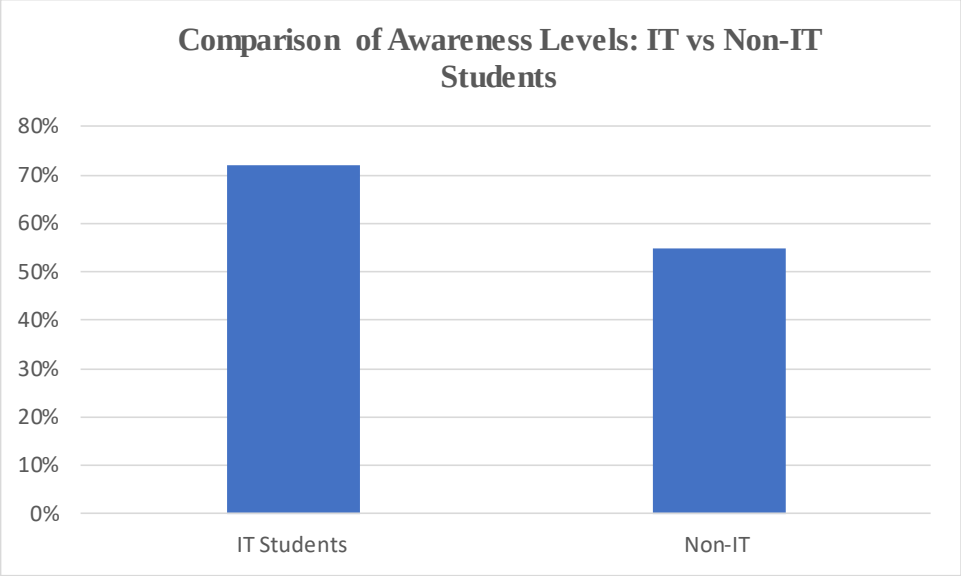
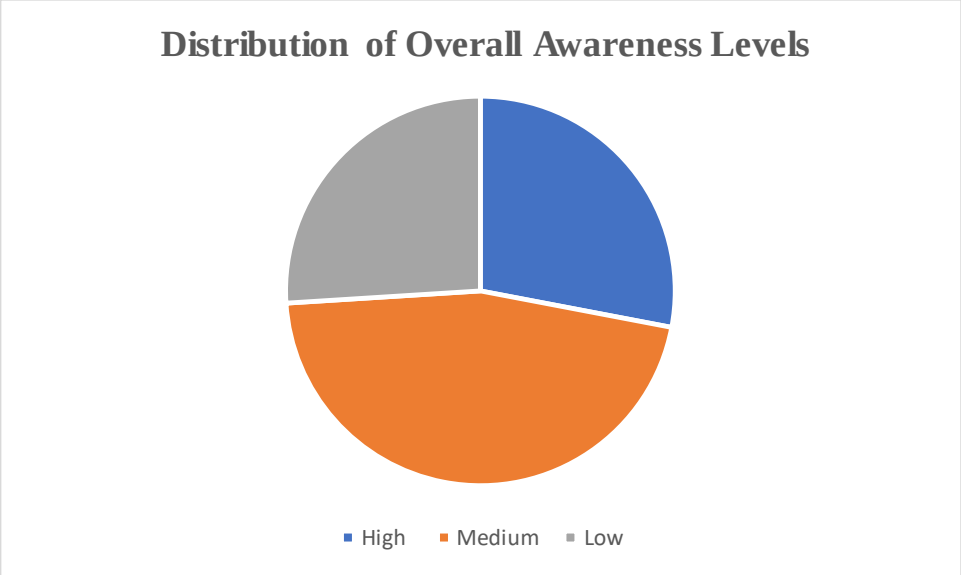


Fig. 4. Awareness level distribution



V. DISCUSSION

The findings reveal a significant gap between awareness and actual behavior. While many respondents demonstrate basic knowledge of phishing, unsafe practices remain prevalent. This indicates that awareness alone is insufficient without behavioral change.

The results also show that IT education improves awareness levels; however, it does not fully eliminate risky online behavior. This highlights the need for practical cybersecurity training and real-world simulation exercises.

VI. RECOMMENDATIONS

To reduce vulnerability to social engineering attacks, the following measures are recommended:

- Regular cybersecurity awareness training programs
- Integration of cybersecurity modules into academic curricula
- Promotion of multi-factor authentication (MFA)
- Encouragement of strong and unique password practices

VII. CONCLUSION

This study demonstrates that although awareness of social engineering attacks exists among students, risky behaviors continue to expose them to cyber threats. Bridging the gap between knowledge and practice is essential for improving cybersecurity resilience. Future work may include automated detection systems and longitudinal studies to track awareness improvement over time.

REFERENCES

[1] R. M. Abdulla, H. Faraj, C. O. Abdullah, and A. H. Amin, "Analysis of social engineering awareness among students and lecturers," .

[2] D. Berrou, "Reducing phishing susceptibility among university students: A pre–post cybersecurity awareness intervention," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, 2025.

[3] M. Khaled *et al*., "A study on cyber attack awareness among students: University of Science and Technology case study," *Journal of Science and Technology*, vol. 30, no. 8, 2025.