IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Social Engineering Attacks And Their Prevention In Educational Institutions

[1]Shreekanth, [2]Harish Kanchan, [3]Ranjith T N

[1]Assistant Professor, [2]Assistant Professor, [3]Physical Education Director
[1]Department of Computer Applications,
[1]Dr. B. B. Hegde First Grade College, Kundapura, India

Abstract: Social engineering attacks are a major problem for cybersecurity, particularly in colleges and universities, where students, professors, and administrative staff might not be properly trained and informed. In this paper, we examine basic social engineering tactics, including phishing, pretexting, baiting, and tailgating, and examine their probable impact in a college campus. In a case study with a Karnataka college's faculty and students, the paper determines the key vulnerabilities and recommends effective preventive measures. The paper concludes by prescribing a cybersecurity awareness program specially designed for colleges to reduce the possibility of human-centered cyber-attacks.

***Index Terms* - Social engineering, phishing, cybersecurity, human-centered attacks.**

I. INTRODUCTION

Cyber security threats have escalated beyond mere technical vulnerabilities; the attackers now exploit the human factor by using social engineering strategies. Social engineering involves psychological manipulation of individuals, compelling them to do something or divulge valuable information. In the case of schools, the students and faculty members alike become prime targets since they operate digital platforms on a daily basis and lack adequate exposure to security training.

In India, the abrupt shift towards online academic services—online exams, digital attendance, and learning management systems—has left higher educational institutions vulnerable to a range of cyber threats. One of them is the phishing emails that masquerade as college administrators or fake sites that ask for login credentials.

The primary objectives of this research are:

- To ascertain the predominant varieties of social engineering attacks occurring within academic institutions.
- To evaluate the level of awareness and readiness among students and staff.
- To advise institution-wide prevention measures and awareness campaigns.

II. LITERATURE REVIEW

Social engineering attacks have been researched extensively in recent times since they are among the most successful forms of cyberattacks. They are inexpensive to execute and frequently successful. Unlike technical issues, social engineering is concerned with the way people think and act, making them more difficult to detect and prevent.

Hadnagy (2018) defines social engineering as misleading individuals into performing something or revealing confidential information. His book identifies some of the methods such as phishing, pretexting, and baiting, most of which are used against schools because of their open and collaborative nature.

Krombholz and colleagues (2015) studied how susceptible users are to phishing schemes. They found that the main reason individuals fall prey is due to a lack of knowledge regarding the schemes and insufficient training. Their results validate what happens in schools, especially among the students.

Jagatic and others (2007) conducted an experiment in which spear-phishing emails were sent to students of a university. The experiment demonstrated that students were more prone to click on harmful links if the emails appear to originate from their teachers or friends, illustrating how social trust can be exploited against them.

Chitrey et al. (2018) carried out research on Indian higher education institutions and discovered that over 60% of the employees were not aware of the fundamental indicators of phishing attacks. They emphasized the importance of implementing cybersecurity awareness programs taking into account language and cultural differences.

A number of frameworks have been proposed to mitigate social engineering attacks. MITRE's ATT&CK framework provides details about the attacker's techniques and tactics, whereas NIST SP 800-50 recommends formal awareness training as an integral part of information security plans in schools.

Even with such resources available, there exists a vast gap between awareness and action. Formal policy, professional cybersecurity training, or even simple posters to inform the users do not exist in most of the institutions. This paper tries to bridge the gap by analyzing actual experiences of students and employees in a college in Karnataka and suggesting pragmatic and actionable steps.

III. METHODOLOGY

The research employs a mixed-method case study design utilizing quantitative and qualitative data collection techniques to examine the perception of social engineering attacks within a university setting.

1. *Participants*

The research was carried out at a Karnataka degree college with 60 participants, comprising students, teaching staff, and non-teaching staff from the Computer Science and Commerce departments. These participants were randomly sampled to provide a balanced sample of all user roles across the digital environment of the institution.

2. *The information was collected via a standardized questionnaire distributed via Google Forms and face-to-face interactions. The survey had 15 questions, such as:*

   - Multiple-choice questions for fundamental cybersecurity knowledge
   - Scenario-based questions for the identification of phishing, baiting, and pretexting
   - Opinion-based Likert scale items measuring the readiness of the institution

There were a few open-ended questions for collecting qualitative information on personal experience and recommendations for enhancing security practices within the institution.

3. *Tools and Resources*

The questionnaire was created with Google Forms, and the responses were analyzed using MS Excel and Google Sheets for charts and statistical summaries. For qualitative responses, thematic analysis was utilized to spot frequent concerns and suggestions.

4. *Ethical Considerations*

The survey was voluntary, and no personally identifiable data were gathered. All the responses were anonymized to maintain privacy and confidentiality. The study had been approved by the internal ethics committee of the college.

5. *Limitations*

The number of participants was kept to one institution and comparatively small numbers due to limited time. Subsequent studies could be extended to more than one college and varied geographies.

IV. RESULTS AND DISCUSSION

The survey was responded to by 60 individuals: 35 students, 15 teaching personnel, and 10 non-teaching personnel. The data was analyzed to determine the level of cybersecurity awareness, specifically against social engineering attacks.

Table 1: Survey Results on Awareness of Common Social Engineering Attacks

Awareness Level	Percentage
Heard of "Phishing"	68%
Know what "Social Engineering" means	45%
Aware of "Tailgating" or "Pretexting"	27%

Less than half of participants were familiar with the more general idea of social engineering, even though the majority had heard of phishing. The awareness levels of staff members were marginally higher than those of students.

Table 2: Experience of Cyber Threats Among Respondents

Experience Type	Percentage
Received suspicious email or message	55%
Clicked on unknown links mistakenly	30%
Faced data loss or account compromise	10%

Nearly one-third of the participants acknowledged unintentionally clicking on unknown links, and more than half reported having come across suspicious messages. These findings demonstrate the genuine threat that social engineering poses, even in educational settings.

Table 3: Institutional Efforts Toward Cybersecurity Awareness

Security Measure	Response Rate
Received any training or workshop	18%
IT department issues awareness emails	12%
Posters or notices on cybersecurity	7%

Institutional efforts to inform employees and students about cybersecurity threats are conspicuously lacking. The majority of respondents stated that peer discussions or unofficial sources like YouTube were how they found out about threats.

Discussion

The findings indicate wide awareness and institutional preparedness gaps. While students and staff are more exposed to threats on the internet, there is no systematic training and policy in place. An affordable awareness campaign such as seminars, posters, and mock phishing emails can significantly lower the threat of such attacks.

The findings also emphasize the need to incorporate cyber hygiene teaching in the regular academic curriculum, particularly for non-technical departments.

IV. CONCLUSION

Social engineering attacks continue to be one of the most underappreciated and menacing types of cyberattacks in educational settings. This research confirmed that while students and faculty engage with digital platforms on a regular basis, their knowledge of methods such as phishing, baiting, and pretexting is low. The absence of formal training, institutional messaging, and overt preventive action further adds to vulnerability.

To take this on, institutions need to incorporate a multi-layered prevention approach that involves ongoing cybersecurity awareness workshops, posters in the labs and libraries, basic training for all new students, and simulated phishing attacks to assess readiness.

REFERENCES

[1] C. Hadnagy, Social Engineering: The Science of Human Hacking, 2nd ed., Wiley, 2018.

[2] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, “Advanced social engineering attacks,” J. Inf. Secur. Appl., vol. 22, pp. 113–122, 2015.

[3] T. Jagatic, N. Johnson, M. Jakobsson, and F. Menczer, “Social phishing,” Commun. ACM, vol. 50, no. 10, pp. 94–100, Oct. 2007.

[4] S. Chitrey, R. Bhandari, and R. Heda, “Cybersecurity awareness among Indian higher education faculties,” Int. J. Comput. Sci. Inf. Technol., vol. 9, no. 2, pp. 65–69, 2018.