IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155186

SOCIAL ENGINEERING ATTACK

Mohammad Salman[1], Thanuja J C[2]

Department of MCA, BIT, K.R. Road, V.V. Puram, Bangalore, India[1]

Assistant Professor, Department of MCA, BIT, K.R. Road, V.V. Puram, Bangalore, India[2]

Abstract: Social Engineering Attacks have become one of the most dangerous threats in the field of cybersecurity. Unlike traditional cyberattacks that target software vulnerabilities, social engineering focuses on manipulating human behavior to gain unauthorized access to sensitive information, systems, or networks. Attackers use psychological techniques such as fear, trust, urgency, and curiosity to deceive users into revealing confidential data like passwords, bank details, or personal information. Common forms of social engineering attacks include phishing, baiting, pretexting, tailgating, and vishing.

The increasing use of digital platforms, online banking, social media, and cloud services has significantly increased the risk of social engineering attacks. Traditional security systems such as firewalls and antivirus software cannot fully prevent these attacks because they target human weaknesses instead of technical flaws. Therefore, awareness and user education play an important role in reducing cyber risks.

This project presents a detailed study of social engineering attacks, their techniques, impacts, prevention methods, and cybersecurity awareness strategies. The system also analyzes how attackers manipulate victims and how organizations can strengthen security through training, authentication mechanisms, and monitoring systems. The study aims to create awareness about cyber threats and promote safe digital practices among users and organizations.

Keywords: Cybersecurity, Social Engineering, Phishing, Vishing, Baiting, Pretexting, Cyber Attacks, Information Security, Human Vulnerability, Authentication, Malware, Cyber Awareness, Digital Security, Identity Theft, Online Fraud, Network Security.

1 INTRODUCTION

The rapid growth of the internet and digital technologies has transformed communication, banking, education, healthcare, and business operations. While technology provides convenience and efficiency, it also introduces serious cybersecurity threats. One of the most dangerous and rapidly growing threats is the Social Engineering Attack. Social engineering is a cyberattack technique in which attackers manipulate human emotions and psychological behavior to obtain confidential information or unauthorized system access. Instead of exploiting technical vulnerabilities, attackers exploit human trust, fear, curiosity, and lack of awareness. Social engineering attacks are highly effective because humans are often considered the weakest link in cybersecurity.

Attackers use various techniques such as phishing emails, fake websites, phone calls, and impersonation to trick users into sharing passwords, OTPs, bank details, or confidential organizational information. These attacks can result in financial loss, identity theft, data breaches, malware infections, and reputational damage.

Traditional cybersecurity systems such as firewalls and antivirus software mainly focus on detecting software vulnerabilities and malicious code. However, they cannot completely protect against human manipulation attacks. Therefore, organizations must combine technical security solutions with cybersecurity awareness and user training programs.

This project focuses on understanding different types of social engineering attacks, analyzing their impact, and studying preventive measures to improve cybersecurity awareness. The study highlights how attackers exploit human psychology and how individuals and organizations can defend themselves against such threats.

1.1 Project Description

The “Social Engineering Attack Analysis System” is a cybersecurity awareness-based project developed to study, analyze, and understand various social engineering attack techniques. The system explains how cybercriminals manipulate users through fake emails, phone calls, websites, and messages to steal sensitive information. The project includes information about different attack types such as phishing, spear phishing, baiting, pretexting, tailgating, and

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155186

vishing. It also demonstrates preventive techniques such as multi-factor authentication, password management, cybersecurity awareness training, and email filtering systems.

The system aims to educate users about cyber threats and encourage safe online behavior. It can be used by students, organizations, and cybersecurity learners to understand real-world cyberattack scenarios and defense mechanisms.

1.2 Motivation

The main motivation behind this project is the increasing number of cybercrimes caused by social engineering attacks. Many users lack cybersecurity awareness and unknowingly share sensitive information with attackers. Cybercriminals continuously develop advanced techniques to manipulate victims through emails, phone calls, social media, and fake websites.

Organizations face huge financial losses, data breaches, and reputational damage due to these attacks. Since human error is one of the primary causes of cybersecurity incidents, educating users and improving awareness has become extremely important.

This project was developed to provide detailed knowledge about social engineering techniques, attack prevention methods, and cybersecurity best practices. It helps users recognize suspicious activities and improve digital safety.

II. RELATED WORK

Reference	Year	Authors	Methodology	Result	Limitation
Phishing Detection Using Machine Learning	2024	Various Researchers	ML algorithms, URL analysis	Improved phishing detection accuracy	Requires large datasets
Cybersecurity Awareness and Human Behavior	2023	Various Researchers	User behavior analysis	Increased awareness effectiveness	Human behavior varies
Detection of Social Engineering Attacks	2023	Various Researchers	AI-based email filtering	Reduced phishing attacks	False positives possible
Human Vulnerability in Cybersecurity	2022	Various Researchers	Psychological analysis	Better understanding of attacker behavior	Difficult to predict user actions
Email Phishing Classification	2022	Various Researchers	NLP and Deep Learning	Accurate spam detection	High computational cost
Social Engineering Attack Prevention	2021	Various Researchers	Security awareness training	Reduced cyber incidents	Requires regular updates
Multi-Factor Authentication Security	2020	Various Researchers	Authentication mechanisms	Improved account protection	User adoption challenges

III. METHODOLOGY

The project follows a structured methodology to analyze and understand social engineering attacks.

1. Data Collection

Information regarding phishing emails, fake websites, cyber fraud reports, and attack case studies are collected from cybersecurity resources and research papers.

2. Attack Classification

The collected attacks are categorized into:

- Phishing
- Spear Phishing
- Vishing
- Smishing
- Baiting
- Tailgating
- Pretexting

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155186

3. Threat Analysis
Each attack type is analyzed based on:

- Attack method
- Human psychology used
- Impact on victims
- Security risks

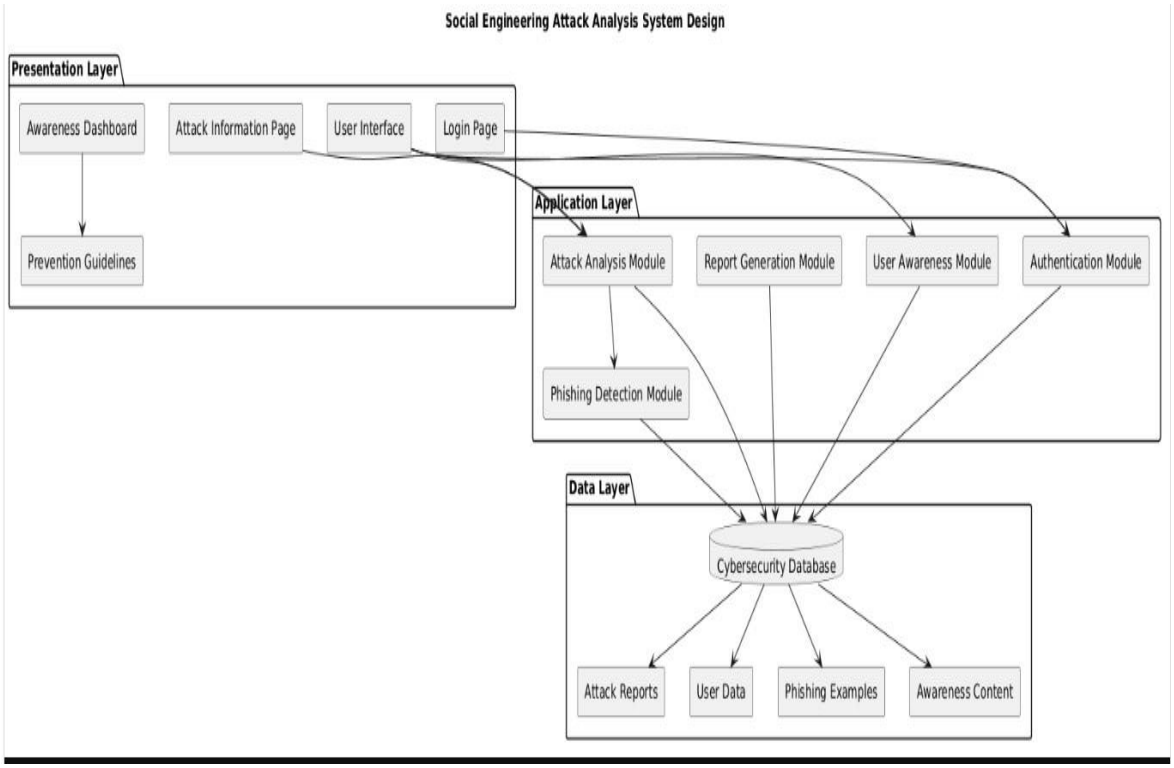
4. Prevention Techniques
The system studies various cybersecurity prevention methods such as:

- Strong password policies
- Multi-factor authentication
- Email filtering
- User awareness training
- Network security monitoring

5. User Awareness Module
The project provides cybersecurity awareness guidelines to help users identify suspicious emails, fake links, and fraudulent activities.

6. Result Analysis
The effectiveness of security awareness and prevention techniques is analyzed based on real-world attack scenarios.

IV. SYSTEM DESIGN



Hardware Requirements
Minimum Configuration

- Processor: Intel Core i3 or above
- RAM: 4 GB
- Storage: 100 GB HDD/SSD

Recommended Configuration

- Processor: Intel Core i5 / Ryzen 5

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155186

- RAM: 8 GB or more
- Storage: 250 GB SSD

Software Requirements

- Operating System: Windows/Linux
- Programming Language: Python
- Frontend: HTML, CSS, JavaScript
- Backend: Flask/Django
- Database: SQLite/MySQL
- Tools: VS Code, PyCharm

V. TYPES OF SOCIAL ENGINEERING ATTACKS

1. Phishing
Attackers send fake emails or websites pretending to be trusted organizations to steal login credentials.
2. Spear Phishing
A targeted phishing attack aimed at specific individuals or organizations.
3. Vishing
Voice phishing attacks performed through phone calls.
4. Smishing
SMS-based phishing attacks using fake text messages.
5. Baiting
Attackers offer fake rewards or free downloads to spread malware.
6. Pretexting
Attackers create fake scenarios to gain sensitive information.
7. Tailgating
Unauthorized individuals gain physical access to restricted areas by following authorized persons.

VI. RESULTS AND DISCUSSION

The study shows that social engineering attacks mainly exploit human behavior rather than technical vulnerabilities. Phishing remains the most common and dangerous attack type due to the widespread use of emails and online services. Cybersecurity awareness training significantly reduces the chances of successful attacks. Multi-factor authentication, spam filtering, and regular security updates also improve protection against cyber threats.
The project demonstrates that combining technical security measures with user awareness is the best approach to minimizing social engineering risks.

VII. CONCLUSION

Social engineering attacks are among the most dangerous cybersecurity threats because they target human psychology rather than software vulnerabilities. Attackers use manipulation techniques such as fear, trust, urgency, and curiosity to deceive users into revealing confidential information.

This project provides a detailed study of different social engineering attack techniques, their impact, and prevention methods. The research highlights the importance of cybersecurity awareness, strong authentication systems, and safe online practices in protecting users and organizations from cyber threats.

Overall, the project emphasizes that cybersecurity is not only about technology but also about educating users and improving human awareness against cybercrime.

VIII. FUTURE WORK

Future improvements for this project include:

- AI-based phishing detection systems
- Real-time cyber threat monitoring
- Integration with cybersecurity awareness platforms
- Mobile application for attack awareness
- Advanced email filtering mechanisms

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026
DOI: 10.17148/IJARCCE.2026.155186

- Behavioral analysis using Machine Learning
- Cloud-based cybersecurity monitoring systems

REFERENCES

[1]. Kevin Mitnick, *The Art of Deception: Controlling the Human Element of Security*, Wiley Publishing, 2002.
[2]. Christopher Hadnagy, *Social Engineering: The Science of Human Hacking*, Wiley Publishing, 2018.
[3]. IBM Security Report on Phishing Attacks, 2024.
[4]. Verizon Data Breach Investigations Report, 2024.
[5]. OWASP Social Engineering Guide.
[6]. National Institute of Standards and Technology (NIST) Cybersecurity Framework.
[7]. Research Papers on Cybersecurity and Social Engineering Attacks from IEEE Xplore and Google Scholar.

