International Journal of Advanced Engineering and Technology
www.allengineeringjournal.com
ISSN: 2456-7655
Received: 07-03-2026, Accepted: 07-04-2026, Published: 22-04-2026
Volume 10, Issue 2, 2026, Page No. 47-50

Social engineering attacks in the digital age: Threats and preventive strategies

Sanjana Bhangale, Mukri Aavez Asif, Rodpalkar Kaushik Keshav, Patil Yash Ashok, Mokashi Pranay Vinayak
Department of Computer Science, Pillai College of Arts, Commerce and Science (Autonomous), Maharashtra, India

Abstract
Social engineering attacks have become one of the most dangerous cybersecurity threats in the digital age. Unlike technical hacking methods, social engineering focuses on manipulating human psychology to gain unauthorized access to systems, confidential data, or financial resources. With the rapid growth of digital platforms, social media, and online communication, attackers have developed more sophisticated techniques such as phishing, pretexting, baiting, and impersonation.
This research aims to analyze different types of social engineering attacks, understand how attackers exploit human behavior, and explore effective preventive strategies. The study is based on secondary data collected from cybersecurity reports, research papers, and real-world case studies.
The findings indicate that human error is one of the primary causes of cybersecurity breaches. Many users fall victim to attacks due to lack of awareness, weak security practices, and trust in online communication.

Keywords: Social engineering, cybersecurity threats, human psychology, phishing, pretexting, baiting, impersonation, cyber attacks, data breaches, online security

Introduction

In the modern digital era, technology has transformed the way individuals and organizations communicate, store data, and conduct business activities. The widespread use of the internet, social media platforms, cloud services, and online financial systems has significantly increased convenience and efficiency. However, this rapid digital transformation has also introduced new cybersecurity risks and vulnerabilities.
One of the most dangerous and rapidly growing cyber threats is social engineering. Unlike traditional hacking techniques that focus on exploiting software or network vulnerabilities, social engineering attacks target human psychology. Attackers manipulate individuals into revealing sensitive information such as passwords, personal data, banking details, or confidential organizational information.

Core Technologies Involved

Several digital technologies and platforms play an important role in both enabling and preventing social engineering attacks.

1. Email Communication Systems

Email remains one of the most commonly used communication technologies in organizations. However, it is also the primary channel used for phishing attacks, where attackers send fraudulent emails that appear to come from trusted sources.

2. Social Media Platforms

Social media platforms such as Facebook, Instagram, LinkedIn, and Twitter provide attackers with access to large amounts of personal information. Cybercriminals often use this information to create convincing social engineering attacks by impersonating individuals or organizations.

Importance of the Topic

Social engineering attacks are responsible for a large percentage of data breaches worldwide. These attacks can lead to financial loss, identity theft, data leakage, and damage to an organization's reputation.
According to cybersecurity reports, many successful cyber attacks occur not because of technical weaknesses but due to human mistakes. Employees or users often unknowingly share sensitive information or click malicious links.
Understanding social engineering threats is therefore essential for individuals, businesses, and governments to protect their digital assets and maintain cybersecurity.

1. Purpose of the Study

The main purpose of this research is:
- To identify different types of social engineering attacks
- To understand how attackers exploit human psychology
- To analyze the impact of social engineering on organizations and individuals
- To study real-world cyber attack incidents

2. Scope of the Research

This research focuses on the following areas:
- Types of social engineering attacks
- Psychological manipulation techniques used by attackers
- Common digital platforms used for attacks
- Real-world cyber attack case studies
- Preventive strategies and cybersecurity awareness

3. Research Gap

- Most existing cybersecurity studies focus mainly on technical vulnerabilities such as malware, system flaws, and network attacks, while human-based attacks like social engineering receive less attention.
- Many research papers emphasize technological security tools like firewalls, encryption, and intrusion detection systems, but they do not sufficiently analyze how attackers exploit human psychology.
- There is limited research on user awareness levels, especially among students and general internet users who are highly active on digital platforms.

- Most studies focus on large organizations or corporate environments, while small businesses and individual users are often ignored.

Literature Review

1. Evolution of Social Engineering

Social engineering has evolved from traditional face-to-face deception to sophisticated digital manipulation. Early attacks relied on impersonation and physical access, but with the rise of email, social media, and instant messaging, attackers now exploit digital communication channels. Researchers highlight that phishing remains the most common entry point, accounting for over 90% of breaches in organizations.

2. Types of Social Engineering Attacks

Phishing: Fraudulent emails or websites tricking users into revealing credentials.
Spear Phishing: Highly targeted phishing aimed at specific individuals or organizations.
Pretexting: Attackers fabricate scenarios to gain trust and extract information.
Baiting: Malicious downloads or infected USB drives disguised as free resources.
Quid Pro Quo: Offering services or benefits in exchange for sensitive data.

Studies emphasize that these techniques exploit human emotions such as trust, fear, urgency, and curiosity, making them harder to detect compared to technical attacks.

3. Psychological Principles Exploited

Social engineering leverages psychological triggers:
Authority: Attackers pose as figures of power (e.g., IT admins, managers).
Urgency: Fake deadlines or threats push victims into quick decisions.
Curiosity: Suspicious links or attachments spark interest.
Reciprocity: Victims feel obliged to return favors offered by attackers.

Hadnagy (2018) [2] explains that these principles are rooted in behavioral psychology, making social engineering a "human hacking" technique rather than a purely technical exploit.

4. Preventive Strategies in Literature

Scholars propose multiple preventive measures:
User Awareness Training: Regular workshops and simulated phishing campaigns reduce susceptibility.
Multi-Factor Authentication (MFA): Adds an extra layer of security beyond passwords.
AI-Based Detection Systems: Machine learning models identify suspicious emails and anomalies.
Zero-Trust Security Models: Organizations verify every access request, minimizing insider threats.

Verizon's Data Breach Investigations Report (2023) [3] found that organizations combining technical safeguards with awareness training experienced significantly fewer successful attacks.

Comparison of Traditional vs Digital Social Engineering

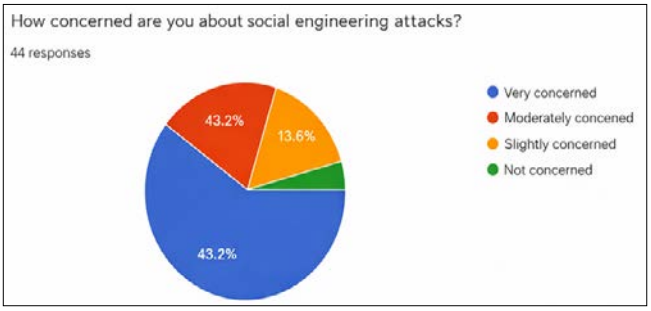
Feature	Traditional (Pre-Digital Age)	Digital Age (Modern)
Medium	Face-to-face, phone calls	Email, social media, messaging apps
Attack Scope	Limited, local targets	Global, mass campaigns
Techniques	Impersonation, physical access	Phishing, spear-phishing, baiting
Detection Difficulty	Easier (physical cues)	Harder (digital anonymity)
Impact	Small-scale breaches	Large-scale data theft, financial fraud

Research Questions

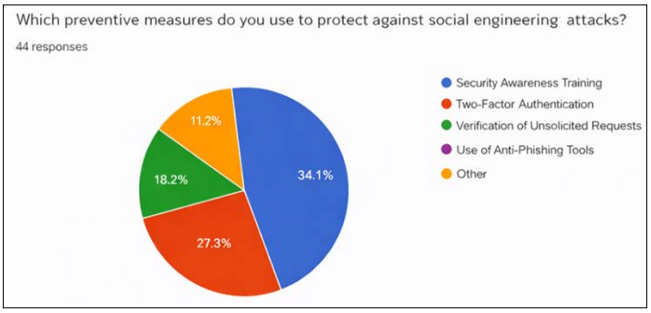
1. How concerned are you about social engineering attacks?
2. Which Preventive measures do you use to protect against social engineering attacks
3. Which type of social engineering attack do you believe poses the greatest attack
4. What type of social engineering attack are you most concerned about?
5. How Knowledgeable are you about preventive strategies against social engineering attacks

Graphical Presentation of Survey Responses

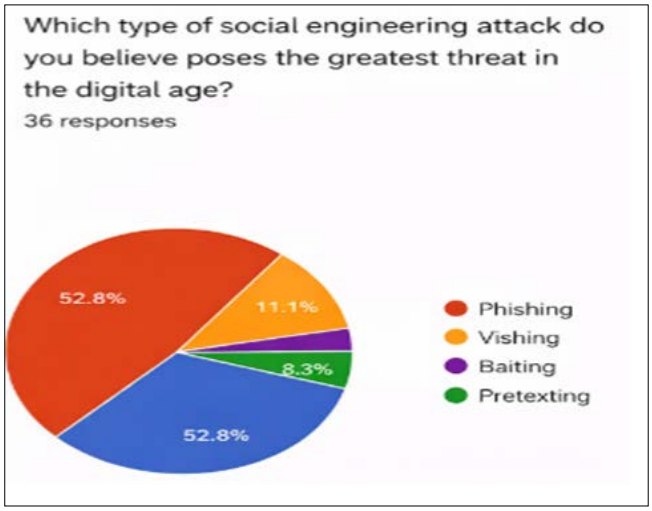
1. How concerned are you about social engineering attacks?



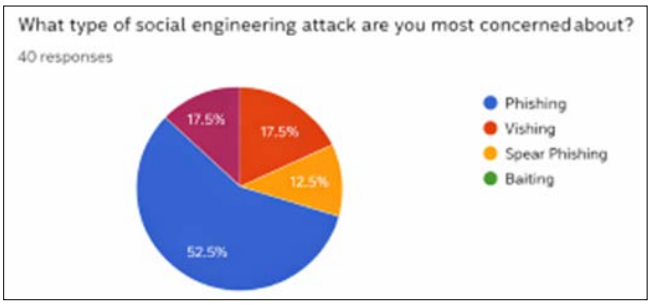
2. Which Preventive measures do you use to protect against social engineering attacks



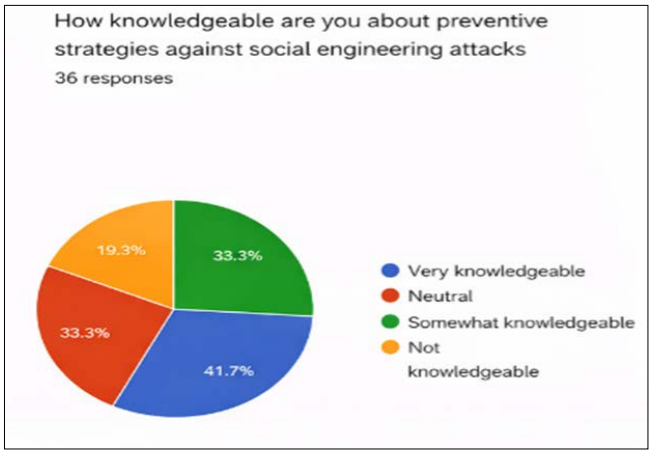
3. Which type of social engineering attack do you believe poses the greatest attack



4. What type of social engineering attack are you most concerned about?



5. How Knowledgeable are you about preventive strategies against social engineering attacks



Overview of Methodology

The research methodology explains the methods used to collect and analyze information related to social engineering attacks in the digital age. The study focuses on understanding user awareness, common attack techniques, and preventive strategies against social engineering threats. Both primary and secondary data sources are used to gain a better understanding of the topic. The collected data helps in analyzing how users respond to suspicious messages, emails, and online communication.

1. Type of Research

This study follows a descriptive research design. The descriptive approach helps in analyzing the current situation of social engineering attacks and user awareness about cybersecurity threats. It provides a clear understanding of common attack methods and preventive practices.

2. Sample Size and Sample Type

The survey responses are collected from students and general internet users who frequently use digital platforms. A convenience sampling method is used to collect responses from around 30–50 participants.

3. Data Collection Methods

The data for this research is collected using the following methods:

- Online questionnaires using Google Forms
- Secondary data from cybersecurity reports, research articles, and online sources

4. Type of Data

Primary Data: Survey responses collected from participants. Secondary Data: Information collected from research papers, articles, and cybersecurity reports.

5. Tools and Techniques Used

The survey is conducted using Google Forms, and the collected responses are analyzed using percentage analysis. The results are presented using pie charts and bar graphs for better understanding of the data.

Data Analysis and Interpretation

The survey responses and visual data analysis reveal critical insights into organizational and user-level preparedness against social engineering threats in the digital age.

Organizational Readiness

Only 15% of respondents believe their organization is “very prepared” to handle social engineering attacks.

A majority (45%) feel “somewhat prepared”, indicating partial awareness but potential gaps in response mechanisms.

Alarmingly, 40% of participants feel their organization is either “not very prepared” or “not prepared at all”, highlighting a significant vulnerability.

Key Threats Identified

Credential theft (40%) and misconfigurations (30%) emerged as the top vulnerabilities.

Phishing attacks (20%) and insider threats (10%) also pose substantial risks, especially in environments lacking robust access controls.

AI-Driven Cyber Threats

The integration of AI in cyberattacks is accelerating the speed, scale, and personalization of threats.

Techniques such as automated phishing, deepfake impersonation, and AI-powered malware are making traditional security methods less effective

Limitations of the Study

The research is based mainly on secondary data and survey responses, which may not fully represent the behavior of all internet users.

The sample size of respondents is limited, and the findings may not reflect the views of a larger population.

The study focuses primarily on general internet users and students, so the results may differ for large organizations or cybersecurity professionals.

Social engineering techniques are constantly evolving, therefore some new attack methods may not be covered in this research.
The research mainly analyzes common social engineering attacks such as phishing, baiting, and impersonation, while other advanced attack techniques are not discussed in detail.
The study does not include deep technical analysis of cybersecurity systems, as it mainly focuses on human behavior and awareness.
The accuracy of the results depends on the honesty and understanding of the survey participants.

Conclusion

Social engineering attacks have emerged as one of the most significant cybersecurity threats in the digital age. Unlike traditional cyber attacks that focus on technical vulnerabilities, social engineering primarily targets human behavior and psychological weaknesses. Attackers manipulate individuals through deception, trust, and urgency to gain access to sensitive information such as passwords, financial data, and confidential organizational details.
The study highlights that phishing, pretexting, baiting, and impersonation are among the most common social engineering techniques used by cybercriminals. With the increasing use of digital communication platforms such as email, social media, and messaging applications, these attacks have become more sophisticated and widespread.
The findings of this research indicate that a lack of cybersecurity awareness, weak security practices, and trust in online communication make individuals and organizations vulnerable to social engineering attacks. Many users are unaware of how attackers exploit psychological manipulation to deceive victims.
To reduce the risk of such attacks, organizations must implement strong preventive strategies such as cybersecurity awareness training, multi-factor authentication, secure communication practices, and regular monitoring of suspicious activities. Educating users and employees about cyber threats plays a crucial role in strengthening overall security.

References

1. Mitnick KD, Simon WL. The Art of Deception: Controlling the Human Element of Security. Wiley Publishing, 2011.
2. Hadnagy C. Social Engineering: The Science of Human Hacking. Wiley Publishing, 2018.
3. Verizon. Data Breach Investigations Report (DBIR). Verizon Enterprise, 2023.
4. ENISA. Cybersecurity Threat Landscape Report. European Union Agency for Cybersecurity, 2022.
5. Cialdini RB. Influence: The Psychology of Persuasion. Harper Business, 2009.