iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** V **Month of publication:** May 2025

DOI: https://doi.org/10.22214/ijraset.2025.72253

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue V May 2025- Available at www.ijraset.com

Social Engineering Attacks in Cybersecurity

Dr. S. Gomathi Alias Rohini[1], B. Rajashree[2], S. Shubha Sree[3]
Department of Computer Science, Sri Ramakrishna College of Arts and Science for Women, Coimbatore

Abstract: ***In recent years, social engineering has become one of the most insidious forms of cyber attack, exploiting human vulnerabilities rather than technical flaws. This paper aims to dissect the landscape of social engineering attacks, especially in the context of recent developments during 2024 and 2025. With advancements in artificial intelligence and deepfake technologies, attackers now possess sophisticated tools to deceive, manipulate, and breach systems through human interaction. The study explores traditional and emerging types of social engineering tactics, including phishing, vishing, baiting, pretexting, and impersonation using AI-generated media. It also provides a deep analysis of real-world incidents like the Snowflake data breach, Salesforce loader phishing, and deepfake impersonations. The goal is to foster awareness and reinforce the importance of security training, multi-layered authentication, and psychological resilience against manipulation. Based on current trends and academic research, this paper proposes robust mitigation strategies for organizations and individuals. In conclusion, as human factors remain an attractive vector for cybercriminals, understanding and countering social engineering must become a top priority in cybersecurity frameworks.***

Keywords: Social Engineering Attacks, Cybersecurity, Phishing Attacks, Security Awareness

I. INTRODUCTION

Cybersecurity has traditionally focused on technical defenses—firewalls, encryption, intrusion detection systems—but the weakest link often remains the human being. Social engineering exploits this vulnerability by psychologically manipulating individuals into revealing confidential information, performing actions that grant attackers access, or unknowingly aiding in cybercrimes. Unlike brute-force or malware-based attacks, social engineering leverages trust, urgency, authority, or curiosity to mislead victims. In recent years, the growth of generative AI and the widespread availability of personal information online have further empowered attackers. This paper explores how social engineering is evolving, analyzes real-world cases from 2024–2025, and suggests ways to mitigate such attacks.

II. MOST COMMON TYPES OF SOCIAL ENGINEERING ATTACKS

A. Phishing

Phishing is a cyber-attack technique in which attackers impersonate legitimate institutions or contacts to deceive individuals into revealing sensitive personal information, such as usernames, passwords, or banking details. It usually takes place through fraudulent emails or websites that appear genuine.

Example: A person receives an email from what appears to be their bank, stating that their account will be frozen unless they verify it. The email contains a link to a fake website that looks identical to the bank's login page. When the user enters their credentials, the attacker captures this information and uses it to access the actual bank account.

B. Spear Phishing

Spear phishing is a more targeted and personalized version of phishing. Rather than sending mass emails, the attacker researches the victim to create a customized message that appears more legitimate and convincing. This attack often uses details like the victim’s name, job title, or personal interests.

Example: An employee at a marketing firm gets an email from someone pretending to be their department head. The message includes the employee’s name and references an actual ongoing project. It requests them to share confidential campaign files via a shared drive. The employee, convinced by the familiarity of the message, uploads the files to the attacker’s link.

C. Baiting

Baiting involves enticing the victim with a promise of something appealing, such as free software, gift cards, or exclusive content. In reality, the “bait” is a trap designed to install malware or steal information once the user interacts with it.

Example: A user sees an online advertisement claiming they can download a free version of an expensive photo editing software. Upon downloading and running the program, the user unknowingly installs spyware on their system, giving the attacker access to their files and activities.

D. Pretexting

Pretexting is a type of attack where the attacker creates a fabricated story or identity to gain the victim's trust and extract confidential information. It often involves impersonating authority figures, colleagues, or trusted service providers.
Example: An attacker calls an employee pretending to be from the IT department, claiming there is a security breach. They request the employee's login credentials to "secure" the account. Believing the story, the employee shares their password, which the attacker then uses to access sensitive company data.

E. Smishing (SMS Phishing)

Smishing is a variant of phishing that uses SMS (Short Message Service) or text messages to deceive victims into revealing private information or clicking malicious links. These messages often use urgency or threats to prompt immediate action.
Example: A user receives a text that says, "Your credit card has been blocked. Click the link to verify your identity: [malicious link]." If the user clicks the link, it either directs them to a fake website asking for banking details or installs malicious software on their mobile device.

F. Quid Pro Quo

Quid Pro Quo attacks involve offering something valuable in exchange for information. Unlike baiting, where the offer is passive, this method involves direct communication offering help or benefits in return for access or data.
Example: A person calls several employees in a company, claiming to be from technical support and offering to "upgrade" their system for better performance. When someone agrees, the caller asks for their system login credentials to proceed, which are then misused.

G. Tailgating (Piggybacking)

Tailgating is a physical breach of security where an unauthorized individual follows an authorized person into a restricted area. This is often done by exploiting human courtesy, such as someone holding a door open for them.
Example: An attacker dresses as a courier and waits near the entrance of a secure office. When an employee opens the door using their access card, the attacker requests them to hold the door, saying they forgot their badge. The unsuspecting employee lets them in, unknowingly allowing a security breach.

Fig 1. Most Common type of Social engineering Attacks

III. REAL WORLD USE CASES

A. Snowflake Data Breach (2024)

In mid-2024, Snowflake—a cloud-based data warehousing company—became the focal point of a major cyber incident involving unauthorized access to its customers' data. Interestingly, the breach did not occur due to a vulnerability within Snowflake's infrastructure itself. Instead, attackers exploited compromised user credentials obtained from previous data leaks and phishing campaigns. These credentials were reused by employees of multiple organizations that utilized Snowflake's services.

Many accounts lacked Multi-Factor Authentication (MFA), which allowed attackers to log in directly. Once access was gained, the attackers siphoned off massive volumes of sensitive data. Notably, customers like Ticketmaster and Santander Bank were impacted, with data including payment details, customer information, and transaction histories being stolen and later sold on the dark web.

Key Insight:

This incident exemplifies how attackers combine credential stuffing (using stolen passwords) with social engineering (posing as legitimate users). It underscores the need for enforcing MFA and regular credential hygiene.

B. Salesforce Data Loader Phishing Attack (2025)

In 2025, a phishing campaign targeted employees from various organizations who use Salesforce CRM tools. The attackers crafted a clone of the Salesforce Data Loader, a widely used desktop tool for importing and exporting Salesforce data.

Employees received authentic-looking emails appearing to come from Salesforce support, urging them to download an "updated" version of the Data Loader due to "critical security updates." To add credibility, some victims were even called (vishing) by people impersonating Salesforce technical staff, a technique that increased the success rate significantly.

Victims who downloaded and installed the fake tool unknowingly installed malware. The tool recorded credentials and gave attackers backdoor access to internal systems. Some businesses saw confidential customer data being leaked and sold.

Key Insight**:**

This attack shows how combining phishing, vishing, and software tampering can successfully bypass both technical controls and employee skepticism. It also reveals the dangers of trusting updates from unofficial sources.

C. Deepfake Voice Attack Targeting Susie Wiles (2025)

A politically driven social engineering attack in 2025 involved the use of AI-generated deepfake audio to impersonate Susie Wiles, a senior advisor to former U.S. President Donald Trump. The attacker created an audio clip of Wiles requesting sensitive campaign information and coordinated a phone call using the voice clone to a campaign staffer.

The voice sounded convincingly real—mimicking tone, pitch, and speaking patterns—and was backed by real contextual information, likely gathered from public social media and insider contacts. The recipient, unaware of the deception, revealed confidential strategy documents, believing they were fulfilling a direct request from their superior.

Key Insight:

Deepfake-based social engineering marks a new era in cyberattacks, where audio and video manipulation adds authenticity to deception. This case highlights the need for multi-channel verification before acting on sensitive voice requests.

D. Vishing Attack on M&S and Co-op (2025)

In early 2025, two British retail giants—Marks & Spencer and Co-op—were hit by sophisticated voice phishing (vishing) scams. Attackers made phone calls to internal help desks, impersonating staff members who had "forgotten their credentials" or had an "urgent system lockout."

Using publicly available employee details (from LinkedIn, data breaches, or social engineering pretexting), the attackers constructed convincing narratives. In some cases, they even spoofed internal phone numbers. The support personnel, not suspecting any foul play, reset credentials or granted temporary access, which was later abused to infiltrate backend systems and retrieve sensitive operational data.

Key Insight:

Even in large enterprises, help desks can be manipulated if proper verification protocols are not in place. This highlights the importance of strict identity checks during support calls and better employee training.

E. Iranian Bank Sepah Hack (2025)

In one of the more geopolitically significant cyber incidents of 2025, Bank Sepah, one of Iran's leading state-owned banks, was breached using classic social engineering tactics. The campaign began with spear-phishing emails sent to senior employees, containing personalized content and a malicious attachment that appeared to be an internal financial document.

Once opened, the malware installed a remote access trojan (RAT), giving attackers access to internal files and email servers. Over weeks, sensitive financial documents, emails, and internal communications—some linked to high-ranking government officials—were exfiltrated and leaked online by a politically motivated hacking group.

Key Insight:
This case shows how targeted phishing campaigns combined with insider reconnaissance can yield devastating results, particularly when aimed at critical infrastructure. It also emphasizes the role of geopolitical motives in modern social engineering attacks.

IV. PREVENTION AND MITIGATION STRATEGIES

Social engineering remains one of the most pervasive cybersecurity threats due to its reliance on human vulnerabilities. This section explores key strategies aimed at preventing and mitigating social engineering attacks, with a focus on technical measures, policy controls, and human-centric approaches.

A. Security Awareness and Behavioral Training

Security awareness training is a critical component of organizational defense mechanisms against social engineering. It aims to educate employees on identifying deceptive tactics such as phishing, pretexting, and baiting, thereby reducing human error—the most exploited vector in cyberattacks.
One practical implementation involves conducting simulated phishing exercises. For example, an organization may distribute a mock email with a subject line such as "Your Leave Request Has Been Cancelled – Click Here for Details." Employees who interact with the deceptive link are redirected to an educational module explaining the phishing technique used.
Best Practices for effective awareness training include:

- Scheduling training sessions on a monthly or quarterly basis.
- Utilizing real-world scenarios, such as CEO impersonation or LinkedIn-based phishing.
- Performing unannounced simulations to gauge actual preparedness levels.

B. Multi-Factor Authentication (MFA)

Multi-Factor Authentication adds an additional layer of security by requiring two or more forms of verification: typically a combination of something the user knows (e.g., a password), something the user has (e.g., a time-based OTP), and something the user is (e.g., fingerprint or facial recognition).
This approach is especially effective in neutralizing stolen credentials. Consider a case where a user is tricked into revealing their email password. An attacker attempting unauthorized access is thwarted when prompted for an OTP sent to the user's mobile device, thereby containing the breach.
Recommended Practices include:

- Enabling MFA for all privileged, financial, and remote access accounts.
- Utilizing authenticator apps over SMS to reduce SIM-swap risks.
- Mandating MFA for all major SaaS platforms such as Office 365 and AWS.

C. Incident Response Planning (IRP)

An Incident Response Plan is a predefined set of procedures for detecting, responding to, and recovering from security breaches. A well-documented IRP ensures that the organization can act swiftly and decisively when a social engineering incident occurs.
For instance, if an employee mistakenly sends sensitive data to a spoofed HR email, the IRP would guide the team to immediately disable compromised credentials, notify the legal and compliance departments, and initiate an audit of system logs to assess further exposure.
Core Elements of a robust IRP include:

- Clearly assigned roles and responsibilities.
- Defined procedures for threat identification, containment, and recovery.
- Post-incident review mechanisms for continuous improvement.

D. Role-Based Access Control (RBAC)

RBAC limits access to systems and information based on a user's specific role within the organization, adhering to the principle of least privilege. This model reduces the risk surface in the event of credential compromise resulting from social engineering.
A practical example can be drawn from a scenario where a junior HR assistant is manipulated into opening a malicious attachment. Because access controls restrict the user to entry-level HR documents, the scope of the breach remains confined.

Implementation Guidelines:

- Assign minimal access rights upon onboarding.
- Conduct periodic audits to validate access requirements.
- Revoke or reassign privileges promptly during role transitions.

E. Email Filtering and Anti-Phishing Tools

Email remains the most common vector for social engineering attacks. Advanced email filtering solutions analyze metadata, URLs, attachments, and sender information to identify and neutralize threats before they reach end-users.

In one scenario, an attacker disseminates a fake invoice embedded with malware to employees across an organization. An AI-driven email security gateway detects the malicious content through heuristic analysis and quarantines the email, effectively neutralizing the threat.

Advanced Capabilities may include:

- Artificial Intelligence (AI) and Machine Learning (ML) models for dynamic threat detection.
- Implementation of DMARC, SPF, and DKIM for domain validation.
- URL sandboxing and real-time attachment scanning.

F. Penetration Testing with a Social Engineering Focus

Penetration testing traditionally targets technical vulnerabilities but can be expanded to assess human and procedural weaknesses via social engineering simulation. This approach exposes potential failures in employee behavior and organizational policy.

A controlled penetration test may involve a red team member impersonating an IT staffer and contacting employees to obtain VPN credentials. The results—such as a 20% failure rate in this case—can inform immediate corrective actions and future training needs.

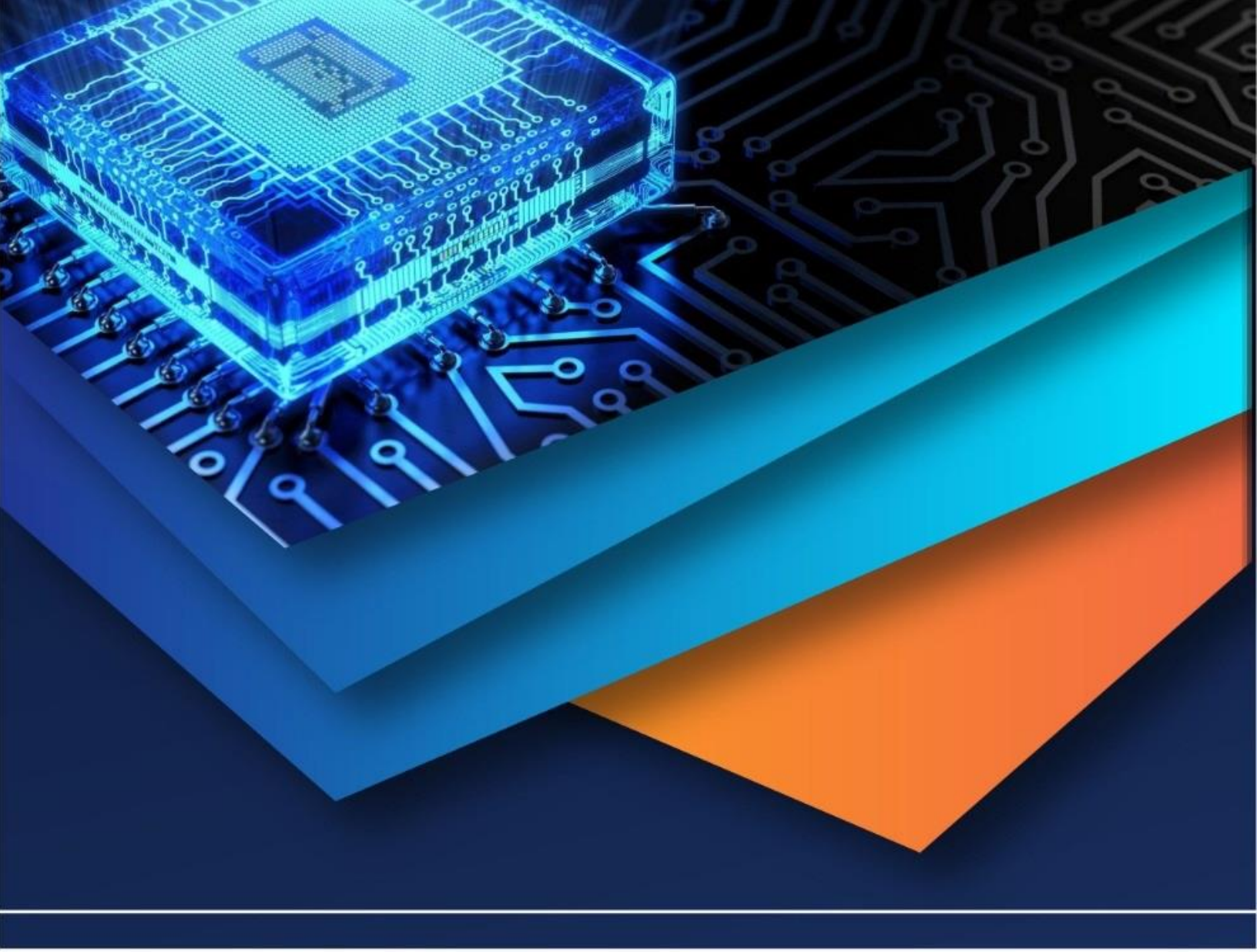
V. CONCLUSION

Social engineering remains a major cybersecurity threat because it targets human weaknesses rather than technical flaws. Recent incidents from 2024–2025 highlight how attackers are using advanced methods such as AI-generated deepfakes to trick individuals and organizations. To defend against these evolving threats, a combination of continuous employee training, strong authentication methods like MFA, strict access controls, and well-prepared incident response plans is essential. Regular testing and monitoring further strengthen defenses. Ultimately, enhancing human awareness and promoting security-conscious behavior are critical to reducing the success of social engineering attacks and protecting valuable assets.

6,8.9,10.14,20

REFERENCES

[1] https://cybersecurity.springeropen.com/articles/10.1186/s42400-021-00094-6
[2] https://www.sciencedirect.com/science/article/pii/S2451958821000749
[3] https://www.mdpi.com/1999-5903/11/4/89
[4] https://www.wiley.com/en-us/Social+Engineering%3A+The+Science+of+Human+Hacking%2C+2nd+Edition-p-9781119433385
[5] https://www.wiley.com/en-us/The+Art+of+Deception%3A+Controlling+the+Human+Element+of+Security-p-9780764544682
[6] https://asistdl.onlinelibrary.wiley.com/doi/abs/10.1002/asi.20779
[7] https://www.securityhq.com/blog/7-types-of-social-engineering-attacks-targeting-you
[8] https://www.mitnicksecurity.com/blog/types-of-social-engineering-attacks
[9] https://www.crowdstrike.com/en-us/cybersecurity-101/social-engineering/types-of-social-engineering-attacks
[10] https://www.terranovasecurity.com/blog/examples-of-social-engineering-attacks
[11] https://www.tripwire.com/state-of-security/5-social-engineering-attacks-to-watch-out-for
[12] https://www.nightfall.ai/blog/5-types-of-social-engineering-attacks-and-how-to-mitigate-them
[13] https://keepnetlabs.com/blog/what-are-common-examples-of-social-engineering-attacks
[14] https://secureframe.com/blog/most-common-social-engineering-attacks



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY