iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** III **Month of publication:** March 2026

DOI: https://doi.org/10.22214/ijraset.2026.78962

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 14 Issue III Mar 2026- Available at www.ijraset.com

The Rise of Social Engineering: Threats, Techniques, and Countermeasures in the Digital Age

Naman Kumar[1], Nikhil Mehta[2]
Chandigarh Group of Colleges, Landran, Mohali, Punjab, India (Affiliated to I.K. Gujral Punjab Technical University, Jalandhar), Mohali, Punjab, India

Abstract: ***Social engineering has emerged as one of the most pervasive and consequential cybersecurity threats in the modern digital era. Unlike conventional cyberattacks that exploit software vulnerabilities, social engineering manipulates human psychology to gain unauthorized access to systems, data, or physical facilities. This paper examines the historical evolution of social engineering, classifies its major attack categories, analyses the psychological and cognitive mechanisms that render individuals susceptible, and surveys the documented impact on both individuals and organisations worldwide. Furthermore, this paper evaluates existing detection technologies and proposes a multi-layered defence framework. The study underscores that technical safeguards alone are insufficient; cultivating a security-conscious organizational culture and delivering continuous user education are equally indispensable. The paper concludes with an assessment of emerging attack vectors facilitated by artificial intelligence and deepfake technologies, and recommends directions for future research.***

Keywords: Social engineering, phishing, pretexting, cybersecurity, human factor, cognitive bias, vishing, deepfake, countermeasures, security awareness.

I. INTRODUCTION

Therapid proliferation of internet-connected devices, cloud services, and digital communication platforms has fundamentally reshaped the global threat landscape. While organisations invest heavily in firewalls, intrusion-detection systems, and cryptographic protocols, adversaries have learned that the most accessible point of entry into any secure system is often the human being sitting in front of it. This insight forms the basis of social engineering—the art of manipulating people into divulging confidential information or performing actions that compromise security.

The term gained prominence through the work of Kevin Mitnick, a former hacker who famously stated that human beings are the weakest link in any security chain. Since then, social engineering has evolved from rudimentary impersonation and confidence tricks into sophisticated, data-driven campaigns that can deceive even highly trained professionals. The global cost of cybercrime, much of which is initiated through social engineering, was estimated at over USD 8 trillion in 2023, with projections suggesting it could exceed USD 10 trillion annually by 2025 (Cybersecurity Ventures, 2023).

For students pursuing a Master of Computer Applications (MCA), a thorough understanding of social engineering is not merely academic. It is a practical necessity. System architects, software developers, and IT managers must design and maintain systems that account for human fallibility. This paper aims to provide a comprehensive, analytically rigorous examination of social engineering, addressing its mechanisms, real-world manifestations, and countermeasures.

II. HISTORICAL BACKGROUND AND EVOLUTION

Social engineering is not a product of the digital age. Its roots extend to ancient military stratagems, confidence swindles, and espionage. The Trojan Horse—recounted in Homer's Iliad—is often cited as the archetypal social engineering attack, in which deception rather than force was used to breach an impregnable fortress. In the twentieth century, telephone-based manipulation, commonly known as phreaking, allowed individuals to exploit the trust placed in voice communication to obtain sensitive information or free long-distance calls. The transition to the internet age accelerated the scale and sophistication of social engineering considerably. Phishing emerged in the mid-1990s as attackers began sending mass emails impersonating legitimate institutions such as banks and internet service providers.

By the early 2000s, targeted spear-phishing campaigns were being conducted against government agencies and multinational

corporations. The 2011 RSA Security breach—in which attackers sent spear- phishing emails to employees and ultimately compromised the company's SecurID token system— demonstrated that even security firms themselves were not immune. More recently, the 2020 Twitter hack, in which attackers used phone-based social engineering to compromise internal tools and take over high-profile accounts, revealed that social engineering had become a primary vector even for technically sophisticated actors.

III. CLASSIFICATION OF SOCIAL ENGINEERING ATTACKS

Social engineering attacks can be classified along several dimensions: the communication channel employed, the psychological trigger exploited, and the target—individual or organisational. The following sub-sections describe the major categories.

A. Phishing and its Variants

Phishing encompasses a broad family of attacks in which the adversary impersonates a trusted entity—a bank, a government agency, a colleague, or a technology vendor—to induce the victim into revealing credentials, clicking on malicious links, or transferring funds. Spear phishing is a targeted variant directed at a specific individual or department, often leveraging personal information harvested from social media. Whaling specifically targets senior executives. Vishing (voice phishing) exploits telephone calls, while smishing employs SMS text messages.

Clone phishing involves duplicating a legitimate email and replacing its links or attachments with malicious ones.

B. Pretexting

Pretexting involves the fabrication of a convincing scenario to extract information or gain access. An attacker might pose as an IT support technician needing an employee's login credentials to resolve a system error, or as a bank auditor requiring account numbers for a compliance review. Pretexting attacks are particularly effective because they exploit the victim's willingness to be cooperative and helpful—prosocial behaviours that organisations actively encourage in their culture.

C. Baiting and Quid Pro Quo

Baiting attacks exploit human curiosity or the desire for gain by offering something enticing. A classic example involves leaving malware-infected USB drives in a company car park; curious employees who plug the devices into their workstations unwittingly install malware. Quid pro quo attacks follow a similar logic but involve an exchange: the attacker offers a service—commonly technical assistance—in return for information. Research has shown that a surprising number of employees will provide passwords to strangers who offer a small incentive such as a pen or chocolate bar.

D. Tailgating and Physical Intrusion

Not all social engineering attacks are digital. Tailgating—or piggybacking—occurs when an attacker gains physical access to a restricted area by following an authorised person through a secured door, often by presenting themselves as a delivery person or maintenance worker. Once inside, the attacker may install hardware keyloggers, photograph confidential documents, or gain direct access to networked terminals. Physical intrusion highlights the importance of comprehensive security policies that extend beyond the digital perimeter.

IV. PSYCHOLOGICAL MECHANISMS AND COGNITIVE BIASES

The effectiveness of social engineering derives from its systematic exploitation of well- documented cognitive biases and psychological principles. Robert Cialdini's foundational work on the psychology of influence identifies six key principles—reciprocity, commitment, social proof, authority, liking, and scarcity—each of which is routinely weaponised by social engineers. Authority exploits the human tendency to comply with perceived figures of power. An attacker impersonating a company's CEO and demanding an urgent wire transfer invokes the principle of authority. Scarcity and urgency trigger fear of missing out or fear of negative consequences, compelling victims to act before they have time to verify a request. Social proof leads individuals to follow the perceived behaviour of others: attackers may claim that several of the victim's colleagues have already complied with a request. Liking ensures that targets are more susceptible to requests from individuals they find attractive, familiar, or similar to themselves—hence social engineers often research their targets extensively before making contact.

Beyond Cialdini's principles, social engineers exploit dual-process theory. System 1 cognition—fast, intuitive, and automatic—dominates under conditions of time pressure, emotional arousal, or information overload, precisely the conditions that skilled social engineers create. When individuals are rushed or frightened, their capacity for critical evaluation is severely diminished, making them significantly more likely to comply with illegitimate requests.

V. DOCUMENTED IMPACT AND CASE STUDIES

The financial, reputational, and operational damage inflicted by social engineering attacks is substantial and growing. According to the Verizon Data Breach Investigations Report (DBIR) 2023, phishing was involved in 36% of all confirmed data breaches, and business email compromise (BEC)—a form of spear phishing—accounted for losses exceeding USD 2.7 billion in the United States alone.

The 2019 Toyota Boshoku BEC incident resulted in a loss of approximately USD 37 million after an attacker convinced a finance executive to change bank account details for a large transfer. The 2020 SolarWinds supply-chain attack, while primarily technical, was facilitated at an early stage by social engineering targeting employees. In healthcare, phishing attacks have compromised patient records, exposed protected health information, and in some instances disrupted clinical operations, with documented consequences for patient safety.

At the individual level, victims of social engineering may suffer identity theft, financial loss, and severe psychological distress. The reputational damage to organisations extends beyond direct financial loss to include regulatory penalties under frameworks such as the General Data Protection Regulation (GDPR), erosion of customer trust, and long-term market capitalisation effects.

VI. DETECTION TECHNOLOGIES AND COUNTERMEASURES

Combating social engineering requires a defence-in-depth strategy that integrates technical controls, procedural safeguards, and human-centred interventions. No single measure is sufficient in isolation.

A. Technical Controls

Email authentication protocols—SPF, DKIM, and DMARC—significantly reduce domain spoofing. AI-powered email filtering systems can detect anomalous sender behaviour, suspicious links, and linguistic patterns characteristic of phishing. Multi-Factor Authentication (MFA) mitigates the impact of credential theft, because even if an attacker obtains a password, access to the account requires an additional authentication factor. Web content filtering and sandboxing of email attachments prevent malicious payloads from executing. Caller-ID verification and AI-based voice analysis tools are being developed to counter vishing.

B. Procedural and Policy Safeguards

Organisations must establish and enforce clear verification procedures for sensitive requests, particularly those involving financial transactions, credential resets, or the release of personal data. The four-eyes principle—requiring two authorised individuals to approve high-risk actions— limits the exposure created by a single compromised employee. Incident response plans should explicitly address social engineering scenarios, including BEC and vishing attacks, with defined escalation paths and communication protocols.

C. Security Awareness and Training

Research consistently demonstrates that regular, engaging security awareness training reduces susceptibility to phishing and other social engineering attacks. Simulated phishing exercises—in which the organisation's own security team sends test phishing emails to employees—provide immediate, personalised feedback and measurable data on vulnerability. Training programmes should emphasise recognition of psychological manipulation tactics, verification procedures for unsolicited requests, and safe reporting channels so that employees who suspect an attack feel empowered rather than embarrassed to report it. A blame-free reporting culture is essential to ensure that incidents and near-misses are surfaced promptly.

VII. EMERGING THREATS: AI, DEEPFAKES, AND ADVANCED PERSISTENT SOCIAL ENGINEERING

Advances in artificial intelligence are dramatically expanding the toolkit available tosocial engineers. Large language models can generate highly fluent, contextually appropriate phishing emails in any language, eliminating the grammatical errors that once served as a warning sign.

AI- powered voice cloning allows attackers to replicate the voice of a trusted individual with a few seconds of audio sample, enabling highly convincing vishing attacks. In 2023, a multinational corporation reportedly lost USD 25 million after a finance employee was deceived during a video conference call in which all other participants were deepfake simulations of company executives.

Advanced Persistent Social Engineering (APSE) refers to prolonged, multi-stage campaigns in which attackers cultivate relationships with targets over weeks or months before executing an attack. State-sponsored threat actors have been documented

using fabricated social media personas to befriend defence researchers and employees of critical-infrastructure organisations before delivering malware or extracting sensitive information. Addressing AI-enhanced social engineering will require new detection paradigms, including behavioural biometrics, liveness detection for video communications, and real-time deepfake identification tools. Regulatory frameworks must also evolve to hold platforms accountable for the misuse of AI-generated content in fraud.

VIII. CONCLUSION

Social engineering represents a persistent and escalating threat to digital security, one that cannot be addressed through technical means alone. Its effectiveness rests on fundamental and relatively stable features of human cognition—the tendency to trust authority, to respond to urgency, and to extend goodwill to those who appear familiar or cooperative. As long as these psychological traits exist and as long as organisations depend on human decision-making, social engineering will remain a viable and highly cost-effective attack vector for adversaries.

The emergence of AI-generated content, deepfake media, and autonomous phishing tools signals that the threat will intensify considerably in the coming years. Organisations and individuals must respond with layered, adaptive defences: robust technical controls, clear verification protocols, a

healthy culture of security scepticism, and sustained investment in human awareness training.

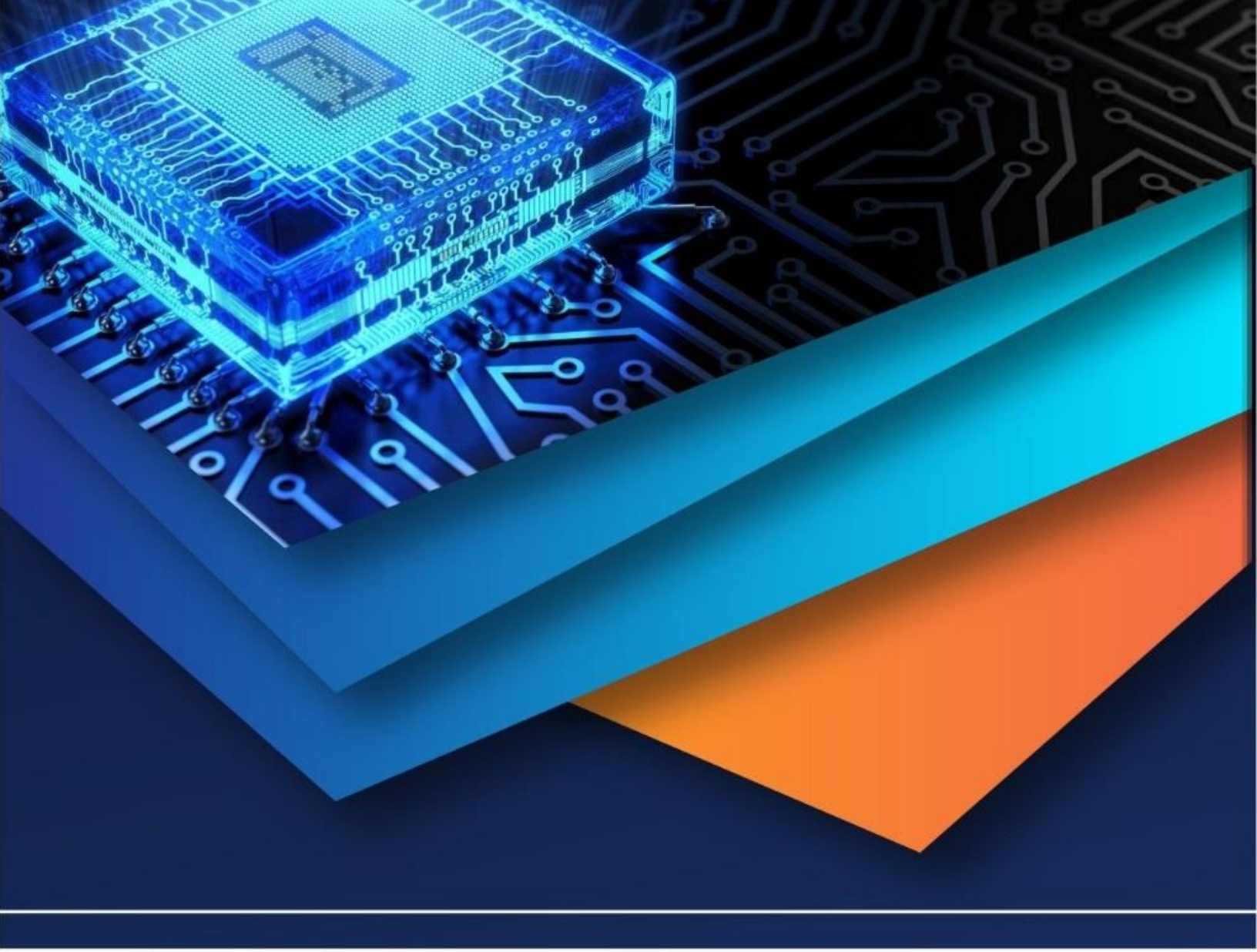
MCA graduates entering the IT profession carry a particular responsibility to design systems that minimise the attack surface presented by human factors and to advocate within their organisations for security practices that are both technically sound and humanistically informed. Future research

should focus on adaptive, personalised training methodologies, the development

of AI detection standards for deepfake communications, the psychology of susceptibility across different demographic and cultural groups, and the legal frameworks needed to prosecute social engineering attacks effectively across international jurisdictions.

REFERENCES

[1] Cialdini,R.B.(2001). Influence: Science and practice (4th ed.). Allyn & Bacon.
[2] Cybersecurity Ventures. (2023). Cybercrime to cost the world $8 trillion in 2023. Cybersecurity Ventures. Hadnagy, C. (2010). Social engineering: The art of human hacking. Wiley Publishing.
[3] Hadnagy, C., & Fincher, M. (2015). Phishing dark waters: The offensive and defensive sides of malicious emails. Wiley.
[4] Kahneman, D. (2011). Thinking, fast and slow. Farrar, Straus and Giroux.
[5] Mitnick, K. D., & Simon, W. L. (2002). The art of deception: Controlling the human element of security. Wiley.
[6] NCSC. (2023). Phishing attacks: Defending your organisation. National Cyber Security Centre.
[7] Proofpoint. (2023). State of the phish 2023: An in-depth exploration of user awareness, vulnerability, and resilience. Proofpoint, Inc.
[8] Symantec Corporation. (2022). Internet security threat report. Symantec.
[9] Verizon. (2023). 2023 Data breach investigations report. Verizon Communications.
[10] Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social
[11] engineering threats to information security. Journal of the American Society for Information Science and Technology, 59(4), 662–674.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY