Volume: 13 Issue: VI Month of publication: June 2025

DOI: https://doi.org/10.22214/ijraset.2025.72502

Understanding Human Vulnerabilities: A Study on Social Engineering Techniques in Cybersecurity

Suramyaa Rajalim
Department of Computer Science, Sikkim Manipal Institute of Technology

Abstract: Social engineering exploits human nature to bypass technical security controls and is thus a threatening cyber-attack. This paper explains common techniques such as phishing and pretexting, examines real-world examples, and explains why these attacks are successful. This highlights the need for user training and awareness in combating such attacks.

I. INTRODUCTION

Although the threat environment for cybersecurity is constantly evolving, technological defences such as firewalls, antivirus solutions, and intrusion detection systems are generally prioritized. Of all the vulnerabilities, perhaps the most important and most frequently exploited is not through systems but through individuals. Social engineering attacks rely on psychological manipulation to persuade individuals to divulge sensitive information or perform actions that compromise security. These attacks do not use traditional defences because they exploit the human factor; therefore, they are subtle and difficult to detect.

Social engineering has been used in some of the most prominent cyberattacks of the recent past, such as the 2020 Twitter Bitcoin scam and a wide range of large-scale phishing attacks against corporations and government departments. Phishing, pretexting, baiting, and tailgating exploit trust, authority, urgency, and curiosity to make users drop their guard. As an increasing number of companies rely on electronic communication and remote access, the dangers of social engineering have become increasingly dominant.

This paper provides a detailed explanation of common social engineering techniques, examines the psychological principles behind their success, and details preventive measures that individuals and organizations can take. Understanding how and why these attacks have been successful allows stakeholders to better prepare to defend against them, to the extent that cybersecurity is not just a technical problem but a human one.

II. LITERATURE SURVEY

Social engineering is an ongoing threat in current cybersecurity, more reliant on psychology than on the weaknesses of technology. Recent academic studies have greatly added to what we already understand about behavioural, contextual, and technological factors of susceptibility to these attacks.

Albladi and Weir [1] compared online usage patterns and personality characteristics of users to identify which users are most vulnerable to social engineering attacks. In their research, susceptibility is best correlated with openness and agreeableness personality characteristics and the users' knowledge of cybersecurity.

Hadnagy [2] expanded on traditional approaches in his book Social Engineering: The Science of Human Hacking published in 2018, covering new threats such as deepfake impersonation and AI voice synthesis. The book offers real-world examples of how attackers exploit trust and communication technology currently.

Almohammadi, Alqahtani, and Alzahrani [3] developed an in-depth taxonomy for social engineering attacks and categorized them based on delivery vectors, psychological strategies, and implementation stages. Their taxonomy provides a structured methodology for organizations to be prepared and respond to different threats.

Okereafor, Adeyemi, and Udechukwu [4] conducted field experiments in organizational settings with phishing simulations. Experiential learning, as employees are exposed to simulated phishing attempts with instant feedback, they found, produces measurable gains in resilience.

Alghamdi and van Moorsel [5] investigated cognitive heuristics in social engineering contexts of user decision making. They found that pressure, authority, and emotional pressure, especially in multitasking, significantly undermine users' ability to detect deception.

Fatima and Wang [6] understood the double-edged nature of artificial intelligence in social engineering. AI is used in hyper-personalized phishing, but it is utilized in anomaly-based intrusion detection. Their paper discusses the investment into AI-based defensive technologies that consider human mistakes.

All these papers together point to a shift towards emphasis on human-oriented security, where psychology, training design, and AI technologies are combined to address the persistent and ever-changing threat of social engineering.

III. COMMON SOCIAL ENGINEERING TECHNIQUES

Social engineering utilizes psychological deception instead of technical exploits to compromise security controls. Attackers deceive users into divulging sensitive data or undertaking destructive endeavours by taking advantage of trust, authority, urgency, and curiosity. Most prevalent social engineering techniques in current cyberattacks are described below.

A. Phishing

Phishing is the most common form of social engineering, in which attackers pretend to be trusted sources through email, SMS, or imposter sites to trick users into divulging confidential information. They are primarily in the form of threatening emails like ”Your account is compromised” or ”Action is required now.” Clicking on harmful links can result in victims being directed to imposter sites that steal their credentials or introduce malware [7]. Variants of phishing include:

- Spear phishing: Highly targeted attacks with custom information, typically gathered from social networks or previous penetrations.
- Whaling: Targeting high-value individuals, such as executives or government members.
- Smishing: Phishing performed through SMS or messaging applications.
- Pharming: Directing users to counterfeit websites despite entering the correct URL.

B. Vishing (Voice Phishing)

Vishing is a phone call or an automated voice that mimics real institutions, such as banks, insurance, or government institutions. The attacker normally informs the victim that they have noticed some unusual activity on their account and requests that the victim confirm their credentials or financial data [8].

A good example is fake calls purporting to be from the IRS (its foreign equivalent), threatening legal action if payment is not made promptly. Scammers employ caller ID spoofing to make the number look legitimate, giving the scam even more validity.

Research has proven that vishing exploits cognitive stress, with stressed users being less vigilant in assessing the situation [9].

C. Pretexting

Pretexting relies on creating a credible pretext upon which to base the manipulation of the victim into a disclosure or action. The attacker typically assumes the role of a person in authority, such as a corporate executive, law enforcement officer, or system administrator, and uses insider-sounding language to gain credibility [9].

In contrast to mass-targeted phishing, pretexting is highly targeted and can entail extended interactions. For instance, the attacker may pose as an auditor of a company requesting payroll data or customer information for a bogus compliance audit. The psychological trick relies on the helpfulness or fear of the victim.

D. Baiting

Baiting exploits false hope or tempting incentives to entice users into traps. The most traditional method is the malicious USB drop, where infected media are left in public places such as lobbies, cafeterias, or parking lots. Curiosity leads someone to insert the device into their company computer, which installs malware [10].

Baiting can also be presented in the form of downloadable software containing free music, software cracks or movie torrents in online communities. These downloads are typically accompanied by ransomware or keyloggers that infect entire systems.

The secret to baiting success is to use curiosity and greed—two potent human motivators–against the target.

E. Tailgating (Piggybacking)

Tailgating is a physical form of social engineering where an unauthorized user gains access to a secured area by following an authorized individual closely behind. This is most dangerous in organizations that utilize ID badges or keycards for access but do not have stringent access policies [11]. They often impersonate delivery personnel, maintenance personnel, or new employees. They employ ordinary human behaviours, such as courtesy (e.g., ”holding the door open”), to overcome security. Although seemingly low-tech in nature, tailgating can lead to major security breaches if intruders gain access to network rooms, unattended hardware, or physical records.

F. Social Media Traps

Social networking websites are fertile ground for social engineering. Attackers create fake profiles, join a community, and send friend requests to harvest individual information or send phishing links [1].

The shared strategies included the following:

- Imitate giveaways or quizzes that ask users to answer personal questions.
- Spoofing accounts of known contacts to transmit malware.
- Monitoring job postings for valuable information, such as company names, work anniversary dates, or travel plans, is used to create more authentic spear-phishing messages.

The voluntarily provided information on social media is a treasure trove for exploiters who want to tailor their exploits to specific individuals. Albladi and Weir [1] found that users who engage in online quizzes daily are most prone to information leakage and are victimized the most by social engineering.

G. Quizzes, Contests, and Free Offers

Online surveys, imposter contests, and free product giveaways are equally effective social engineering tactics. They are particularly prevalent on social media and clickbait websites. They ask users to respond to a series of questions or supply their email addresses, phone numbers, or home addresses in return for rewards. Often, the information obtained is utilized for additional phishing or, even worse, sold on the dark web. These techniques depend heavily on the spontaneous nature of users and the spectacle of innocent entertainment.

These methods emphasize the dynamic changes in social engineering, from conventional physical penetration attacks to sophisticated, step-by-step psychological attacks conducted entirely over the web. The versatility of these attacks makes them all the more sinister, forcing users and organizations to remain vigilant at all times.

IV. CASE STUDIES

Social engineering has always been the most powerful technique used by hackers to circumvent technology-based defences. Attackers exploit procedural and psychological vulnerabilities by targeting individuals rather than systems. A brief description of some of the highly publicized intrusions—local and international—is presented below, showing how social engineering can be applied against even the most security-conscious organizations.

The most well-known case is likely the Google and Facebook invoice fraud (2013–2015), in which Lithuanian national Evaldas Rimasauskas presented himself as a legitimate hardware supplier and sent out fictitious invoices. Over $100 million was paid into accounts in his name before the fraud was discovered [12].

The 2011 RSA SecurID attack is a good example of a social engineering threat, where a phishing message containing an Excel attachment exploited a flaw in Flash. Hackers managed to steal sensitive data concerning RSA's two-factor authentication products, putting the security of millions of client computers at risk [13].

Scattered Spider, a cybercrime group, used vishing and impersonation in 2023 to trick MGM Resorts' IT support helpdesk into remotely resetting passwords. The attackers later used ransomware, leading to the interruption of operations in several casinos and hotels. Caesars Entertainment in yet another similar attack paid a ransom of $15 million to prevent such interruption [14].

In the latest attack, Co-op UK and Marks & Spencer were hit by a coordinated attack in 2024, where the attackers employed SIM swapping and phone impersonation to alter admin-level credentials, leading to service disruption and an estimated financial loss of more than £300 million [15].

In India, such social engineering activities have increased. In 2020, staff members of a prominent private sector bank in Mumbai were spoofed through fake internal HR emails with links to mimic the login pages. The entered credentials were compromised and utilized to send out unauthorized fund transfers, leading the Reserve Bank of India (RBI) to make phishing simulation training mandatory in the sector
[16].

Another attack occurred in 2022, when the All India Institute of Medical Sciences (AIIMS) in Delhi was targeted by a severe ransomware attack that suspended the hospital's services for over a week. Investigations revealed that the attack began with a phishing email to non-clinical administrative staff. The email was disguised as an internal IT email regarding new login procedures. If clicked, it installs malware and provides attackers with backdoor access to patient databases and critical servers [17].

In June 2024, CDK Global, a leading auto dealership software company, was attacked by the BlackSuit Ransomware Group. The attackers gained backend access via reused login credentials or social engineering via phishing, disrupting services at over 15,000 U.S. and Canadian dealerships. A ransom of over $25 million was reportedly paid. [18].

Similarly, Japan’s Kadokawa Corporation was attacked in July 2024 via phishing, resulting in a massive ransomware attack on its video-sharing platform, Niconico. The attack caused disruptions, revealed over 250,000 user records, and dealt a huge blow to investor confidence [19].

Most recently, in May 2025, a TxDOT incident led to the exfiltration of approximately 300,000 crash reports from the TxDOT database. Initial suggestions were internal impersonation via phone and email, which are typical vectors of social engineering attacks against the public sector [20]. Common patterns observed include:

- Helpdesk and support personnel are frequent targets due to their privileges.
- Phishing is the most common initial vector, followed by that of ransomware.
- Multifactor authentication is often circumvented by user manipulation.
- Sectors such as finance and healthcare are particularly vulnerable.

These case studies underscore the necessity of combining technical defences with human-centric strategies such as employee training, zero-trust models, and robust incident response protocols.

V. PSYCHOLOGICAL MANIPULATION TACTICS IN SOCIAL ENGINEERING

Social engineering is based on a close acquaintance with human psychology. Instead of exploiting weaknesses in software or hardware, attackers exploit cognitive biases, emotional circumstances, and habits. These deceptions are aimed at evading critical thinking and tricking individuals into doing something that they would not do otherwise, for example, revealing passwords, installing malware, or providing permission to access.

A. Exploiting Authority and Trust

Humans have a natural tendency to oblige instructions from a person in power and believe known sources. In most instances, social engineers impersonate IT administrators, upper management, or service personnel when attempting to provide essential commands. For example, a phishing message claiming to belong to the” IT Department” requesting employees to renew security credentials may sound authentic when presented in an official font and formal language.

Trust is also deceived whenever scammers pose as coworkers or known organizations. If a user is presented with a message from a known contact—especially one with whom they frequently interact—they are far more likely to click on the links or download the attachments without hesitation.

B. Creating Urgency, Fear, and Pressure

The best social engineering technique is to create a sense of urgency among the targets. Email messages regarding account suspension, unpaid balances, or unauthorized logins are likely to prompt users to act. At the time of greatest need, users are likely to bypass usual precautions and fall prey to attackers.

This tactic is normally coupled with fear, a mindset that overrules rationality. Threats of loss (reputational or financial), punishment, or undesirable outcomes tempt the receiver to react in a knee-jerk manner.

C. Triggering Curiosity and Greed

The majority of attacks exploit curiosity, such as in a doubt-provoking email with the subject line” Confidential Salary Information” or” Q1 Performance Report.” This doubt, combined with the promise of insider information, is likely to prompt users to click. Baiting attacks also exploit greed or reward-seeking by offering false rewards, such as vouchers, awards, or jobs, to get users to interact with malicious content. They work because they are rooted in automatic response behaviour rather than rational choice.

D. Take Advantage of Cognitive Biases and Habits

Individuals are greatly dependent on mental shortcuts or heuristics in decision-making, particularly when multitasking. Attackers also take advantage of the default effect (selecting the easiest or most common choice), confirmation bias (accepting information that verifies expectations), and repetition effect (accepting messages that seem to occur frequently or normally).

Additionally, most users exhibit default behaviours, such as reading emails at full speed, opening links without even looking at URLs, and using the same password for multiple accounts. Social engineers take advantage of this presumption by composing emails in a formal tone and taking advantage of weak authentication practices.

E. Emotional Appeals and Masquerading

In addition to impersonating experts, attackers typically attempt to appeal to sympathy or empathy as a means of deceiving users. These include impersonating a stranded relative, an ill co-worker, or a charity organization in need of instant help. They normally attempt to appeal to the user's sympathy as a means of evading critical thinking. As technology continues to advance, especially voice and video created through AI, today's attackers continually find ways to mimic the style, tone, and even voice of genuine people. This helps in" masquerading" genuine interactions with fake ones, making it even harder to identify.

VI. PREVENTION AND MITIGATION STRATEGIES

With the growing sophistication of social engineering techniques, the answer to this threat is not technical in isolation. Organisations must adopt an integrated, multilayered solution that addresses user awareness, procedural controls, and technical controls. There is no one solution that can eliminate the risk, but an integrated solution can reduce the success rate of social engineering attacks.

A. User Awareness and Training

Human behaviour is also key as a line of defence. Frequent practice-based training enables users to notice red flags in the form of unusual requests for credentials, suspicious attachments, or high-pressure requests to take action. Phishing simulations can be used most effectively to raise awareness and assess the effectiveness of training campaigns.

Training does not have to be limited to frontline staff. Executives, administrators, and support staff are high-privilege individuals and the primary targets of spear-phishing and vishing attacks. A cybersecurity awareness culture—wherein employees are guaranteed to report suspected threats without repercussions—is a must.

B. Multi-Factor Authentication (MFA)

While password hygiene is essential, attackers will typically circumvent credentials through deception. Multi-Factor Authentication has the essential additional security of requiring users to authenticate themselves using a second method like a phone application, token, or biometric signature.

Even when login credentials are compromised via phishing, MFA can guard against unauthorized access. However, organizations need to be careful against social engineering that tricks users into authenticating malicious login requests. User education must therefore include MFA fatigue and session hijacking attacks education.

C. Email Filtering and Domain Protection

Email remains the most common attack vector. Organizations can employ sophisticated email filters to identify and quarantine suspicious messages like spoofed email addresses, malicious attachments, and URLs to spoofed login phishing sites. With the use of techniques like SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), and DMARC (Domain-based Message Authentication, Reporting, and Conformance), it becomes impossible for an attacker to spoof trusted domains.

While nothing is ever foolproof, these tools definitely do increase the barrier for the attacker by adding authentication verification at the mail server level.

D. Clear Incident Reporting and Response Procedures

Staff become less susceptible to scams if they know where and how to report suspicious activity. Companies need to have a simple, well-advertised reporting method—by email, portal, or hotline—so that staff can act quickly when something feels off.

Most importantly, organizations must respond to such reports promptly. There should be an incident response team on hand to examine notices and, as required, take containment measures such as disabling accounts, revoking access tokens, or quarantining systems.

E. Access Control and Principle of Least Privilege

Not all employees require the same level of access. Least privilege and role-based access controls are employed so that even when an account is compromised, the attacker has limited scope. This avoids maximum damage, especially in ransomware or credential theft attacks. Regular access audits can also discover superfluous privileges, dormant accounts, or overlooked exposure points.

F. Periodic Security Assessments and Red Team

Exercises Organizations must actively challenge their defences through penetration testing, social engineering testing, and red teaming. These controlled attacks can provide useful insights into how employees and systems respond under pressure. They expose vulnerabilities that might go unnoticed through automated scans or checklists for compliance. The intention is not to assign blame but to improve policies on a continuous basis, improve user behaviour, and improve detection and response measures.

G. Behavioural Analytics and Anomaly Detection

Another emerging asset defence measure is the use of behavioural analytics and anomaly detection systems. These systems monitor user activity to establish a baseline for typical behaviour—such as typical login times, device usage, and access locations—and trigger alarms on anomalies that can indicate compromise. Examples include abrupt massive data transfers, out-of-hours access, or logins from unexpected geographies triggering automated alerts or access controls. Although these systems do not stop social engineering attacks directly, they are a valuable safety net by catching anomalous activity early, enabling faster incident response and reducing the potential damage.

VII. CONCLUSION

Social engineering is the most common and dynamic threat in the online world, merely because it targets the weakest point in any system—the human factor. Social engineering differs from the traditional software-based cyber attacks, as it employs psychological manipulation, trust, time pressure, and normal behaviour to deceive people into compromising security. Employing the strategies of phishing, pretexting, baiting, and other fraudulently engineered methods, the attackers manage to bypass even the most robust technological defences by exploiting cognitive biases and emotional responses.

This article provided a clear overview of the most common social engineering techniques, complemented by a study of major psychological manipulation techniques and a range of international and domestic case studies. These real-life examples demonstrated how seemingly basic techniques in action, if used astutely, can cause enormous financial and reputational loss to individuals, businesses, and governments alike. Instances like the 2020 Twitter Bitcoin heist or phishing in India are the best examples of the cross-cultural and leveraging nature of these threats.

Prevention and counter-measure for social engineering has to be multi-faceted. Technical counter-measures such as multi-factor authentication, secure mail gateways, and anomaly detection systems form the first line of defence. However, awareness and education are the key to resisting social engineering. Continual training, simulated attacks, open reporting practices, and instilling caution in dealing with unsolicited communication are all crucial in minimizing human error.

With changing technology, so will the methods used by cybercriminals. Deepfakes, voice AI, and targeted phishing attempts are already the new normal of deception. So, now it becomes the responsibility of individuals and organizations to stay a step ahead and on their toes. Future defences will no longer merely require smarter tools but smarter users. In short, social engineering prevention isn’t technical vs. human—it’s both. An informed public and the assistance of intelligent, vigilant systems is the greatest defence against these assaults on the mind. As cyber threats continue to transform and shape-shift, so must we adapt our awareness, education, and countermeasures against them.

REFERENCES

[1] S. M. Albladi and G. R. Weir, “User characteristics that influence judgment of social engineering attacks in social networks,” Humancentric Computing and Information Sciences, vol. 8, no. 5, pp. 1–24, 2018. doi: 10.1186/s13673-018-0128-7

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

[3] K. Almohammadi, H. Alqahtani, and A. Alzahrani, ”A comprehensive survey on social engineering techniques in the cyber domain,” Journal of Information Security and Applications, vol. 48, 2019, pp. 102–123. doi: 10.1016/j.jisa.2019.102370

[4] E. Okereafor, O. Adeyemi, and C. Udechukwu, “Simulated phishing attacks and human behavior: Evidence from Nigerian enterprises,” Cybersecurity, vol. 3, no. 1, pp. 1–14, 2020. doi: 10.1186/s42400020-00052-2

[5] M. Alghamdi and A. van Moorsel, ”Decision-making under social engineering attacks: A cognitive heuristic study,” in Proc. of the 15th Int. Conf. on Availability, Reliability and Security (ARES), 2021. doi: 10.1145/3407023.3407032

[6] S. Fatima and Y. Wang, “Leveraging artificial intelligence in social engineering attacks and defenses,” Journal of Cybersecurity and Privacy, vol. 3, no. 1, pp. 15–31, 2023. doi: 10.3390/jcp3010002

[7] J. Hong, ”The State of Phishing Attacks,” *Communications of the ACM*, vol. 55, no. 1, pp. 74–81, Jan. 2012. doi: 10.1145/2063176.2063197

[8] R. Hadnagy, *Social Engineering: The Science of Human Hacking*, 2nd ed., Wiley, 2018.

[9] M. Workman, “Wisecrackers: A Theory-Grounded Investigation of Phishing and Pretext Social Engineering Threats to Information Security,” *JASIST*, vol. 59, no. 4, pp. 662–674, 2008. doi: 10.1002/asi.20779

[10] T. N. Jagatic, N. A. Johnson, M. Jakobsson, and F. Menczer, ”Social Phishing,” *Communications of the ACM*, vol. 50, no. 10, pp. 94–100, 2007. doi: 10.1145/1290958.1290968

[11] K. D. Mitnick and W. L. Simon, *The Art of Deception: Controlling the Human Element of Security*, Wiley, 2002.

[12] ”FBI: Lithuanian scammer tricked Facebook and Google out of over $100 million,” Ars Technica, Mar. 2017. [Online]. Available: https://arstechnica.com/

[13] J. Leyden, “RSA finally comes clean over SecurID breach,” The Register, Jun. 2011.

[14] K. Weise and N. Perlroth, “Hackers Disrupt MGM Resorts, Caesars Entertainment,” The New York Times, Sep. 2023.

[15] “M&S and Co-op cyberattackers ’tricked IT into resetting passwords’,” The Times, May 2024.

[16] Reserve Bank of India, ”Cybersecurity in Banks – Phishing Incidents & Simulation Guidelines,” RBI Circular, Jul. 2021.

[17] “AIIMS Delhi servers under ransomware attack: Patient services paralyzed,” The Hindu, Nov. 2022.

[18] “CDK Global paid ransom to restore car dealership software,” Bloomberg, Jun. 2024.

[19] “Kadokawa confirms ransomware attack impacts Niconico,” NHK World Japan, Jul. 2024.

[20] “Hackers target TxDOT, download thousands of crash records,” San Antonio Express-News, May 2025.