Social Engineering Attacks in the Digital Age

Shimna sherin P T, 53, MES24MCA-2053

Introduction:

Social engineering attacks are one of the most common and dangerous threats in today's digital environment. Unlike traditional cyberattacks that focus on exploiting software or hardware vulnerabilities, social engineering attacks manipulate human psychology to gain unauthorized access to sensitive information. Attackers exploit trust, fear, curiosity, and urgency to deceive individuals into revealing confidential data such as passwords, OTPs, bank details, and personal information.

With the rapid growth of internet usage, social media platforms, online banking, and digital communication systems, social engineering attacks have become more sophisticated and widespread. These attacks can target individuals, organizations, and even governments. Understanding the nature of social engineering attacks is essential to protect digital assets and ensure cybersecurity awareness among users.

Background/Need /Relevance of the Topic:

In the digital age, humans are often considered the weakest link in cybersecurity. Despite advanced security mechanisms such as firewalls, encryption, and intrusion detection systems, attackers still succeed by exploiting human behavior. Social engineering attacks take advantage of lack of awareness, poor security practices, and over-trust in digital communication.

The relevance of this topic has increased due to the rise in phishing emails, fake calls, online frauds, and identity theft cases. Remote work culture and increased dependence on digital platforms have further increased the risk of such attacks. Studying social engineering attacks helps in understanding how these attacks occur and highlights the importance of user awareness and preventive measures in cybersecurity.

Literature Review:

Various researchers and cybersecurity experts have studied social engineering attacks and their impact. Kevin Mitnick, in his work *The Art of Deception*, explains how attackers manipulate human trust rather than technical systems. Studies published by organizations such as OWASP and Cisco highlight phishing as one of the most common cyber threats worldwide.

Research papers and security reports indicate that a majority of data breaches occur due to social engineering techniques. Literature also emphasizes the role of security awareness training and multi-factor authentication in reducing the success rate of such attacks. These studies provide valuable insights into attack methods, human vulnerabilities, and effective countermeasures.

Details of the topic:

Social engineering attacks manipulate human psychology to trick users into revealing sensitive information.

Common types include phishing (fake emails or messages), vishing (fraudulent phone calls), smishing (deceptive SMS messages), pretexting (fake identities or scenarios), and baiting (malicious free offers or downloads). These attacks can lead to financial loss, identity theft, and data breaches. Prevention includes user awareness, verifying unknown sources, strong authentication methods, and regular cybersecurity training.