Chapter 2
Exploring Social Engineering Attacks Involving Insights From Case Studies

Shirisha Kakarla
https://orcid.org/0000-0003-4970-4634
Sreenidhi Institute of Science and Technology, India

Geeta Kakarla
Sreenidhi Institute of Science and Technology, India

Shirina Samreen
Majmaah University, Saudi Arabia

Sukanya Vuppala
University College of Engineering, Osmania University, India

ABSTRACT

The social engineering attack is one of the most common forms of cyber-attacks. Attackers are using psychological tricks and more covert tactics to coerce victims into disclosing private information that belongs to them or that has been approved by authorities. Social skills are commonly employed to manipulate people by tricking, revealing, and acting upon them. This chapter discuss many types of social engineering assaults, the methodology for analyzing these attacks and data gathering methods utilized as case studies. This chapter also encompass the consequences, implications, legal and regulatory concerns, as well as strategies to mitigate them, such as awareness initiatives, security protocols, and technology remedies with

DOI: 10.4018/979-8-3693-6665-3.ch002

contingency measures that are regularly utilized. The chapter finishes by providing insights and recommendations for organizations to enhance their security measures against social engineering assaults. It highlights the importance of maintaining constant awareness and adjusting cyber security defenses as necessary.

1. OVERVIEW OF SOCIAL ENGINEERING

Cyber criminals employ social engineering as a strategy to coerce people into disclosing private information, acting in ways that jeopardize security, or choosing courses of action. Social engineering focuses on the human aspect of security, in contrast to conventional hacking techniques that depend on taking advantage of technological flaws in systems. It uses social skills, psychological manipulation, and deceit to fool people into giving it access to private data or systems.

Fundamentally, according to the works of Chetioui et al. (2021), social engineering preys on a number of psychological and behavioral traits in people, including fear, empathy, trust, authority, and curiosity. To manipulate their targets, attackers frequently create plausible scenarios or assume the identity of reliable sources. Phishing emails, phone scams, baiting with malware-infected devices, tailgating into secure locations, and authority figure impersonation are just a few examples of the various ways that social engineering attacks can be carried out.

Wang et al. (2021) has expressed that social engineering attacks can have a wide range of final goals, from obtaining unauthorized access to networks or physical locations to stealing financial information and sensitive data. Serious repercussions from these attacks may include monetary losses, data breaches, harm to one's reputation, and legal repercussions.

Organizations need to combine technical controls, security policies, and employee awareness programs to counteract social engineering threats. Organizations can lessen the possibility that people will fall for these deceptive strategies by offering security awareness training and educating people about the strategies employed in social engineering attacks.

1.1 Social Engineering Attack Life-cycle

The social engineering attack life cycle, as per Chetioui et al. (2021), delineates the sequential stages that attackers commonly adhere to in order to fool targets and accomplish their nefarious objectives. Gaining a comprehensive understanding of this life cycle might enable organizations and individuals to enhance their defense mechanisms against such threats. Below is a comprehensive analysis of the stages involved in a social engineering attack, as shown in Figure 1 and detailed: