Chapter 12
Social Engineering in Social Media and Online Interactions

Tarun Kumar Vashishth
https://orcid.org/0000-0001-9916-5575
IIMT University, India

Sachin Chaudhary
https://orcid.org/0000-0002-8415-0043
IIMT University, India

Vikas Sharma
https://orcid.org/0000-0001-8173-4548
IIMT University, India

Sachin Kaushik
https://orcid.org/0009-0004-1135-7168
HRIT University, Ghaziabad, India

Kewal Krishan Sharma
https://orcid.org/0009-0001-2504-9607
IIMT University, India

Vinod Kumar Bagar
Dewan Institute of Management Studies, India

ABSTRACT

Social engineering in social media and online interactions has emerged as a critical concern in the digital age, driven by the increasing interconnectivity and sharing of personal information online. This study is motivated by the growing prevalence of cyberattacks that exploit human psychology rather than technical vulnerabilities, targeting individuals through platforms where they share personal details. By examining various social engineering techniques such as phishing, pretexting, and baiting. This research highlights the methods attackers use to manipulate individuals and the specific vulnerabilities they exploit in social media environments. The study leverages data from recent cases and surveys to analyze the effectiveness of these techniques and the impact on both individuals and organizations. The findings underscore the significant risks posed by social engineering attacks, revealing the psychological underpinnings that make such tactics so effective.

DOI: 10.4018/979-8-3693-6665-3.ch012

1. INTRODUCTION

In the current virtual age, social engineering has emerged as a widespread threat to cybersecurity, exploiting the great and interconnected networks of social media and online interactions (Wang et al., 2021). Unlike conventional cyberattacks that rely upon technical exploits, social engineering leverages mental manipulation to misinform people into divulging personal statistics or acting moves that compromise security. Social media structures, wherein customers freely proportion non-public details, opinions, and everyday sports, have become fertile grounds for cybercriminals. These platforms offer attackers with a wealth of facts that may be used to craft incredibly customized and convincing attacks, which includes phishing, pretexting, and baiting. The insidious nature of social engineering lies in its capacity to make the most human psychology, specifically cognitive biases and emotional responses. Attackers often gift themselves as honest entities, creating scenarios that evoke a experience of urgency, fear, or interest, thereby compelling sufferers to act towards their higher judgment (Albladi and Weir, 2018). For example, an apparently innocent buddy request or a message from a supposed colleague can cause the revelation of sensitive information or the unwitting down load of malicious software. The effectiveness of those approaches is amplified by way of the inherent accept as true with and openness that represent social media interactions. This look at delves into the mechanisms and impacts of social engineering inside the realm of social media, examining each the strategies hired via attackers and the vulnerabilities they take advantage of. By dissecting numerous case research and real-international examples, the studies highlights the profound results of social engineering assaults, which range from non-public identity theft and monetary loss to corporate espionage and extensive facts breaches. Furthermore, the analysis also highlights the need for robust preventative measures, as well as consumer education, technology security, and organizational policies intended to increase resilience against such risks (Kumar et al., 2024).

Understanding the intricacies of social engineering is crucial for developing powerful protection strategies. As we navigate an increasingly digital international, it will become imperative to foster a tradition of protection attention, equipping individuals and groups with the knowledge and tools important to apprehend and mitigate the risks posed by means of social engineering. By doing so, we are able to better defend the integrity of our private and professional lives in opposition to those state-of-the-art and evolving assaults (Kumar et al., 2024).