Chapter 13
The Use of Deep Fakes in Social Engineering Attacks: A Case Study on Social Media Engagements

Avinash Saxena
https://orcid.org/0000-0003-1956-0510
Moradabad Institute of Technology, India

Himani Grewal
Moradabad Institute of Technology, India

ABSTRACT

Deepfakes, a recent and compelling technique that is used in social engineering attacks, allows cybercriminals to falsify audio, videos, and video to deceive individuals. These deepfakes can be used in phishing attacks, where fake hyperlinks lure victims into providing sensitive information. Deepfakes in social engineering attacks pose a significant cybersecurity threat. This spread of falsehood and misrepresentation on social media platforms has been shown to have a significant impact, with falsehood spreading farther, faster, deeper, and more broadly than the truth. The use of deepfakes in social engineering attacks raises ethical concerns, as these technologies can be used to manipulate individuals and spread disinformation on social media networks. The present chapter highlights the types of social engineering attacks, the meaning of deepfake technology, the positive side (benefits) of deepfake technologies, and the possible threats of deepfakes, with some real-time cases of the Indian political and entertainment industry followed by possible solutions.

DOI: 10.4018/979-8-3693-6665-3.ch013

SOCIAL ENGINEERING ATTACKS

Introduction and Types of Social Engineering Attacks

The greatest communication tool we have access to nowadays is the internet, which allows us to communicate in different ways through a jumbled media tools. The best ways for us to connect with others, whether personally or professionally is through social networks. Employers are expecting more and more from their staff members to have access to work devices, through either company-issued devices or personal smartphones (Krombholz et al., 2015). Social engineering attack term is used to persuade users to provide personal information (Gupta et al., 2016) by taking the advantages of different human traits, is a technique which helps the attackers to forged the sensitive information of the users (Fuertes et al., 2022). Social engineering attack is still very young and struggling to get a formal definition. This attack is still regarded as one of the most dangerous in the digital realm (Algarni et al., 2013). Social engineering attacks have been shown to provide the biggest security threats since they are more difficult to prevent (Bullée & Junger, 2020). Because user-provided personal information is the most important component to social networking site providers, there is an expectation that the danger of social engineering may rise in the future (Algarni et al., 2013). It can be regarded as an AI technique to convince a person to fulfill any request which can be made by the attacker for his personal goal (Mouton et al., 2016). Humans are still manipulable, even with the increased efficacy of security measures to safeguard sensitive data, making humans a weak link in the system. A social engineering attack takes advantage of this vulnerability by coercing sensitive information out of the target through a variety of manipulation strategies (Mouton et al., 2014). The social engineering attackers attacks the weakest relationship links of the victims. An attacker using social engineering is someone who seeks to get private data or funds. By making the victim feel uncomfortable, the assailant will alert the victim of their intended revenge while manipulating them. As per the definition given by National Institute of Standards and Technology "social engineering is an effort to deceive someone into disclosing information—like a password—in order to compromise networks or systems" (Scarfone et al., 2008). Attacks using social engineering have expanded to include emails, phone conversations, and in-person meetings. Automated social engineering, semantic attacks, social engineering in online communities or social media, and impersonation are examples of social engineering attack strategies. A multitude of social engineering techniques are emerging from the widespread use of information technology. Previous studies on human manipulation have revealed that offenders mentally coerced or deceived workers into divulging private information or making security blunders, for example, by employing social engineering and