

In the article titled "A survey of social cybersecurity: Techniques for attack detection, evaluations, challenges, and future prospects," the authors aim to provide an in-depth analysis of social cybersecurity attacks and the incorporation of potential predictive techniques against such attacks. Countless other research projects are utilized to reinforce and build upon their findings with machine learning, and AI plays a significant role in detection. The authors feel that currently, research within this field is inadequate, and they strive to create a more detailed analysis, laying groundwork for future research in social cybersecurity. This paper evaluates 18 types of cyberattacks, ranging from basic phishing attacks to online terrorist activity, gives a comprehensive analysis of the outcome of these attacks in the event that they are successful, and lists potential solutions to reduce the likelihood of such attacks. Additionally, the importance of datasets in this research was stressed due to their contribution in recognizing the tactics involved in social cyberattacks. This research greatly contributes to the understanding of social cyberattacks and successfully builds upon research in this field, laying the foundation for future projects involving the dynamics of social cybersecurity.