Abstract

The popular communication Social Networking Sites (SNS) like Facebook, Twitter, LinkedIn etc have become in style and well-liked during the past few years and are utilized by billions of individuals irrespective of their age groups for communicating either with old friends, relatives from far places or total strangers. As they allow users to both articulate their eccentricity and meet people with similar interests. Risks posed by SNS are becoming harder to conquer due to publication of social network data by user which may contain personal or confidential information. There is a high possibility of this information to be misused by people with harmful motives like stalking, identity theft, online victimization etc. Therefore there arises an urgent need to safeguard users from attacks occurring in SNS, as users are still unaware of these threats. Moreover, a user does not have control about what others reveal about them. The attackers of SNS mainly use social engineering attack to victimize the user through malicious URL links, applications, Spam messages etc. URL has an important role in detecting phishing websites. So, this focuses on the detection and prevention of malicious URLs as they are used to mount various attacks like spamming, phishing, malware etc.
References


Index Terms

Computer Science

Security

Keywords

Suspicious URLs, cyber criminals, cyber threats, SNS users, approaches etc.