IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, July 2022
Impact Factor 6.252

Social Media Privacy and Security (Benefits & Risks)

Aakash Panchal
Hiray School of Information Technology and Engineering, Mumbai University, Mumbai, India

Abstract: *Over the past several years, social networking sites have arisen to facilitate social interactions on the Internet while revolutionizing how online users interact with others. Most social networking sites offer the basic features of online interaction, communication, and interest sharing, letting individuals create online profiles that other users can view. Unfortunately, current trends in social networks indirectly require users to become system and policy administrators to protect their online contents. Social networks' security and privacy requirements still aren't well understood or fully defined. Nevertheless, it's clear that they'll be quite different from classic security and privacy requirements because social networks involve user-centric concerns and allow multiple users to specify security policies on shared data. So, we must bring a depth of security experience from multiple security domains and technologies to this field, as well as a breadth of knowledge about social networks.*

Keywords: Social media; Privacy; Policy; Security

I. INTRODUCTION

The Internet's wide adoption has contributed to online social networking sites' thriving popularity, which is evident in the attention such sites receive from both the media and academia. Over the past several years, several social networking sites have arisen to facilitate social interactions on the Internet while revolutionizing how online users interact with their friends, coworkers, colleagues, family, and even strangers. Moreover, some social networks let users further partition their sets of friends based on social community, organization, geographical location, or how well they know each other. Most social networking sites offer the basic features of online interaction, communication, and interest sharing, letting individuals create online profiles that other users can view. One of the most important issues we must immediately address in this context is the security and privacy of sensitive information, which is generally any data an adversary, could use to cause significant harm to users. Such data might include financial information, which an attacker could use to perpetrate identity theft, or medical information, such as health conditions, diagnoses, or treatment histories. Unfortunately, current trends in social networks indirectly require users to become system and policy administrators to protect their online contents. Further complicating this issue is social networks' rapid growth as well as their continual adoption of new services.

1.1 Types of Social Networking Sites

Facebook, Twitter, Snap chat, YouTube etc.

II. POSSIBLE THREATS AND PRIVACY RISK IN SOCIAL NETWORK SITES

The use of personal information in social networks raises new privacy concerns and requires insights into security problems. Online social networks have recently emerged as a challenging research area with a vast reach and application space. Several studies and recent news reports have highlighted the increased risk to personal data processed by online social networking applications, as well as the user population's lack of awareness. In general, the privacy issue in social networking is coupled with the identifiability and linkability of the information available in this social setting, its possible recipients, and its potential uses. Protecting information's identifiability and linkability is quite challenging given that even those sites that don't disclose users' personal information might provide enough data to identify and link a profile's owner. Possible recipients for such personally identifiable information include hosting servers for the social networking sites, the network itself, and third parties that might abuse or misuse such critical and sensitive information.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, July 2022
Impact Factor 6.252

Social networks' security and privacy requirements still aren't well understood or fully defined. Nevertheless, it's clear that they'll be quite different from classic security and privacy requirements because social networks involve user-centric concerns and allow multiple users to specify security policies on shared data. So, we must bring a depth of security experience from multiple security domains and technologies to this field, as well as a breadth of knowledge about social networks.

When users first sign up to Facebook, they will be constantly asked and reminded by Facebook to update their profile with more personal information such as date of birth, hometown, workplace, and/or school in order to find more friends and Enjoy the experience more. The growing popularity of Social Network Sites and the fact that they contain enormous amounts of information make these websites an attractive target for malicious hackers.

The terms 'privacy' and 'security' sometimes overlap and may be used interchangeably by users and researchers. Therefore, in order to provide a clearer conceptualization, the key terms, privacy and security, will be defined as follows with respect to Social Network Sites:

Security: In Social Network Sites, security threats result from the technical vulnerabilities of the network. In 2009, the Secure Enterprise 2.0 Forum identified and listed eight main security threats that may occur when using social networks insufficient authentication controls; cross-site scripting; cross-site request forgery; phishing; information leakage; injection flaws; information integrity; and insufficient anti-automation.

III. SOCIAL NETWORKS DATA MINING

There are two methods for collecting data from SNSs, either via a crawling API, or by screen-scraping crawled over 11.3 million online profiles in order to examine the structures of multiple SNSs for academic purposes. Most Social Network Sites do not now publish their APIs for security reasons, but screen- scraping is possible using appropriate sources. Web-scraping is prohibited by the European Court of Justice as it is considered to be an intellectual property infringement. In the US, website operators can sue screen-scrapers under copyright laws and trespass to chattels claims. Screen-scraping, however, still occurs using illegal technical methods and can result in two privacy and security violations:

If malicious hackers are able to screen-scrape SNSs, they can obtain a huge number of names and contact details; hence, they can perform large-scale attacks such as spamming or phishing attacks.

Research companies harvest users' data without their consent or the website operator's consent. With the appropriate tools, they can collect millions of users' online information and sell it to other companies, such as marketing companies, which can design targeted ads for their products. It can be argued that this information is already public and the users put this information in the public domain; hence, it is free for anyone to use. However, screen- scraping companies do not ask for users' consent to use their information, which results in ethical issues and privacy violation. In 2010, Nielsen Co., a media-research company, used highly sophisticated web-scraping software to collect messages that were exchanged between users of a website called PatientsLikeMe. In this network, users post and exchange with others highly personal stories about their physical and mental health, such as their desire to hurt themselves. Nielsen Co. registered on the website as a member and screen-scraped numerous messages that contained people's emotional problems. The company then sold this information (Angwin & Stecklow, 2010). The users of the site believed that it was a safe environment in which to share their suffering but their privacy was violated and their information was collected without their consent.

IV. ANALYSIS OF FACEBOOK, SNAPCHAT, INSTAGRAM AND TWITTER PRIVACY POLICIES AND PRIVACY VIOLATIONS

This section will review and discuss Facebook, Snapchat, Twitter and Instagram privacy policies. All information regarding privacy policies was retrieved from each Social sites latest published privacy policies on their website/application in May-June 2016. This section will also discuss each network's general privacy settings and related privacy and security concerns.

Firstly, a privacy policy is prepared by individuals or organizations to provide users with information about how their data will be collected; stored, used and shared It may contain any relevant laws that are applicable to the industry. The terms and conditions, however, state what the user must agree to if they want to sign up or use the website. The privacy policy is included as one of the items that the user is agreeing to when they agree to the terms and conditions.

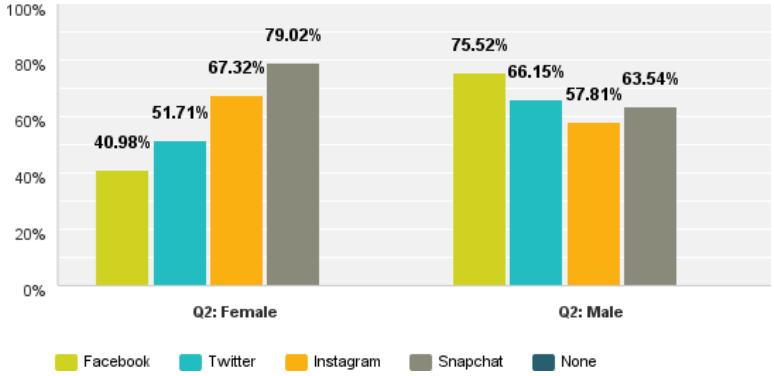
IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, July 2022
Impact Factor 6.252

V. TYPES OF SOCIAL NETWORK SITES USERS SURVEYED

The first question in the survey is: Which of the following Social Networking sites do you currently have an active account with and use? The purpose of having this question at the start was to disqualify any non-Social Network Sites users and to identify what SOCIAL NETWORK SITESs the survey participant was currently using. The results disqualified 14 respondents who chose the 'none' option and were excluded from the survey. The results revealed that Snapchat was the dominant SOCIAL NETWORK SITES among the four networks, with a response rate of 69.6%. Snapchat is the newest social network compared to the other three networks. Facebook, which is one of the oldest SOCIAL NETWORK SITES, had the lowest percentage of users in this survey at 55.9%. Table 4.1 presents the findings and the rankings of the SOCIAL NETWORK SITESs by the survey participants.

Answer Choices Responses	
Facebook	66.90% N=*237*
Twitter	58.87% N=*239*
Instagram	61.97% N=*257*
Snapchat	70.64% N=*290*
None	4.38% N=*15*
Total Respondents: 815	

The results for this question also showed that there was a difference between male and females in the choice of Social Network Sites.



Male vs. Female Choice of Social Network Sites

VI. USAGE OF SNSS AND MAIN PRIVACY CONCERNS

This section presents the findings for the third page of the survey, which investigated users' motives for using Social Network Sites, frequency of use, and main privacy-related questions. The questions in this section aimed to identify users' Social Network Sites usage habits and their main privacy perceptions and were used as a comparison with later questions in order to see how users' privacy perceptions compared with their actual usage. In addition, these findings provided a better understanding of the sample, which allowed more effective qualitative analysis.

The first question addressed the main reason for using Social Network Sites. Keeping in touch with family and friends (61%) and checking news and staying updated (35.6%) were the most prevalent reasons for using Social Network Sites, as displayed in

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, July 2022
Impact Factor 6.252

VII. LAST AND MAIN RESEARCH QUESTION

How aware are users of the extent to which their information is protected by SNS providers according to the privacy policies that the users have agreed to?

An important part of this research focused on analysing Social Network Sites privacy policies in the outcome of that analysis indicated that Social Network Sites could legally perform certain actions without prior approval from users, such as tracking user web browsing histories. Facebook, Snapchat, Instagram, and Twitter all state in their privacy policies that they

Monitor the web pages accessed by the user. Therefore, this research investigated users' awareness and knowledge of how their personal information is collected, stored, processed, and shared with other parties. The survey participants were presented with statements that were derived directly from each Social Network Site's privacy policies and were asked whether they believed that those Social Network Sites had the legal right to perform those actions on the user's data, based on the terms and condition that the users had agreed to prior to using the service. The results, which are listed in detail in indicated that a statistically significant majority of users were not aware, as they stated that they did not believe the statements listed were accurate. The results indicate that the majority of survey takers were not aware of how their information was handled. The survey results also show that 94.1% of the respondents did not read the privacy policies/terms of condition before signing up.

VIII. CONCLUSION

Firstly, the three main research questions and related sub-questions were answered. The results showed a significant amount of personal identifying information was revealed by the users. The chapter provided more detail by identifying the factors that may have influenced such behavior. It was apparent that age, gender, and education have a significant influence on users' behavior. In addition, the chapter also discussed users' perceptions of privacy and whether these had any effect on their actions online. The chapter also discussed the results in terms of privacy policies and users' levels of awareness. After discussing the results, the chapter linked the results to the literature reviewed in and briefly reflected on the consequences of sharing such information on users' safety. Lastly, the chapter suggested some practices that may provide users with more private Social Network Sites browsing experiences.