IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

ANALYSIS OF SECURITY AND PRIVACY ISSUES IN SOCIAL NETWORKS

Amitvikram Nawalagatti

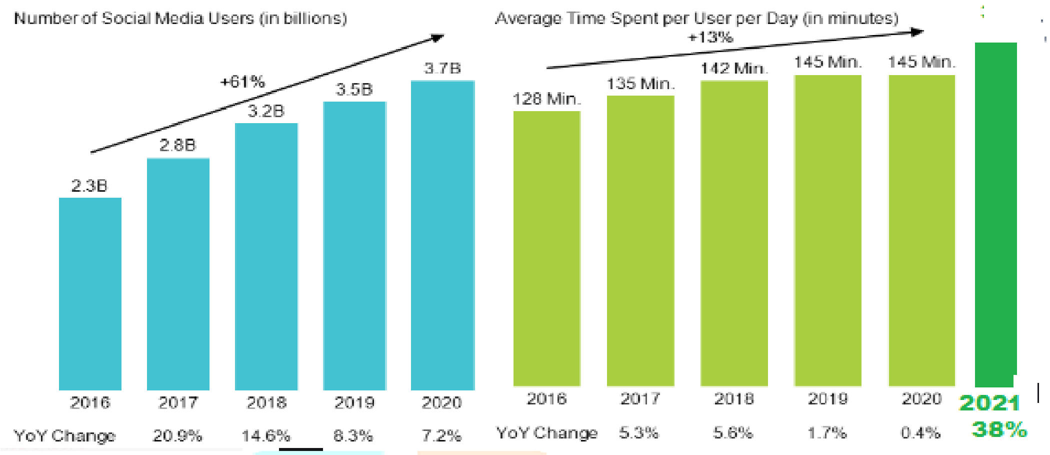
Faculty of Msc. Computer scienceKarnataka State Rural Development and Panchayat Raj University, Gadag

ABSTRACT : Social networks are now a part of human life. Interact online, communicate and share interests, allowing people to create online profiles that can be viewed by other users. These are the basic features offered by most of the social networking sites. Unfortunately, in many cases, users are not even aware of the disclosure of their personal information through profiles. their Leakage of users' personal information can happen in a variety of ways. Many of the security risks associated with the use of social networks are discussed in this document. In addition, the issue of privacy and its connection with security is described. Based on these discussions, some key points are provided to improve a user's privacy and security on social networks. Our inquest will help the readers to understand the security and privacy issues for the social network users, and this research will help the user.

Keywords: security; classic privacy threats; modern threat, network, OSN

INTRODUCTION

The evolution of social media has created a new paradigm of communication and interaction. It has become a part of our social life that helps us connect to friends, family, colleagues, or others. We have witnessed how the advent of social media platforms like Facebook, Twitter, and What's App brought a revolutionary change in how we use the internet for personal and professional purposes. Social media are a medium of interaction between the data sender (data generator) and receivers (end users) for online interaction create virtual communities using online social networks. Information security should be at the forefront of everyone's mind because much of our personal information is out there on the Internet. the staggering popularity of these social networks, which are often used by teenagers and people who do not have privacy or security on their minds, leads to a huge amount of potentially private information being placed on the Internet where others can have access to it. [1] It is essential to be careful what we upload in this way; Carelessness can lead to disclosure of information that others should not have.In 2021, there are 4.48 billion people actively using social media in the world, and this is an increase of **13.13% year-on-year** from 3.69 billion in 2020. Back in 2015, there were only 2.07 billion users – that's an overall increase in users of 115.59% in just six years.



Source google.com

An extraordinary greater part of long range interpersonal communication manages protection. Besides the revolution that Online Social Network have generated in social networking, they have introduced new threats to their users due to their attractiveness, the ever increasing number of users, and the massive amount of personal information they share. Being a part of users' daily lives, online social networks introduce new security concerns especially because of the potential exposure of huge amounts of personal information. Security and privacy attacks to online social networks and the countermeasures that can be used to protect the privacy of Online Social network users and keep shared data secure against different types of attacks. Online social media can introduce new threats for their users because of the potential for accessing a vast amount of personal information disclosed by Online Social networking users themselves. Different types of assets are prone to attacks in Online Social Networking, including private information of the individuals or organizations, digital identity, financial assets, intellectual property (IP), and corporate secrets and resources.

LITERATURE RIVEW

Recently, internet is one in all the foremost efficient and effective ways to communicate and sharing the data especially in terms of social networking sites. With over billions of users connected through online social network and because of popularity of social network sites, more people are concerning about the privacy and it's become a very important issue. It's been noted that security concerns are very low on social networking sites, and users' attempts to form reasonable improvements to their social media security are considerably low than other types of security operations. Compared, many social media users lack technical knowledge and have an occasional degree of security concerns. Ensuring the social networks can perform desired behavior is one thing, but when sharing a wealth of (personal) data, one should also consider what undesired behavior might occur. In this section, we will examine privacy, its role in social networks, and potential threats to user privacy. Therefore, at step of He's finding, many companies do not have good social network security policies and programs and do not know how to implement effective social network security policies to reduce the risk of cyber security. social network security. With the development of social networking sites, online personal information safety protection has been and is a heavy and important research topic. The privacy and security of social networking sites were researched and reviewed in this article. In this article, we'll look at how the current privacy plays out on social networking sites, analyze how personal information is affected by the Internet and social networks, and the also So, we'll discuss how privacy becomes a risk and how to use security awareness. to avoid increasing privacy, affecting self-disclosure of users' private data. Using privacy calculus, the perceived benefit was combined into this paper and a few features need modifications, like .Data should be handled without breaching the users' privacy and data protection should be enormously scrutinized. The foremost grounded measure that must be taken is to form undaunted quality of one's privacy whoever has affiliated with the social media.

RISK of SECURITY

Social media accounts are not monitored. Social media accounts that are not monitored or are no longer in use are targets of hackers. ...

1. Impersonated accounts

2. Privacy settings

3. Vulnerable third party apps

4. Human error

5. Phishing attacks and scams

6. Malware attacks and hacks

7. Cell phones are not secure

METHODS TO BE USED

1. Predicting Social Media User Behavior In the age of social commerce, users often connect from e-commerce sites to social networking sites like Facebook and Twitter. However, little effort has been made to understand the correlation between users' social media profiles and their e-commerce behavior. This article describes a system that predicts the purchasing behavior of users on e-commerce sites from the users' social network profiles. We specifically focused on understanding whether user profile information in a social network (e.g. Facebook) could be leveraged to predict the product categories users would purchase (e.g., Facebook). e.g. eBay Electronics). Article provides in-depth analysis of the correlation between users' Facebook profile information and eBay purchases, and analyzes the

performance of of different feature sets and learning algorithms. on the task of predicting shopping behavior.

2. **Privacy challenges and Concerns** : Electronic media can have positive and negative effects on adolescents. Overall, electronic media use is positive when used for education, access to positive health information, and developing and sustaining social connections. Despite these benefits, electronic media can be harmful and may have negative health consequences. For the research of password based authentication in decentralized systems, the authentication mechanisms of P2P backup and storage systems were analyzed. This is followed by design analysis of new password authentication protocols as well as new encryption-based access control mechanisms that address privacy issues without sacrificing performance.

3 **PRIVACY SETTINGS:** IT is very important that a person should maintain strict privacy
Settings in all of the social media accounts so that only close friends and relative can read your post /status.

SOLUTION FROM SOCIAL MEDIA THREARTS

1)Creating strong passwords is the main option for keeping your information secure.

2) Secure complex passwords, including upper and lower case letters, numbers, and special characters. It should be memorized and never written down.

3) We should be sensitive in what we upload/share on our social media accounts and avoid sharing personal information like date of birth, social security details, phone number, Names and photos of family members.

4) Connect our devices only with authorized Wi-Fi access, use security options provided by different mobile operating systems, use auto-lock features of and only download apps from authorized app stores.

5) Keep the operating system updated with the latest patches, turn on the firewall, and avoid installing cracked software.

6) Ensure our antivirus is updated and scans are performed frequently.

7) We need to be smart using the internet and avoid visiting un trusted websites; referral links to visit websites are never to be clicked; instead, type in the browser's URL address.

8) Care needs to be taken to accept friend requests only from people we know and block those who post upsetting content .

CONCLUSION

In this paper we specify the details about privacy and security in social media. It is genuinely obvious from the greater part of this examination that interpersonal organizations are huge security and protection dangers. Organizations should take appropriate measures to be cybercrime safe, and users, too, shall protect their personal information to avoid any misuse. Cyberspace is becoming a significant area for crimes, so there is a need for comprehensive collaboration among nations to work together and combat these social network security and social media cyber-attacks, which is a continuously gowning menace. It’s fairly clear from all of this research that social networks are big security and privacy risks.

REFERENCES

1.Basilisa Mvungi, Mizuho Iwaihara. Associations between privacy, risk awareness, and interactive motivations of social networking service users, and motivation prediction from observable features. Computers in Human Behavior, Dec 2014; 4(c):20-34.

2. Joshana Shibchurn, Xiangbin Yan.Information disclosure on social networking sites: An intrinsic˛extrinsic motivation perspective. Computers in Human Behavior. 2015; 44:103-117.

3. Yan Li, Yingjiu Li, Qiang Yan, Robert H. Deng, Privacy leakage analysis in online social Networks, Computers and Security, Mar 2015; 49(c):239-254.

4. Patrick Van Eecke, Maarten Truyens, Privacy and social networks, Computer Law & Security Review;2010; 26(5):535-546.

5. Benson Vladlena, George Saridakis, Hemamali Tennakoon, Jean Noel Ezingeard, The role of security notices and online consumer behaviour: An empirical study of social networking users, International Journal of Human Computer Studies;Aug 2015; 80:36-44.

6. Yuan Li.Theories in online information privacy research: A critical review and an integrated framework, Decision Support System. June 2012; 54(1):471-481.

7. Nader Yahya Alkeinay, Norita Md. Norwawi. User Oriented Privacy Model for Social Networks. International Conference on Innovation, Management and Technology Research, Malaysia; 22 – 23 September, 2013; 191-197.

8. Gail-Joon Ahn, Mohamed Shehab, Anna Squicciarini. Security and Privacy in Social Networks. IEEE Internet Computing; 2011; 15(3): 10-12.

9. Paul Lowry, Jinwei Cao, Andrea Everard. Privacy Concerns versus Desire for Interpersonal Awareness in Driving the Use of Self-Disclosure Technologies: The Case of Instant Messaging in Two Cultures. Journal of Management Information Systems; 2011; 27(4):163-200.

10. Carl Timm, Richard Perez. Seven Deadliest Social Network Attacks. Syngress Publishing; 2021