iJRASET
International Journal For Research in
Applied Science and Engineering Technology

Volume: 9 Issue: XII Month of publication: December 2021

DOI: https://doi.org/10.22214/ijraset.2021.39203

Various Privacy and Security Issues in Online Social Networks

Miss. Komal K. Khandare[1], Dr. G. R. Bamnote[2], Prof. Ms. S. G. Pundkar[3]
[1]PG Scholar, [2]Professor, [3]Professor, Computer Science & Engineering, Prof.Ram Meghe Institute of Technology & Research, Maharashtra, INDIA

Abstract: Social networks have become a part of human life. online interaction, communication, and interest sharing, letting individuals create online profiles that other users can view these are basic features that are offer by most of social networking sites Unfortunately, In many cases, users are not even aware of the disclosure of their personal information through their profiles. Leakage of a user's private information can happen in different ways. Many of the security risks associated with using social media are presented in this paper. Also, the issue of privacy and how it relates to security are 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: OSN; security; classic privacy threats; modern threat.

I. 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 WhatsApp brought a revolutionary change in how we use the internet for personal and professional purposes.[4] 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 put online in this way; being careless can lead to information being posted that should not be available to others.

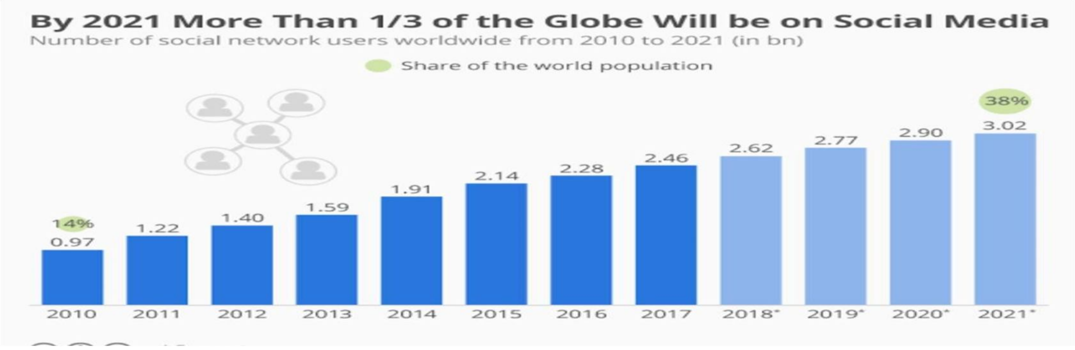


Fig. 1:- Social network growth from 2010-2021

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. [5]

II. COMMON SOCIAL MEDIA SECURITY RISKS

A. Unattended Social Media Accounts

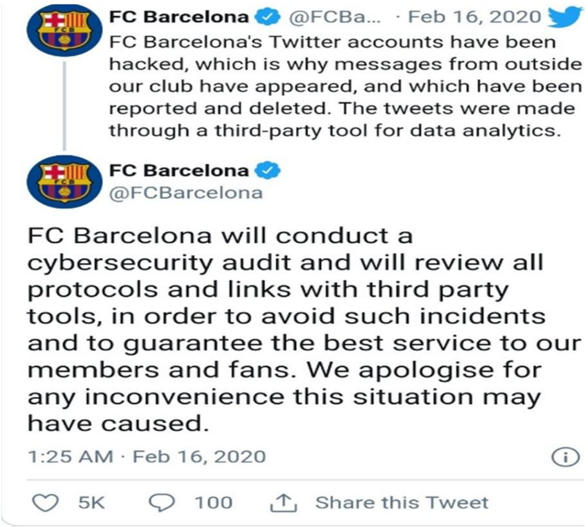
It's a good idea to reserve your brand's handle on all social media channels, even if you don't plan to use them all right away. This making it easy for people to find you, but it's important not to ignore the accounts you don't use yet, the ones you stopped using, or don't use often. Unmonitored social accounts can be the target of hackers, who could start posting fraudulent messages under your name. [2]

B. Human Error

Everyone makes mistakes. In today's busy world, it is all too easy for an employee to accidentally expose the company to threats online. In fact, "employee weakness" was responsible for 20% of cyberattacks, according to the EY Global Information Security Survey. Some online challenges and quizzes can also be problematic. By completing them, employees can accidentally create social media security issues. [2]

C. Vulnerable Third-Party Apps

Locking down your own social accounts is great. But hackers may still be able to gain access to secure social media through vulnerabilities in connected third-party apps. Hackers accessed Twitter accounts associated with the International Olympics Committee. They got in through a third-party analytics app. FC Barcelona was a victim of the same hack. [3]



FC Barcelona @FCBa... · Feb 16, 2020

FC Barcelona's Twitter accounts have been hacked, which is why messages from outside our club have appeared, and which have been reported and deleted. The tweets were made through a third-party tool for data analytics.

FC Barcelona
@FCBarcelona

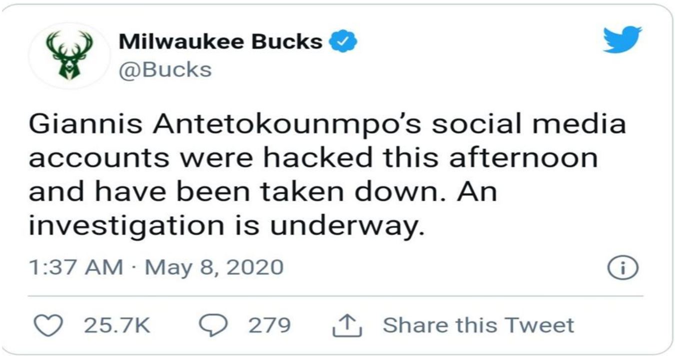
FC Barcelona will conduct a cybersecurity audit and will review all protocols and links with third party tools, in order to avoid such incidents and to guarantee the best service to our members and fans. We apologise for any inconvenience this situation may have caused.

1:25 AM · Feb 16, 2020

Fig. 2. Twitter tweet hack example

D. Malware Attacks and Hacks

If hackers gain access to your social media accounts, they can cause enormous band reputation damage. Hackers recently gained access to the accounts of NBA MVP Giannis Antetokounmpo. When they tweeted racial slurs and other profanities, his team had to do damage control.



Milwaukee Bucks
@Bucks

Giannis Antetokounmpo's social media accounts were hacked this afternoon and have been taken down. An investigation is underway.

1:37 AM · May 8, 2020

Fig. 3. Twitter Accounts Malware Attack

III. LITERATURE REVIEW

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 behaviour is one thing, but when sharing a wealth of (personal) data, one should also consider what undesired behaviour might occur. During this section, we'll check up on privacy, its role in social networks, and potential threats to users' privacy. Thus in step with to He's findings, many companies lack a good social media security policy and program and are unaware of the way to implement effective social media security policies to mitigate social media security risks. With the development of social network sites, security protection of personal information online has been a heavy and important research topic. Privacy and security of social network sites has been investigated and reviewed during this paper. This paper we are going to review how the current privacy plays on social network sites, analysed how personal information is being influenced by internet and social network, and also we will discuss how the privacy become a risk and the way to use security awareness to avoid privacy rise, affecting users' self-disclosure of 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.

The constructs of data sensitivity and perceived benefit were redefined after reviewing the literature. Through a study on the constructs of privacy concern and self-disclosure, this research paper aims at reducing the degree of privacy concern

IV. METHODOLOGY

A. *Predicting the Behaviour of Social Media Users*

Within the era of social commerce, users often connect from e-commerce websites to social networking venues like Facebook and Twitter. However, there are few efforts on understanding the correlations between users' social media profiles and their e-commerce behaviour's. This paper portrays a system for forecasting a user's purchase behaviour's on e-commerce websites from the user's social media profile. We specifically concentrate at understanding if the user's profile information in a social network (for example Facebook) will be leveraged to predict what categories of products the user will buy from (for example eBay Electronics). The paper provides in an depth analysis on how users' Facebook profile information correlates to purchases on eBay, and analyses the performance of various feature sets and learning algorithms on the task of purchase behaviour prediction.

B. *Privacy Glitches 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 authentica-tion mechanisms of P2P backup and storage systems were analyzed. The analysis was followed by the design of the new protocols for the password-based authen-tication and also the new encryption-based access control mechanism aimed toward solving the privacy problem without sacrificing performance. Lightweight custom simulators were developed to judge the efficiency of design from Facebook. Security properties of the proposed architectures were thoroughly analysed, but no formal security proofs were made.

C. *Various Possible Threats in Social Networking Sites*

The security issues and privacy concerns are the key requirements of the social networking sites. But there were many deadliest attacks persists in all these social networking sites and safeguarding the potential users from these heinous attack have been the challenging task of the many social analyst and developers. The fundamental security attacks are classified into three categories.

1) *Privacy Breach:* Find link between nodes and edges and possibly identify the relation between them.
2) *Passive Attacks:* This can be totally anonymous and undetectable.
3) *Active Attacks:* Form the new nodes intrinsically and trying to attach to the opposite nodes and gain the access to the other nodes.

D. *Privacy Setup on Social Networking Sites*

Social network sites destinations work to bloster privacy settings. Facebook and other long range social communication destinations limit protection as a significant aspect of their default settings. It's essential for clients to travel into their client settings to modify their protection as per liberties. These locales like Facebook give clients the choice to not display individual data, as an example, conception date, email, telephone number, and business status. For the individuals who arrange to incorporate this material, Facebook permit clients to limit access to their profile to just permit the individuals who they acknowledge as "companions" to work out their profile. Be that because it may, even this level of privacy can't keep one among those companions from sparing a photograph to their own PC and posting it elsewhere. Be that because it may, at this time less social media site clients have constrained their profiles.

For example, allows us take how the users to limit the profile visibility to others in a numerous social media sites:
Facebook: Facebook's privacy setting for new users is ready to Friends Only. To set this, visit Settings > Privacy >

Who can see your future posts?

- Twitter: Settings > Security and privacy > Privacy > Tweet Privacy > Protect my Tweets.
- LinkedIn: To vary this: Settings > Account > Helpful Links > Edit your public profile.
- Google+: To vary this setting, type the name of a Circle within the "To" field below your post before you publish it.

V. SOLUTIONS ON SOCIAL MEDIA THREATS

1) Creating strong passwords is the primary option to ensure the privacy of your information.
2) Ensure passwords are complex, including upper & lower case, numbers, and special characters. It should be memorized and never be written on paper.
3) We need to be sensitive in what we upload/share in our social networking accounts and avoid sharing personal information like date of birth, social security details, phone numbers, names, and pictures of family members.
4) Connect our devices only to authorized Wi-Fi access, use privacy options provided by various mobile operating systems, use auto-lock features, and download apps only 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 untrusted 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 or comments.

A. *Advantages*

1) Individual users can detain touch with friends and relatives easily. You'll sit up to this point with what people do, and also allow them to know what's happening in your life, using words, photos, and other media.
2) Users can connect with like-minded people. Social networking makes it easy to hitch groups and make friends online with others who share your particular interests, whether or not it is relatively obscure.
3) Connections with others can be made long distance and across international boundaries.
4) Social networking can increase voting rates and facilitate political change. Political campaigns like elections, boycotts, rallies, and marches can all be set up and run via social media.
5) Large amounts of people will be contacted quickly in the event of an emergency event, such as a hurricane, wildfire, or act of terrorism.

B. *Disadvantages*

1) Users can't be sure that their personal data are going to be safe. It should be stolen, or may sell by the site itself in some instances.
2) Scams, computer viruses, fraud, and identity theft all occur on social networking sites.
3) Children use social networking sites to cheat and replica their assignments.
4) People can waste a plenty of your time on social networking sites with none obvious benefits. Their work career, education, social life, and even physical health will suffer as a result.
5) Businesses using networking run the danger of making a faux pas or worse, and undermining the brand.

VI. CONCLUSIONS

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 cyber-crime 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.

VII. ACKNOWLEDGEMENT

First and foremost, I would like to express my sincere gratitude to my guide Dr. G. R. Bamnote and Prof. Ms. S. G. Pundkar who has in the literal sense, guided and supervised me. I am indebted with a deep sense of gratitude for the constant inspiration and valuable guidance throughout the work.

REFERENCES

[1] Jagatic, T.N., Johnson, N.A., Jakobsson, M., Menczer, F.: Social phishing. Comm. ACM 50(10), 94–100 (2007

[2] Mahmood, S.: Online social networks: The overt and covert communication channels for terrorists and beyond. In: IEEE HST, 2012.

[3] Mahmood, S.: New privacy threats for Facebook and Twitter users. In: IEEE 3PGCIC, 2012.

[4] Dey, R., Tang, C., Ross, K.W., Saxena, N.: Estimating age privacy leakage in online social networks. In: INFOCOM, pp. 2836–2840, 2012 70 S. Mahmood.

[5] A. Mislove, M. Marcon, K. P. Gummadi, P. Druschel, and B. Bhattacharjee, "Measurement and analysis of online social networks," in Proceedings of the 5th ACM/USENIX Internet Measurement Conference (IMC'07), October 2007.

[6] Warren, S.D., Brandeis, L.D.: The right to privacy. Harv. Law Rev. 4(5), 193–220 (1890)

[7] Chaabane, A., Acs, G., Kaafar, M.: You are what you like! Information leakage through users' interests. In: Proc. Annual Network and Distributed System Security Symposium, 2012

[8] Chaum, D.: Untraceable electronic mail, return addresses, and digital pseudonyms. Comm. ACM 24(2), 84–88 (1981)

[9] Chaum, D.: Blind signatures for untraceable payments. In: CRYPTO, pp. 199–203, 1982

[10] Cooper, B.: Italian drugs fugitive jailed after posting pictures of himself with Barack Obama waxwork in London on Facebook. Mail Online February 14, 2012

[11] Westin, A., Blom-Cooper, L.: Privacy and Freedom. Bodley Head, London (1970)