International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 5 Issue 5, July-August 2021 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Privacy and Security on Social Media

Rachana Khandagale, Manali Gamre

Master of Computer Application, ASM Institute of Management & Computer Studies, IMCOST, Mumbai, Maharashtra, India

ABSTRACT

Social Media have become a integral part of human life. With over 1 billion users connected through online network. Social media is an online platform where we can share our information like text, photos, thoughts, videos, messages and many people have started to share seminar, workshop in Education domain and online survey, marketing, and targeting customers in Business domain. There are various social media platforms like Facebook, Twitter, WhatsApp, Instagram etc. The main purpose of these sites is to allow people to share activities, interests, real-life connections. Using social media we can communicate with the people in a world in a powerful and fun way. While enjoying on the social media platform it requires a great knowledge of privacy and security. The Internet is the safe place for only those people who are aware about the risk and the security, and can protect themselves from any fraud. Social media is a sometimes good because it allows you to share what actually we want to share, but it can also be used for negative purpose and in both the cases we are responsible for our security. In this paper we will describe about the privacy and security issues associated with social media.

KEYWORDS: *Privacy, Security, Social media*

How to cite this paper: Rachana Khandagale | Manali Gamre "Privacy and Security on Social Media" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-5 | Issue-5, August 2021, pp.485-489, URL: www.ijtsrd.com/papers/ijtsrd43821.pdf

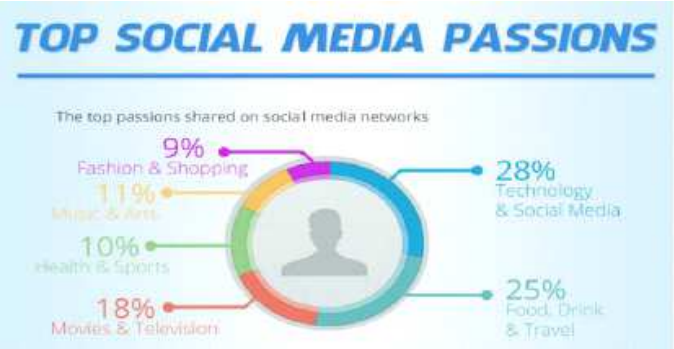
IJTSRD43821

INTRODUCTION

Social media is interactive technology that allow the user for creation or sharing and exchange of data, ideas, career interests, and other sorts of expression via virtual communities and social networks. It allows individuals to stay in-tuned with friends, family and relatives. Some people will use various social media applications to seek out career opportunities, connect with people across the world with like-minded interests, and share their own feelings, thoughts, and insights online. The level of human connectivity has reached extraordinary levels with over 4.33 billion social media users round the world at the beginning of 2021, equating to quite 55 percent of the entire global population. The massive amount of knowledge provided and shared on these social networks. It's going to add the knowledge a few users like personal details, current address, hometown, email addresses, activities, interests, favorite sports, teams, athletes, favorite music, favorite television shows, games, languages, his religious views, politics, inspirations , education history, relationship status, relations. The user also provides information within the sort of status information and tweets, which could include an idea, an act, a link. Of this information confess tons about the user, which can be of interest to varied groups.

Now a day, online social media websites such as Facebook, Twitter and LinkedIn all are the prime sites that are widely accessed on the Internet all over the world. The top 10 social media apps as of now are Facebook, YouTube, WhatsApp, Facebook Messenger, Instagram, WhatsApp, TikTok, QQ, Douyin, and Sino Weibo. Facebook is the most used social media platform in India, with around 86% traffic on internet. Instagram and YouTube are far behind than Facebook. Privacy and security are the major concerns in IT application like to run or install software. The social media should not disclose personal information of users' profile. The privacy challenge is privacy is not only attacked from the outside, but in reality 80% chances of attacks are found to be due to human errors. This happens because the user do not understand the consequences of data they have provided on social network. Some information is private, and some information is public.

Social media sites gained 490 million users in a year. Social media platforms gained 1.3 million users each day and we can say 15.5 new users every second. Facebook has around 2.7 billion monthly active users .4.3 billion peoples use social media platform around the world .90% of people have access to the internet use social media.



Information shared in social media

In social media, 9 % information has shared is related to fashion and a shopping, 28% is related to a technology and social media, 18 % is related to movies and a television, 10 % is related to a sport and health and 25 % is related to food, a drink and travel.

What is data privacy?

Data privacy is the protection of personal information from those people who not have access to it and the ability of individuals to determine who can access their personal information.

What is data security?

Data security is the process of protecting our sensitive data from unauthorized access. It includes all the various cyber security methods you have used to secure your data from a misuse, like an encryption, digital access restrictions, and more. Data security can be applied using a range of techniques and technologies, including a physical security, logical controls, administrative controls, organizational standards, and other techniques that limit access to an unauthorized user or a process.

RELATED WORK /LITERATURE REVIEW

1. Paper: In [April 2015] A Critical Analysis of Privacy and Security on Social Media.

Abstract: Privacy and security are the main concern of any social media sites such as Facebook, WhatsApp and Twitter etc. The social media network must not disclose personal data of the end-users profile. The privacy challenge is usually seen only in one direction because a person's privacy is not only attacked from the outside, but in reality 80% chance of attacks found to be due to human errors.

2. Paper: In [December 2015] On Privacy and Security in Social Media — A Comprehensive Study.

Abstract: It has been observed that privacy concerns are very feeble in the social networking sites and the users endeavors to make the appropriate changes on their social media privacy is lower than other mode of security methods. An enforcing a set of well-defined policies for social media, like, a strong password, awareness of changing password, awareness of information disclosure etc., we would secure the social networks from further attacks and vulnerabilities.

OBJECTIVE/ PURPOSE OF THE STUDY

We are trying to create awareness and common understanding related to privacy and security. There are many peoples who are using social media, but they are not aware about potential risk on the social media. Main purpose of the study is social media user should know about their privacy.

How to protect your information on social media?

1. Make sure to set your social media account preferences to private. Before posting anything on social media, check with whom you are sharing information. Make your post only visible to your friends not everyone on the internet.
2. Do not connect with any stranger on social media. Before friending someone once go through the mutual friends things or list which you have in common.
3. Don't upload high resolution images to your profile picture because it's easy to download from a computer or mobile. Make sure hide a street name, location, family members and any other information that can tell your where about.
4. Make sure you're not over sharing information on social media. Revealing much information online is never a good idea. When signing up for a social media never put your residential address. Never share pictures of any documents.
5. Don't tag or add any locations around your house on your pictures. Also, you can turn off location, geotagging so that no location-disclosing metadata is added to your photo files.

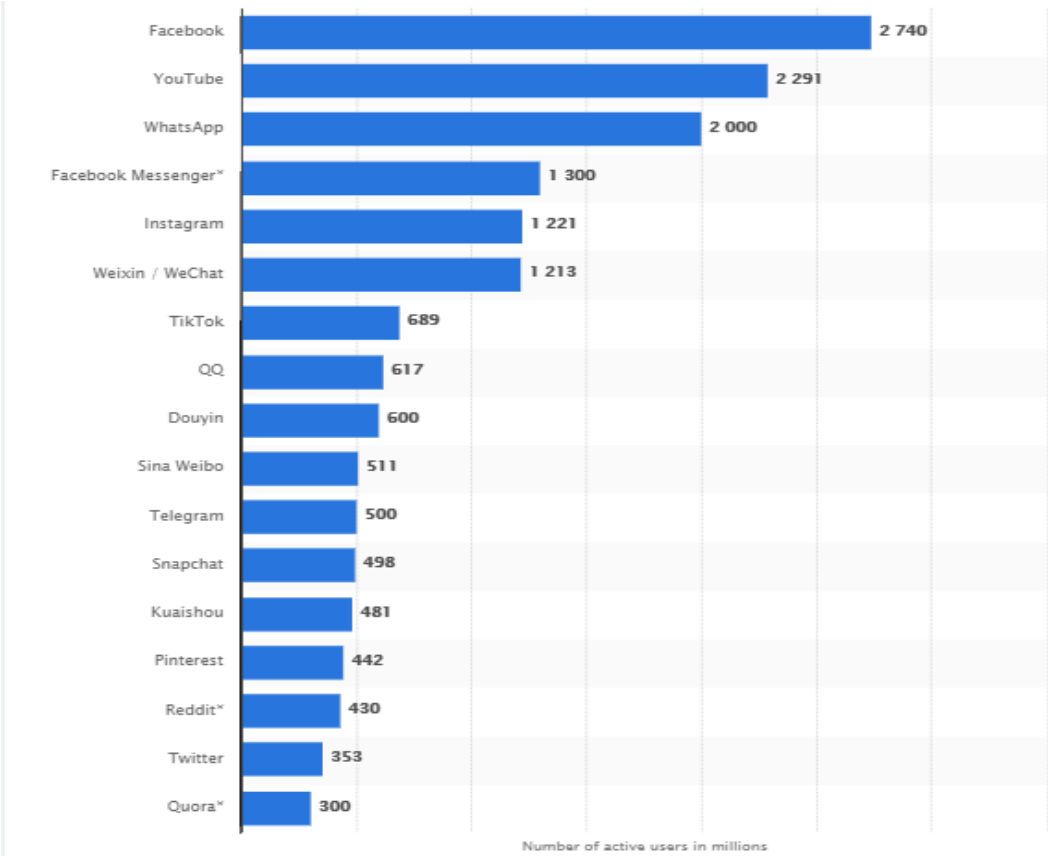
RESEARCH METHODOLOGY

We gather information from a different type of sources like research paper, Google browser, surveys, a newspaper, blogging, personal observation etc. after gathering all this data we put all this information in research paper. The information which we are gathering it all into the support of this research topic and also providing the information of how you can secure data on social media. We can say all it is happening because lack of a security, and privacy. There are some people who are unaware about

privacy on social media. We did Research on social media attacks which were happened in last few months, which tells us that how importance security is. In this research paper we put all this information related and privacy and a security and social media attacks.

Data Analysis and Interpretation

Facebook having 2.797 billion monthly active users. YouTube's has reached to 2.291 billion users. WhatsApp has 2 billion monthly active users. Facebook Messenger has reached 1.3 billion monthly active users. Instagram's potential advertising reach is 1.287 billion monthly. WeChat has around 1.225 billion monthly active users. TikTok has around 732 million monthly active users. Douyin has 600 million daily active users. QQ has around 595 million monthly active users. Telegram has around 550 million monthly active users. Snap chat's potential advertising reach is 528 million monthly. Sina Weibo has 521 million monthly active users. Kuaishou has around 481 million monthly active users. Pinterest has around 459 million monthly active users. Reddit has 430 million monthly active users. Twitter's potential advertising reach 396 million.



THREAT

Threat is vulnerability in network, is an action performed by attackers or hackers to attack our data. In simple words, any sort of attack which is harmful to our computer and which corrupt our data is called as threats.

Types of Threats:

Spam- Spam is the same thing as junk mail. It's typically unsolicited advertisements for things like saving on insurance plans, home security installations, seafood offers or even personal loans. It's a type of messages we typically just toss in the trash can.

Malware- Malware is a program that is harmful to a computer user. These malicious programs can perform a variety of activity such as stealing and deleting sensitive information and monitoring users' computer activity.

Phishing- Phishing is deceptive and tries to manipulate you into revealing data about your identity, you're all account passwords and tries to infect your computer with malware. An attacker use collected social media data to spoof the sender of an email message and trick users into clicking links or sending the attacker private information.

Clickjacking- Clickjacking is an attack that tricks a user into clicking a webpage which contains invisible other content. The invisible page could be a malicious page and the user did not intend to visit that page. This simple clickjacking trick can force Facebook users to like groups or fan pages without knowing the user.

Fake Profiles- A fake profile is the representation of a person does not truly exist on social media. The images they use are taken actual people or organizations and later alter them. They are used to

spreading fake news related to politics or any famous people to create distrust.

Social leakage- Users share large amounts of data about themselves on their online social media. Besides the intended information, this sharing process often also "leaks" sensitive information or data about the users.

Chat Attack: Chat messages can be used to spread malware or promote phishing applications by impersonating you on chat and messaging your contacts the spam or malware to your contacts.

Viral spam chain: If we click a link on Facebook it will send a spam to our Facebook friends. To prevent such spam chain you do not open such type of links.

PRIVACY

Data privacy is the protection of personal information from those who should not have access to it and the ability of individuals to determine who can access their personal information.

Types of privacy issue

1. **Privacy concerns regarding Social Media Sharing Services**

Social media sharing services, which allow user to create or share contents. YouTube is an example of sharing service for video and audio, Instagram is the service for sharing photos and many more. Posting Content such as video and picture arise new privacy concerns due to their context revealing details about the physical and social context of the subject.

2. **Privacy concerns regarding Social networking services**

Social Networking sites are the sites aimed for to document about one's life, micro-blogging his/hers liking and disliking and everyday happenings in life. Social networking sites such as Facebook create a repository of personal data.

3. **Sites Convergence**

A recent issue of site convergence related to privacy on today's internet is the that users have 'profiles' and accounts on different social media sites, if we gather the information from all the sites and if puzzled together provides the picture of user.

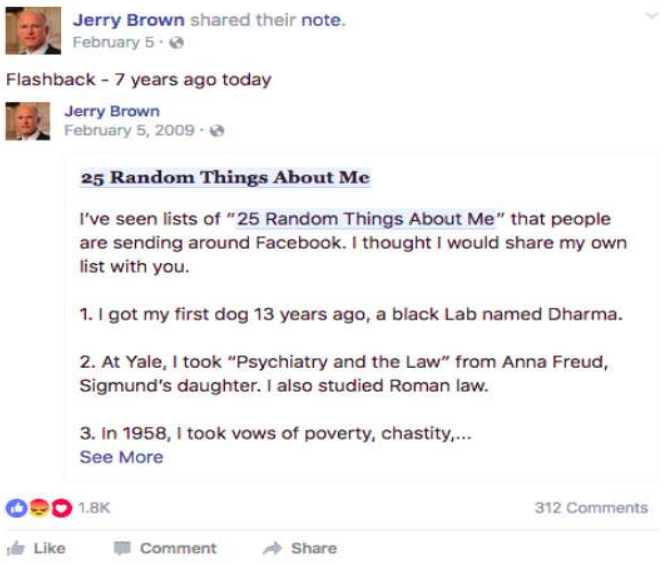
SECURITY

In privacy concerns, social media sites or applications can be used by cyber criminals or hackers to attack you or your devices. Following are some steps to protect yourself:

1. **Login**: Protect your social media account with a strong password and do not share that password with anyone and never reuse that password for other any sites. Some social media sites like WhatsApp support two-step verification. Whenever possible enable stronger authentication methods to your accounts.
2. **Encryption**: Many social media sites allow us to use encryption called HTTPS to secure your connection to the site. Some sites like Twitter, Facebook and Google+ have already this enabled by default, while other sites require you to manually enabled HTTPS via settings. Whenever possible use HTTPS rather than HTTP.
3. **Email**: Be suspicious of emails that claim to come from a social media site; these can easily be spoofed attacks sent by cyber criminals or hackers. The easiest way to reply to such messages is to log in to the website directly and check any messages using the website.
4. **Malicious Link**: Be cautious of suspicious links or potential scams posted on social media sites. Cyber criminals can post malicious links, and we click on link, then they can take you to websites that attempt to spread or infect your computer. Always think, just because a message or link is posted by our friend does not mean it is from them, it can be also from criminals, as their account may have been hacked.
5. **Apps**: Some social media sites give you the permission to install third-party applications, such as games. Always Keep in mind they may have full access to our account and personal information. Data Breach on social media.

DATA BREACH

We all are using Facebook there are some viral social media quizzes. Innocent though they may seem, but these social media quizzes can put us in the crosshairs for hackers and cyber. They are a prime example of over-sharing sensitive information online, which has grown rampant with the advent of social media.



Over-sharing not limited to viral quizzes or trends. Posting publicly about vacations, a family, your physical location can, in some cases, put you at a risk. Most people know not to post images of their debit, credit cards or disclose any type of sensitive login of financial information, but a surprising number of people posts their phone numbers, a residential address on social media. Because if we have internet banking at that time they are asking us some security question, sometimes the question has asked by banks and Facebook quizzes a question is same. If hackers have our any banking details, and they have needed some more information. In such case they are got answers of this question from any social media then they can easily hack your bank account password.

SCOPE

As we know that when we are using social media we need to very protective about our data because some hackers or cyber criminals are always hungry for the information. A privacy is not only attacked from the outside, attacks can be happened due to human errors. And some attacks are planned by the hackers. A privacy protects our data we do not want shared publicly like health or personal finances related information. But some time data breach or a data leakage happens via social media, they can reveal our information to the third party and a target the organization or users. To avoid such problems we can protect data are using privacy tools provided by social media applications, that's why privacy and a security have a huge scope in this study.

CONCLUSION

It has been seen that Social networking sites have become a target for attackers due to the availability of sensitive information, as well as its large user base. That's why privacy and security issues in social media are increasing. The purpose of this paper is to address different privacy and security issues. A privacy issue is the main concern, since many social media user is not very careful about what information they expose on their social media. If we went for enforcing a set of well-defined policies for social media, like, awareness of changing a password often, awareness of an information disclosure, a strong password, we would secure the social media from further attacks and vulnerabilities.

REFERENCES

[1] https://www.researchgate.net/publication/301234158_On_Privacy_and_Security_in_Social_Media_-_A_Comprehensive_Study

[2] https://www.researchgate.net/publication/281711350_A_Critical_Analysis_of_Privacy_and_Security_on_Social_Media

[3] https://core.ac.uk/download/pdf/82396532.pdf

[4] https://ris.utwente.nl/ws/portalfiles/portal/5095526/literaturereview.pdf

[5] https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/