International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT2173147

A Study on Extent of Awareness Among College Students in Security and Privacy Issues in Social Media

Dr. J. Padmavathi, Sirvi Ashok Kumar Mohanlal
Associate Professor[1], BCA Student[2]
[1, 2]Department of Computer Science & Application, SRMIST, Kattankulathur, Chengalpattu District, Tamil Nadu, India

Article Info
Volume 7, Issue 3
Page Number: 676-682

Publication Issue :
May-June-2021

Article History
Accepted : 12 June 2021
Published : 20 June 2021

ABSTRACT

Today Social Media is an integral part of many people's lives. Most of us are users of one or many of these such as Facebook, Twitter, Instagram, LinkedIn etc. Social media networks are the most common platform to communicate with our friends, family and share thoughts, photos, videos and lots of other information in the common area of interest. Privacy has become an important concern in social networking sites. Users are not aware of the privacy risks involved on social media sites and they share their sensitive information on social network sites. While these platforms are free and offer unrestricted access to their services, they puzzle the users with many issues such as privacy, security, data harvesting, content censorship, leaking personal information etc. This paper aims at analyzing, the major users of social media networks, namely, the college students. It was intended to assess the extent the consumers' are aware of the risks of free usage and how to mitigate against these privacy issues.
Index terms : Social Media Networks, Data Security, Privacy, Data Harvesting, Mitigation Techniques.

I. INTRODUCTION

The users of social media networks have no control over their data. Once the user creates a social account, he/she unknowingly relinquish their right to personal information and have no control over the data consent. The service providers take wholesome right to dictate terms on our usage. It is from our likes and interest the owners of social networks dispose of data to the advertising agents and make a profit for themselves without the users' consent. This leads to the misuse of data causing threat to privacy and security of user information. Users are unaware of the privacy risks involved in social media sites and they share their sensitive information on the social network sites [1].

The recent Facebook data breach shows that security is poor. In 2012 a hacker broke open the LinkedIn network and got away with about 6.5 million encrypted passwords. In 2016, LinkedIn said hackers were attempting to sell what they claimed were 117 million email addresses and passwords of its users. In 2018, 52.5 million users were affected in a new

Google Plus data breach. These users are susceptible to attacks which expose their personal information. The privacy leak is based on studying how the users use these sites. Attackers can easily access and gather the personal and sensitive information of users. Users are the least concerned about the security setting. Hence they easily become a victim of privacy and identity breach.

Lack of cyber knowledge is the main cause of all problems. People publicize their private photos and personal information on the network and fall prey to the anti-social elements that create unimaginable troubles in the personal life of a person. The addiction to these social media network also brings in imbalance in psychological behavior of a person. A graduate from Tiruchengodu is a victim due to excess use of Facebook which enticed her to share her personal life and day to day activities. This has put her into severe mental trauma and the family had to fight and rescue her with medical support.

II. METHODOLOGY

In this research, a well-structured questionnaire was created and 450 students participated and registered their answers through Google form. The survey covered both male and female undergraduate students, and a survey is conducted anonymously. Research questions such as:

- How old are you?
- Do you really know all the fiends on Facebook or Twitter or Instagram?
- Have you ever got a friend request from someone who is already your friend, any
- How frequently do you post? , and so on, were framed to assess the awareness factor of privacy and security. Statistical analysis was performed and it was.
- How concern they are about their privacy?
- Have you ever checked out your page to see what it looks like to a stranger?
- Do you use the same user name and/or password for multiple social media applications?
- Does your password contain general words or phrases or place names or dates that you have posted online, or that are available in your social media profile?
- Have you ever received a message (of any type), asking you to log in and verify something on one of your social media applications?
- Do you permanently keep any social media app logged in on your mobile phone?
- Do you store your bank account details, credit card numbers, pin numbers, passwords on your mobile?

III. EXPERIMENT AND RESULTS

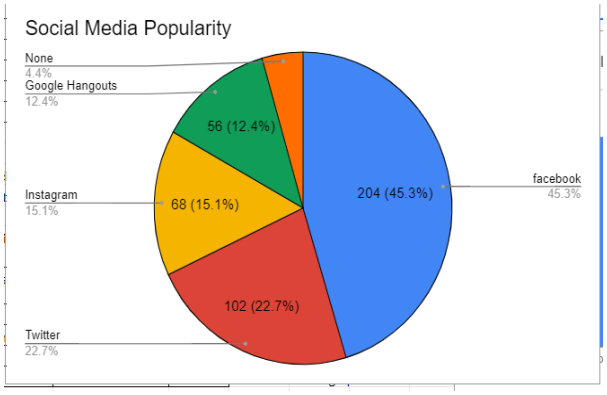

Fig. 1. Social Media Popularity

The survey shows that nearly 45% of students love to spend their time on Facebook. Twitter and Instagram were the second and third choice of students 23% and 15% respectively

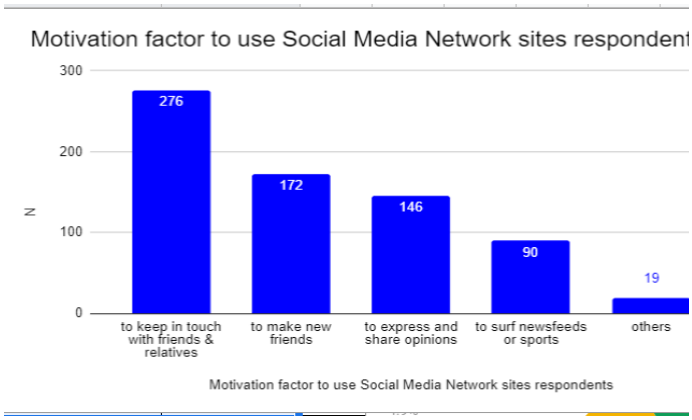

Fig. 2. Motivation factor to use social media

This pie chart shows the motivation factor for them to use social media

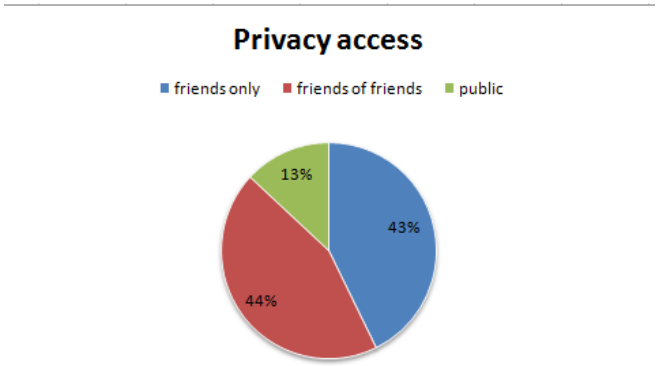

Fig. 3. Privacy access on social media

More than 44% of students profile always remains on friends of friends

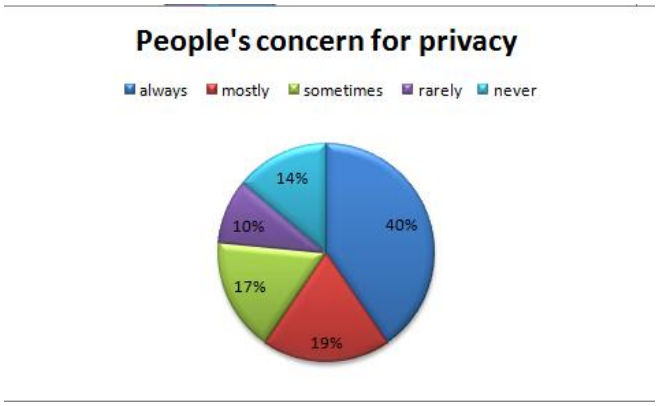

Fig. 4. People's Concern for privacy

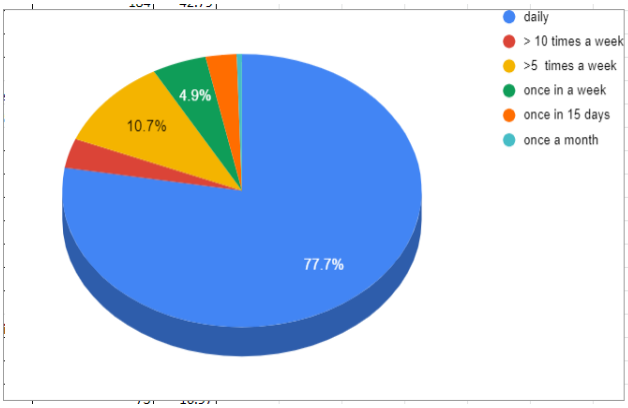

Fig. 5. Frequency in status update

It was observed that about 77.76% of the students were using the social media sites update their status daily and Post something on their timeline.

In a survey it was asked to students how many hours they usually spend on social media, the survey showed on average students usually spend 4 hours on social media and the maximum record was 15 hours a day

SOME STATISTICS

- More than 60% of students accepted a friend request from someone they aren't sure that they know.
- More than 70% of students have received a friend request from someone who is already their friend? More than 80% of time students accepted that request.
- 59% of students have checked out their page to see what it looks like to a stranger.
- 60% of users use the same user name and/or password for multiple social media applications.
- More than 75% of users keep their account login into device.
- More than 80% of students never ever accept privacy policy before accepting it.

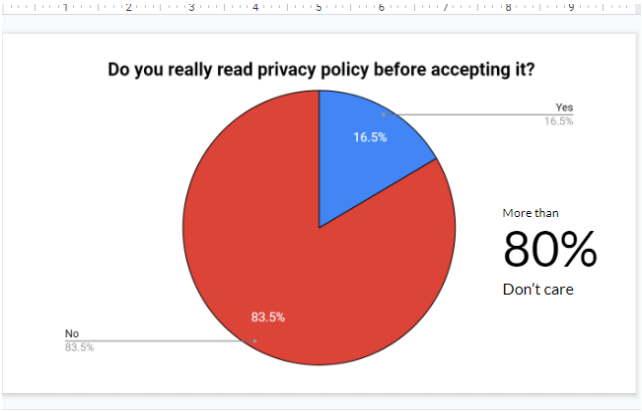

Fig. 6. People's Concern for privacy policy

The following methods restrict an unauthorized user from viewing our photos and information [2].

a. In Facebook, click on privacy setting for new users and set to Friends Only. To set this, visit Settings > Privacy -> who can see your post?

b. In Twitter, click on Settings > Security and privacy > Privacy > Tweet Privacy > Protect my Tweets.

c. LinkedIn: Settings > Account > Helpful Links > Edit your public profile.

d. Google+: To change this setting, type the name of a Circle in the "To" field below your post before you publish it to make sure who can see your post.

According to the author [3], their analysis showed that privacy leakage could still happen even after users correctly configure their privacy settings. We examined real-world OSNs (Online Social Media Network) including Facebook, Google+, and Twitter, and discovered the exploits which lead to privacy leakage

IV. MAJOR THEFTS

Some of the major threats in social media are as follows:

4.1. Identity theft

Identity thieves gather your personal details from social media sites. Even the account is on the highest security settings, there are still ways to access your information. Most social network sites have information have information such as email address or birthday. It's common for an identity thief to hack an email account by using social information because the most common type of password can be guessed. For example, a common technique to get your personal information is by clicking on "forgot password" and trying to recover the information through recovery email. Once the thief has access to your email account, they can easily access to all information on your social networking sites or they can change the password and hack your account.

Some precautions to tackle this are:

- Setting a strong password. The stronger our password, the harder it is to guess. Use of special characters like symbols and capital letters when creating your password, and avoiding passwords, like your birthday or your child's name.
- One should be careful with one's status updates. We often post status updates that would give an identity thief information they need and misuse it. For example, you may post Birthday wish to mother and then tag her in the post. Likely, your mother's maiden name will be posted with that tag. A popular security question on these sites is "What is your mother's maiden name?" and if you share such information online, you put your account on risk and thieves get access to your account by answering these commonly used question.
- Do not reveal your location. You can use a fake location by updating your location as another city and state. You can leave this information blank. Be cautious and never use a city and state where you live until there is a necessity for it.

4.2. Getting Your Profile Hacked

Hackers love social networking if they get access to source code they can interject malicious code. These code hackers, can steal our identity, data, inject

viruses in our computer, and steal bank account details, etc. Shortened URLs, such as those created on bit.ly, are especially vulnerable to hackers. These can trick users and make them visit harmful sites where personal information can be compromised because the full URL is not seen.

The best advice is to never click on a link until we are sure of the source. The following methods help in checking if a site is safe or not.

- Hovering over the link: - If we hover over a link without clicking, we will see the full URL in the lower corner of our browser. If this is a website that we are able to recognize then we can go ahead and click.
- Trying a link scanner. A link scanner is a website that lets us enter the URL of a link that we suspect to be suspicious and checks for safety. We can try URLVoid or MyWOT for this.
- Check shortened links. A shortened link is quite popular on sites like Twitter where; character length matters. Some shortened link sites such as bit.ly, Ow.ly, and TinyURL are used. Use a service like SuCuri to we suspect if the real link is secure helps us from falling prey to hackers.

According to author[6] ,If we would pass for imposing a fixed of nicely described guidelines for social media, like, a robust password, recognition of changing password often, awareness of information disclosure, purpose of antivirus or related software program, and proprietary software and so on, we might secure the social networks from similarly attacks and vulnerabilities

4.3. Letting Stalkers Find Your Details

When we use social networking sites, and we post private personal information, it can be misused. The more we post, the more vulnerable we become to those who may wish to harm us. Even if we have the highest security settings, friends, associates, and even the brands we "like" on our networking sites, can unintentionally leak information about us. Apart from this, the websites we subscribe to, the apps that we download, and the games that we play on social networking sites contain personal information about us. Every time we browse a website, companies can put invisible markers on our computer called cookies. In theory, no two cookies are alike. When we are online, these cookies track our activity as we move from site to site.

To prevent sites from tracking our activity, we must click on the "Do Not Track" feature. Most websites provide an option for this. We can also clear the cache and cookies on our browser regularly to help prevent any problems.

4.4. Letting world know you are not home

Telling the online world where we're going and when we aren't at home is inviting burglars to our house. Burglars are fond of constant updates, especially about our travel plans.

The general don'ts that are to be followed when we go on a vacation are:

- Avoid posting specific travel plans. Never post such plans like when, where, or how long you'll be gone.
- Wait until you come back home to post pictures to a vacation album.
- Use the highest privacy control possible. Only let a very close group like a family group, view your photos.
- Be very selective in terms of status updates. It is better to use the audience-selector dropdown menu on Facebook to choose which groups can see your status updates.
- Stay offline. After all, you are on vacation enjoy your time. Relax and forget about social media for a few days.

4.5. Overconfidence is very dangerous

Overconfidence is one of the biggest threats to once privacy. When they are at home or at work many users believe as long as they have a firewall and an antivirus installed in their system, there is no threat to their privacy and security. Many people do believe that they don't have anything worth hacking or stealing so there's no need to worry about security. The kind of technology we have today, we are more connected to each other than ever before. When we neglect our own security, we not only put our self at risk, but others who are socially connected with us are at risk as well.

The Location-Based Social Network Services (LBSNS) such as FireEagle, Google Latitude, Nearby etc, are able to identify not only the location of a person but also the location of other people connected to that person[9].

To keep us and our information safe, pay careful attention to your online activity. Avoid posting information including:

- Travel plans
- Bank account information
- our full address and birth date
- Our children's names, school, and birthdates, etc.
- Location information, such as the name of your workplace
- Our daily schedule, etc…

The author [7] concluded that the importance of online social networks sites to human social development cannot be over-reduced but it needs a way to fix it. On the other hand, privacy and security of a social network is not the same as any web2.0 which is centralized, because in social networks you are dealing with data integration and online social networks sites allows people to interact to each other freely, conduct businesses and above all serve as a media for all

V. ALTERNATIVE

The whole issues with social media are that it is centralized that all of the user data is handled by the 'Giant social media Company'. They own user's data. Data harvesting is one of the other issue faced by social media network, people are not able to keep track of their content. Question is, where it goes? , who controls it? And what they do with it?

Blockchain can be an alternative system for the next generation social media concept [10], The data on blockchain are decentralized and even people can keep track of their post as to where it goes, who shares it, who accesses it. One of the most preferable feature is that once a post is deleted it should get deleted from everywhere or at least get cryptographically encrypt so that no one can read or see it again nor does it get spread across the social media.

We live in a world where people are continuously creating content online and posting it, some of them are truly providing values to society but they don't get paid much. Distributed ledger technology enables users to make transactions privately as only the sender and recipient know about the transaction's contents.

VI. CONCLUSION

There is huge difference between knowing social media security issues and getting aware of it. Our survey showed that the college students knows about the security issues , they have concern for their privacy but still they don't do anything that can make them secure. They are vulnerable.

Social Media is a great way to connect with each other, but as with every good fortune, there is a curse. Students should get aware of their privacy and

data. We can still use social networks for all they were meant to accomplish, but we need to take extra precautions for ourselves to make sure our personal information doesn't get in the wrong hands. To know what threats you are most vulnerable and to take steps to protect self and our networks is mandatory.

VII. REFERENCES

[1]. Roshan Jabee and M. Afshar Alam Issues and Challenges of Cyber Security for Social Networking Sites (Facebook) International Journal of Computer Applications (0975 – 8887) Volume 144 – No.3, June 2016.

[2]. Joshana Shibchurn, Yan. Xiangbin Information disclosure on social networking sites: An intrinsic–extrinsic motivation perspective Computers in Human Behavior., 44 (2015), pp. 103-117.

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

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

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

[6]. Mrs. Lekana L, Mr. Venkatesh S Bhat & Prof. Santhosh Rebello , Secure Platform To Enhance Privacy And Security In Online Social Media,International Journal of Latest Trends in Engineering and Technology Special Issue SACAIM 2017, pp. 534-538 e-ISSN:2278-621X.

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

[8]. Gail-Joon Ahn, Mohamed Shehab, Anna, Squicciarini Security, and Privacy in Social Networks IEEE Internet Computing, 15 (3) (2011), pp. 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, 27 (4) (2011), pp. 163-200.

[10]. Blog post by katalyse.io section 'How blockchain can be a solution?' https://medium.com/swlh/how-blockchain-is-solving-the-biggest-problems-in-social-networking-4d78faa233fc (2018).

[11]. Imrul Kayes , Adriana Iamnitchi Privacy and security in online social networks: A survey Elsevier B.V (2017).

[12]. David Hiatt ,Young B. Choi Role of Security in Social Networking (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 2, 2016.

Cite this article as :

Dr. J. Padmavathi, Sirvi Ashok Kumar Mohanlal, "A Study on Extent of Awareness Among College Students in Security and Privacy Issues in Social Media", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 7, Issue 3, pp.676-682, May-June-2021. Available at doi : https://doi.org/10.32628/CSEIT2173147
Journal URL : https://ijsrcseit.com/CSEIT2173147