National Conference on Communication Technology & Network Security In association with
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 7 | ISSN : 2456-3307

# Security and Privacy Issues in Online Social Networking

**Prof. K Adisesha*[1], Dr. Lakshma Reddy[2]**
*[1]Research Scholar, Himalayan University, Karnataka, India
[2]Research Guide and Principal, SJES College of Management Studies, Bangalore, Karnataka, India

## ABSTRACT

The advent of online social networks (OSN) has transformed a common passive reader into a content contributor. It has allowed users to share information and exchange opinions, and express themselves in online virtual communities to interact with other users of similar interests. However, OSN have turned the social sphere of users into the commercial sphere. This should create a privacy and security issue for OSN users. OSN service providers collect the private and sensitive data of their customers that can be misused by data collectors, third parties, or by unauthorized users. In this paper, common security and privacy issues are explained along with recommendations to OSN users to protect themselves from these issues whenever they use social media.
Keywords: OSN; security; classic privacy threats; modern threats, risk management in youth.

## I. INTRODUCTION

Social media are a source of communication between the data owner (data generator) and viewers (end users) for online communications that create virtual communities using online social networks (OSN). A social network is a social graph that represents a relationship among users, organizations, and their social activities. These users, organizations, groups, etc., are the nodes, and the relationships between the users, organizations, groups are the edges of the graph. An OSN is an online platform used by end users to create social networks or relationships with other people that have similar views, interests, activities, and/or real-life connections. A large number of different types of social-networking services are available in the current online space.


**Figure 1: Usage of social-networking sites**

The following are some of the common features in social-networking sites:

- All current online social-networking services are web-based, using an Internet connection. Contents are stored on cloud storage through a centralized access management system. These contents can be accessed from anywhere using an Internet connection and web browsers.
- OSN users need to create a public profile for social-network sites as per their predefined format. This profile information is primarily used for the

authentication process to log into the social-networking site.

- Almost all existing social-networking services facilitate users in developing their social relations with other users by connecting a user's profile with others having similar profile information.
- One interesting feature of the existing OSNs is that contents on these sites are user-generated, while OSNs use these contents for business purposes.

The main goal of OSNs is to share contents with maximum users. Users utilize OSNs, such as Facebook, Twitter, and LinkedIn, to publish their routine activities. Sometimes, OSN users share information about themselves and their lives with friends and colleagues. However, in these published data, some of the revealed contents through the OSN are private and therefore should not be published at all. Typically, users share some parts of their daily life routine through status updates or the sharing of photographs and videos. Currently, various OSN users utilize smartphones to take pictures and make videos for sharing through OSNs. These data can have location information and some metadata embedded in it. OSN service providers collect a range of data about their users to offer personalized services, but it could be used for commercial purposes. In addition, users' data may also be provided to third parties, which lead to privacy leakages. It also offers a set of techniques to an organization for data analysis and making decisions based on this retrieved information. Data privacy protects information from unauthorized and malicious access that discloses, modifies, attacks, or destroys the data stored or shared online.

For example, researchers related to information retrieval sometimes do not consider privacy issues while designing solutions for information retrieval and management. On the other hand, researchers who work on data privacy usually restrict information-retrieval techniques to protect sensitive data from adversaries who seek personal information.

With the emergence of social media and the growing popularity of online communication using OSNs, more sensitive information about individuals is available online. Though much of the data that are shared through OSNs are not sensitive, some users publish their personal information. Thus, the availability of publicly accessible sensitive data can lead to the disclosure of user privacy.

The privacy of users is at more risk when publicly available data can be traced, and their activities can be connected with these data for mining and extracting sensitive information from it.

Privacy has different meanings in different situations, and the intensity of privacy depends upon the context of shared contents. Information gathered from social media for analysis purposes is generally unintended and often irrelevant. However, it may be related to the private activities of a person, for example, religion or political affiliations.

The main focus of the paper is to point out that privacy and security issues related to OSN, and educate ordinary users on how to protect themselves from these security and privacy issues. Privacy is the right of someone to keep information to themselves or at least share it only with relevant people. Privacy-preservation and -protection terms are used to keep private information away from irrelevant users.

## II. Objective

The objective behind this work is to give a brief overview of raised privacy and security issues due to the use of OSNs. This is a fact that is necessary for everyone to use one a technological acility for smooth and fast communication. Social media are one type of these communications that have both negative and positive effects to their users. OSNs make information sharing more convenient and rapid than real-life communications. They make globalization a reality

and provide a chance to their users to express themselves. OSNs are also a new way for international relationships, whether the relationship is related to business or social interactions. It is easy for people to interact with each other using OSNs anytime and anywhere in the world. Along with these advantages, social media have disadvantages, one of which being the issue of privacy and security. In this paper, the issues that can harm OSN users are discussed, in addition to giving them recommendations on how to protect their privacy while using OSNs. The rest of the paper is organized as follows. Section 3gives an overview of the privacy and security threats in OSNs. Section 4 gives about different privacy and security treats for youth in OSNs.

## III. Privacy and Security Threats in OSNs

User-generated content on social media may include users' experiences, opinions, and knowledge. In addition, it may also include private data, for example, name, gender, location, and private photos. Online-shared information is electronically stored and is therefore permanent, replicable, and rechargeable. OSN users generally face the challenges of managing their social identity while compromising their social privacy. The popularity of social media is such that worldwide active users of social media are expected to reach around 2.95 billion by 2020, which is about one third of the world's entire population.

The total active users accessing different popular social media networks are presented in figure 2. Popular Online Social Networks (OSNs) and their total active users in millions.


**Figure 2** : Frequency of Social Media Usage

Taking into account this global number of users, privacy is one of the obvious and critical issues regarding OSNs. Various privacy issues are fostered because of OSNs, such as surveillance, in which the social sphere of OSNs changes to a commercial sphere and OSN service providers supervise user actions for market force access control. Standard OSNs share users' personal data with third parties for advertisement purposes that may be exploited. Likewise, OSN users leave digital imprints when they browse OSN sites, and therefore are targeted as data sources for commercial uses and user profiling.

In India, the number of internet users stood 296.6 million when compared to 2015 and 2016 where the increase rate is relatively lower as compared to the growth ranging from 142.23 million to 168.1 million. Nevertheless, the number of Social Media users in our country are expected to cross over 450 million by 2023 as shown in the figure 3. The most popular social media site in the year 2017 was Facebook, and later WhatsApp and Instagram remained the popular choice among the social media platforms.

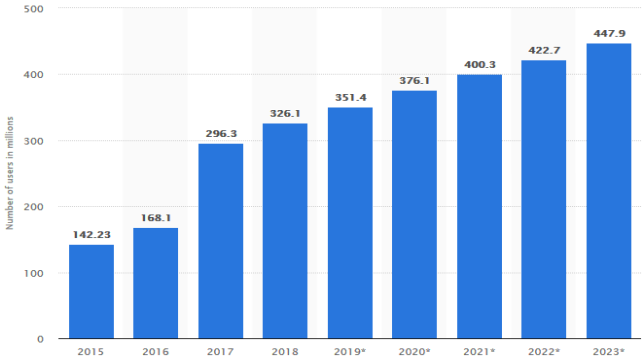


**Figure 3 :** Social network users in India from 2015 to 2023 (in millions)

Social-networking tools have changed the way we interact in our personal and professional lives.

Although they play a significant role in our social and business lives, at the same time they bring

about high risks concerning privacy and security. As hundreds of thousands of users use OSNs on a regular

basis, they have attracted the attention of attackers more than any other target in recent years. Because of the high usage of social media, online users have been exposed to privacy and security threats. These threats can be categorized into classic and modern threats. Classic threats are online threats that not only make OSN users vulnerable, but also other online users who do not use any OSN. The second type of threats is modern threats, which are related to OSN users only because of the OSN infrastructure that can compromise user privacy and security. The report states that social media are not included in the risk-evaluation scoring system but they are one of the top types of platform for cybersecurity.

**Classification of Threats in social Media are:**

### 3.1. Classic Threats

Classic threats have been an issue ever since the development of the Internet. These threats are spam, malware, phishing, or cross-site scripting (XSS) attacks. Although researchers and industries have addressed these threats in the past with the invention of OSNs, they can spread in a new way and more quickly than ever before. Classic threats are used to extract the personal information of users, which are shared through an OSN, not only to attack the target users but also their peers by adjusting the threat to correlate to users' private attributes.

#### 3.1.1. Malware

Malware stands for malicious software. It is a generic term that refers to intrusive software.

It is developed with the intention to log into someone's computer and access their private contents. A malware attack on social networks is easier as compared to other online services because of the structure of an OSN and the interactions among users. The worst malware case is to access users' credentials and impersonate them to send messages to their peers. For example, the Koobface malware was spread through OSNs such as MySpace, Facebook, and Twitter. It was used to collect login credentials and make the target-infected computer a part of a botnet. An OSN has a vital role for various purposes, for example, marketing and entertainment. However, it has opened up its users to harmful activities. Committing fraud and propagating malware are criminal actions wherein users are engaged to access a URL and run a malicious code on the computer of an OSN user.

#### 3.1.2. Phishing Attacks

Phishing is another type of fraudulent attack in which the intruder acquires the user's personal information by masquerading as a trustworthy third party through either a fake or stolen identity.

For example, during an attack that was attributed to intelligence by the Chinese government, senior U.K. and U.S. military officials were tricked into becoming Facebook 'friends' with someone impersonating the U.S. Navy Admiral James Stavridis. Similarly, social media were used in many places by phishers posing as other persons.

#### 3.1.3. Spam Attacks

Spam messages are unwanted messages. In OSNs, spam comes as a wall post or a spam instant message. Spam in OSNs is more dangerous as compared to traditional email spam because users spend more time on OSNs. Spam messages normally contain advertisements or malicious links that can lead to phishing or malware sites. Generally, spam comes from fake profiles or spam applications. In case of a fake profile, it is normally spread from a profile created in the name of a popular person. Spam messages normally come from compromised accounts and spamming bots. However, the majority of spam spreads from compromised accounts. Spam-filtering approaches are used to detect a malicious message or URL in a message and filter it before delivering it to the target system.

#### 3.1.4. Cross-Site Scripting

XSS is a vulnerable attack on web-based applications. It is one of the most common and serious security problems that drastically affect web applications. An XSS attack allows an intruder to run malicious code on the targeted user's web browser that results in compromised data, theft of data stored in the form of cookies, and saving passwords and credit-card numbers. Furthermore, an attacker can use XSS with a social-network infrastructure and develop an XSS worm that can be virally spread on OSNs.

### 3.2. Modern Threats

These threats are typically related to OSNs. Normally, the focus of modern threats is to obtain the private information of users and their friends, for example, an attacker wishes to know about a user's current employer information. If users have their privacy setting on their Facebook account as public, they can be easily viewed. However, if they have the customized privacy setting, then it is viewable to their friends only. In this situation, the attacker can create a Facebook profile and send a friend request to targeted users. Upon acceptance of the friendship request, details are disclosed to the attacker. Similarly, the intruder can employ an inference attack to collect users' personal information from their peers' publicly available contents.

#### 3.2.1. Clickjacking

Clickjacking is also known as a user-interface redress attack, wherein a malicious technique is used to make online users click on something that is not the same for which they intend to click. In clickjacking attacks, an attacker can manipulate OSN users into posting spam posts on their timeline and asks for 'likes' to links unknowingly. With a clickjacking attack, attackers can even use the hardware of user computers, for example, a microphone and camera, to record their activities.

#### 3.2.2. De-anonymization Attacks

De-anonymization is a strategy based on data-mining techniques, wherein unidentified information is cross-referenced with public and known data sources to re identify an individual in the anonymous dataset. OSNs provide strong means of data sharing, content searching, and contacts. Since the data shared through OSNs are public by default, they are an easy target for deanonymization attacks. In existing online services, pseudonyms are used for data anonymity to make the data publicly available.

#### 3.2.3. Fake Profiles

A typical attack in most of the social networks is a fake-profile attack. In this kind of attack, an attacker creates an account with fake credentials on a social network and sends messages to legitimate users. After receiving friendship responses from users, it sends spam to them. Usually, fake profiles are automated or semi-automated and mimic a human. The goal of the fake profile is to collect the private information of users from the OSN, which is accessible only to friends, and spread it as a spam. The fake-profile attack is also a problem for the OSN service providers because it misuses their bandwidth.

#### 3.2.4. Identity Clone Attacks

An attacker using theft credentials from an already existing profile, creating a new fake profile while using stolen private information, can perform Profile cloning. These attacks are known as identity clone attacks (ICAs). The stolen credentials can be used within the same network or across different networks. The attacker can use the trust of the cloned user to collect contents from their peers or perform different types of online fraud.

## IV. Social Media Privacy & Security Risks for Youth

Let's find out what are the privacy & security risks the youth generation is facing from social media. In

addition, we will try to find out how to access the risks and what are the options to prevent those:

#### 4.1.1. Profile Hacking:

Profile hacking is the most common issue in social media scam lists. Hacking one's social media account is not a difficult task for hackers. It takes just minutes for them to do it. Cracking the passwords of social media user accounts is the most common way to hack one's profile. These hackers include mostly the ones who are technically sound in computing.

#### 4.1.2. Fake Apps and Malicious Links

There are many fake apps and links, which attain all your personal information including mobile numbers, email ids, passwords, residential addresses, and other personal details. With the help of these details, one can be easily prone to fraudulent situations; maybe a life of unwanted and unfortunate disturbances. All these apps and links have been deleted from the web network. However, there are still many people who are trying to get into it by creating more new things to carry out frauds.

#### 4.1.3. Fake offers & schemes:

It is often observed that young people have a tendency to do shopping through several e-commerce platforms or online portals. They often get to see advertisements regarding their recent searches on social media platforms. Almost all of them get tempted to click on those links to check out recent offers on their favorite items. Hackers are taking advantage of this eagerness amongst young users. They are creating fake offers on expensive products; thereby encouraging them to click on those links and piercing into the system of users.

#### 4.1.4. Login to social media channels through other networks:

As most of the young adults don't have premium smartphones or laptops, they try to serve their needs by using devices of their friends or cyber café. They often tempted to access their social media profiles through strange devices and even forget to log-off in rush. This may put them in serious risks of account privacy. An unknown person can access their social media profile and make changes to it according to their wish.

#### 4.1.5. Fake Gaming software and apps:

Young adults spend maximum time of their day on playing games. They either prefer to play these games online or tempted to download and install gaming software to play it offline. Hackers are very much aware of this fact. They create several fake online and offline games that help them to sneak into the system of young users without even giving them a slight hint. Downloading any unknown or new game also put users in the high risk of downloading viruses or dangerous malware.

### 4.2. Risk Assessment

If you clicked on any link through your social media profile but observed that you are directed to some other websites which are not even close to what you were looking for then it's time to get alert. Most of the fake websites even make it hard for you to take an exit. They want you to spend maximum time on their platform; thereby they force you to share your personal details with them.

Most of the fake websites persuade you to check on their 'allow' notification bar. It thereby sending a lot of spam messages to your email id or social media profile. If you are getting constant emails or notifications on your social media profile from the

website to which you have never subscribed before then take it as a threat signal.

**Following are some prevention methods.**

**4.2.1. Think twice before clicking any links:**

There are many malicious links presents on social media nowadays which are meant for making cyber frauds. These lead to unwanted viruses or maybe one might create the links to attain the address of the social media users who click the links. These things further lead to undesirable and much devastating issues. So, think twice before you click any link!

**4.2.2. Identifying Fake Apps before installation**

As mentioned above, there are many applications in the market of social media which gains almost all the confidential information of social media users (that should not be shared by any means), and this information is proven to be helpful for the cybercriminals to make cybercrimes at a greater level.

**4.2.3. Think before you share:**

Every social media user is eager to share what he/she is doing currently or has visited new places with their friends and family. So, before you share anything on the web, just make sure that you do not tag your mates and share much of the information (as of location), which may lead to unwanted issues in your life.

**4.2.4. Get accustomed to your network:**

It is very necessary to make yourself well acquainted with your friend circle and people in your network. Avoid accepting friend requests or prevent chatting with people that you don't know in real life. Most of the hackers try to get familiar with young adults who are new on social media. Once they create rapport with you, they will start asking your personal details. So, it is always recommended to stay away from such people.

**4.2.5. Avoid participating in surveys or questionnaire:**

As young people have a habit of spending a significant amount of their daily internet time on entertaining activities, they often receive messages regarding contests, winning jackpots; online quiz competition and much more. It is always recommended to stay away from such contests. Most of them will not only waste your valuable time. They will also ask you to share your personal details to claim the award. This is a very common trick followed by hackers; you should not participate in such competition unless you verify the details of the competition.

**4.2.6. Protect your location privacy:**

Young adults tend to personalize their social media profile by updating the live location from their Smartphone device. They find it quite interesting to tag images or posts with a live location displayed to the public. This can be good if they are attending an educational event or corporate conference. But in other scenarios, if you follow to avoid sharing your location details to everyone. You can customize your settings or uncheck the box while installing a new app that asks your permission to access location details.

## V. Conclusion

Social media is considered as a most lucrative and effective way to engage new users and develop communities online. However, in order to be successful with your diverse strategies on various social media platforms you need to identify, monitor and manage the risk associated in it as a part of your governance plan. Operating any of the social media channels without following preventive measures may put you into serious jeopardy. It will create harm to your personal or company image in the long term.

Social media is a want of life for everyone, without which no one can live. Every person is present on the web eagerly, and some are prone to unwanted risks and issues. The dangers can be avoided by following the simple steps mentioned above. So, simply follow the steps, stay alert from hackers and fake account users. Enjoy a social media life free from frauds.

## VI. REFERENCES

[1]. International Journal Paper Publication "A Survey on Security and Privacy Challenges in Internet of Things (IoT)." By Prof. K. Adisesha, and Prof. Praveen Moses, in International Journal of International Journal of Business and Administration Research Review (IJBARR), Vol.6, Issue.2, April-June 2019, Pg. No. 06-13, E-ISSN -2347-856X, Impact Factor- 5.494

[2]. International Journal Paper Publication "Usage of Machine Learning and Hadoop Usage in Social Media Analytics" By Prof. K. Adisesha & Prof. Praveen Moses in GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES (GJESR), volume 4 Issue 5, January 2017 Pg. No. 53 to 59, ISSN: 2348 – 8034, Impact Factor-4.022.

[3]. National Journal Paper Publication "Security Issues in Mobile Payment" By Prof. K. Adisesha in Parivriddhi: A National Reference Journal of Multidisciplinary, Volume 2, August 2016 Pg. No. 70 to 78, ISSN: 2394 – 9112.

**Cite this article as :**

Prof. K Adisesha, Dr. Lakshma Reddy, "Security and Privacy Issues in Online Social Networking", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 7, pp. 132-139, September-October 2019. Journal URL : http://ijsrcseit.com/CSEIT194724