DE JURE NEXUS LAW JOURNAL

Author:

Shradha Vats

Symbiosis Law School, Noida

2nd Year, BBA LL.B.

CYBER THREATS THROUGH SOCIAL MEDIA ACCESS

ABSTRACT

In today's world of socio-economic environment one of the fastest growing areas of technical infrastructure development is the Internet and there is no denial of this fact. The continuous increasing cyber-attacks over the past decade tend to pose a serious threat to the entire digital world. The paper focuses on the issues of cyber threats that is happening through social media access since social media adoption among individuals and even businesses is skyrocketing. The mere fact that the majority of the users are not aware of these risks and their lack of knowledge and awareness leads to further increase in cyber-crimes is a major challenge. The tremendous increase of the social networking sites has said to pave the way to connect between people and business organizations much faster than the previous era of Information Technology. In todays world social networking sites are considered to be the primary source of communication and on the other hand these sites are also the peak targets for misusing the information that it contains. Privacy and security are said to be the major concerns that has to be taken care during various online activities. Cyber security is the practice that ensures security to the user information and networks from the various unauthorized access. This paper presents the issues on cyber threats and it also discusses about the security issues through various social media access.

INTRODUCTION

The tremendous and increasing growth in the use of information technology and the continuous increasing dependence on various social networks around the world has become particularly marked in recent decades because of its great value at all the levels of professional as well as personal life, raising productivity and also solving various issues and to facilitate much easier way of life.

The interaction between human has become increasingly dependent on instant and communication that is continuous through the Internet in general and various social networking sites in particular, Further in addition to e-mail, various information exchange, e-learning, and various other applications and uses in professional and also various non-professional domains. With the increasing popularity of mobile devices and applications, combined with social networking technologies, communication using online social networking tools is now becoming a new way of life for each individual. further as a result of the continuous increasing need for managing with various information technology, threats have also tend to increase which hinder progress and it also prevent complete control over various kinfds of data and information. Various malicious programs have spread in different ways and are also evolving continuously and in rapid manner in their complexity, making it more difficult to stop their negative and often destructive effects. Data piracy has increased in the recent years at various institutional level, as well as on the level of the private user. number of users often tend to take various risks with their confedential and personal information when utilizing social networks services; for example, users are often prone to using programs that are unapproved, misusing PCs of the corporate, accessing unapproved networks, and also tend to share sensitive data on unsecured networks. In the recent years there has been a significant amount of increase in the rate of use of social networks at the global level. For example, Facebook has now officially surpassed 2.25 billion monthly active users, making the important issue of piracy of user data and the privacy of such information extremely important.

In the present era of Smartphone and computers the internet has completely changed the idea of communication. because of lack of security, number of cyber-crime cases have emerged in the past decade. Cyber security tend to play an important role in the current development of vareious information technology and services. Cyber security is therefore an attempt by users to keep their

personal and professional information intact from the attacks on the internet. The major function of cyber security is to protect various networks, computers, programs from unauthorized access and loss.cyber security is the main concern in today's world of computing. According to the report of IC3 2015 (Internet Crime Complaint Centre) an alliance between the National White Collar Crime Center and Federal Bureau of Investigation the top five countries by count in complaints of the victims as numbered by Rank are as follows. -United States-United Kingdom-Nigeria-China-India.

SOCIAL NETWORKING SITES

Various Social network sites are the main platform for different people to connect and share the required and relevant information. Social network sites are online community where different can create individual public profiles, interact with their friends, business clients and also connect with any number of people based on their interests. The different functionality of each social networking site may differ but all such site pushes user to provide their personal information and then also allows user to communicate through e-mails, instant messaging and various other such mediums. The basic step in every social network involves is to create a public profile which may include the unsers private and can also contain sensitive information's such as a the users photo, personal information (name, age, sex, dob) and some more additional information's like what are their favorite shows, movies, places, hobbies. Each and every social network operates with different scenarios and communication methods also vary. Some of the most popular social network sites include Facebook, Twitter, LinkedIn and instagram. majority of the online users will essentially have an account in the above mentioned social networking sites.Various Online activities in social network includes simple chat and call, watch videos, listening to music, online gaming, publishing and also posting contents and it is also used for various educational and business purpose. Security is reciprocation. [1]

The more the user tend to isolate from their social network account, limit content from appearing on profile page, and restrict people from accessing photos and other sensitive content the less there is chance of vulnerabilities. The core or the main objective of cyber security is to protect

[11] Available at-Threats of online social Network.
Available at-social networking sites.

information from various unauthorized access.

Cyber security tend to provide confidentiality, integrity and availability for authorized informations, various business users. Cyber security also offers protection of the users system against viruses, spywares, hacking, cracking and most importantly offers privacy to the users.

TYPICAL SECURITY ISSUES IN SOCIAL MEDIA SITES

Online activities of user in any social media site will contain the. user generated information and user's personal information such as private data, photos and basic information such as (name, place, location). The challenging task for any social network user is maintaining the social identity while risking the social privacy. It is estimated that in 2020, number of social networking site users may reach 3 billion which is one third of entire population. Malicious users gain access to the user's private information and other useful information from social networking sites via unauthorized access and initiate attacks. the users which are unauthorized with the knowledge gained from various social networking sites may perform unwanted and even criminal activities like hacking, spoofing, phishing etc risks the privacy and security of online social network users since user's information are disclosed. Social Networking sites security and privacy issues are basically not a technologically issue it is completely due to user behavior. The more the user tend to disclose the personal information the more there is chance of security threat. Posting sensitive and confidential content may encourage higher risk of vulnerabilities and those contents are viewed by vast set of audience which may attract malicious users to loophole and gain access to the private account or network. Threats keep changing, so security must evolve and overlook them. Even with rightly configured

Various Attacks in Social Networks

1.Identity Theft - Various Unauthorized users attack through the application in which they seek permission for accessing the information provided in the profile of social networking sites. When a user allows to do so, they tend to get all the information and can misuse that without the user knowledge which can be extremely dangerous.

2.Phishing - This cyber-attack also tend to use e-mails and different websites to track the user information. Sensitive information's like credit card numbers and passwords are targeted by

disgusting the e-mails. Phishing ends up in issues like unauthorized purchases, identity theft, looting money. In a business scenario [2]phishing may also end up in some adverse effects such as dropping of market share, customers trust, and reputation

3.Hacking - It is an unauthorized access to control computer system, a network. Hacking is always not unethical.The Black hat hackers are experts of computer who perform hacking for the purpose of personal gain whereas Grey hat hackers intimate the loopholes in the network to the admin of that particular network.

4.Spoofing -Malicious users also get into account of user or system by masquerading as a trusted entity. This involves email spoofing, IP spoofing. Email Spoofing is said to involve requesting private sensitive data, financial information via e-mails froma trusted sender. Spoofing e-mails can also tend to carry trojan and other malwares. IP spoofing mainly targets the entire network. Malicious users pick up these IP address and then they modify the packet headers forwarded from their own system to disguise as an original entity.

5.Spam - Spam tend to utilize social networks and also tend to spoil the network this even includesdifferent advertising or inserting malicious code and even collecting sensitive and private information's in the social network sites, earlier spam tend to target only e-mails. However nowadays it include Instant Messaging spam, Forum and comment spam, Mobile phone spam.

6.Virus - here Any malicious software designed to access the user system. Viruses tend to replicate when the software or even the file is shared across the network. Viruses may also infect the resources of the system, software, change applications and primary functions of the system,

7.Worm - Malicious code that often tend to replicates itself and then they dispatch to the entire network. These worms may come as attachment in spam e-mails or even instant messages. Worms may also change and corrupt files of the users and may also inject malicious code. Also these worms overload the shared network and occupy the space of the hatrd drive.

8.Password Sniffing - The malicious code that tend to explore network traffic to track the users usernames and passwords. Many encryption standards are especially set for the various protocols

[2] Available at-Cyber crime reports.

to avoid these types of dangerous attacks.

9.Key logger - Key logger can be hardware or software which tracks and records the keystrokes and also finds passwords, banking, business and credit information. Operating system based keylogger is difficult to detect and is often considered more harmful.

CONCLUSION

In today's digitalized era disclosure of user private information, business information and other sensitive contents are strikingly and continuously increasing in social networking websites. Though cyber security experts keeps on update and also evolve the various security features for social media accounts and even with the advancement of the technology alarmingly security threats and vulnerabilities are rapidly increasing. In addition to,attacks towards social networking sites usually tend to extend much faster than any other types of attacks that are online. In this paper we reviewed the common threats in social media access. Other than the use of automated tools for the monitoring of security threats there are other simple ways to reduce the various social networking attacks i.e educating and making the online users aware on how much to expose on public network and also how to make the best use of the various available privacy settings. Cyber security policies guides us to stay away from various security threats in social networking sites.

As there is a growing popularity of the Social Networking Sites these have become a prime and a major target for various cyber-crimes and attacks. Cyber-crime is becoming a widespread and posing a major threat to the national and and also economic security. public and private institutions both in sectors of public health, information and telecommunication, defense, banking and even finance are at risk. Thus the organizations must take proper security measures to be cyber-crime safe and also the users should protect their personal information[3] to avoid and identity theft or misuse. The cyberspace is even becoming a major and a significant area for various cyber-crimes and attack of terrorist on crucial and sensitive information. So, there is an urgent need of universal collaboration of nations to come and work together to reduce the constantly growing cyber threat.

[3] Available at-Cyber security policy.