PRIVACY OF USERS AND OF SOCIAL NETWORKING SITES

Sandhya Kumari[1].

Assistant Professor, Department of I.T

L.N. Mishra College of Business Management, Muzaffarpur[1]

Dr. Vijay Kumar Singh[2]

Assistant Professor, Department of I.T

L.N. Mishra College of Business Management, Muzaffarpur[2]

Abstract:

Social Networking Sites are the part of life style of people today. The Social Networking Sites provide the wider range of services mostly for free. The users of these sites are from all age group. Many of the users are not aware of the data thefts, they freely share the information. Thus all major issues in Social networking sites need to addressed by the social networking Sites.

In this paper we focus on the study on the different ways of personally identifiable information leakages. This study is an overview on privacy in social networking sites. We try to aware the users of social networking sites, and try to find the new methods of privacy on the social networking sites, that will definitely help in raising user awareness about sharing data and managing their privacy with SNSs. It will also help Social Networking Sites providers to rethink about their privacy policies.

Key Word: Social Networking Sites, Privacy, Personally Identifiable Information, Leakage, SNS, Privacy Related Threats.

Introduction:

Social Media: Internet-based software and interfaces that allow persons to interact with one another. It is an exciting platform to exchange details about one's lives such as biographical data, professional information, personal photos and up-to-the-minute thoughts.

Social media originated as strictly a personal tool that people used to interact with friends and family but were later adopted by businesses that wanted to take advantage of a popular new communication method to reach out to customers.

social network sites (SNSs) such as MySpace, Facebook, Twitter, Cyworld, and Bebo have attracted millions of users, many of whom have integrated these sites into their daily practices.

Social network sites may defined as web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system. Most sites support the maintenance of preexisting social networks, but others help strangers connect based on shared interests, political views, or activities. Some sites cater to diverse audiences, while others attract people based on common language or shared racial, sexual, religious, or nationality based identities.

History of Social Networking Sites:

A Social media are the medium to share the information. The sharing of information is used by the human being from when they develop the society. In early days they used the letters for communication.

In 1792, the telegraph was invented. This allowed messages to be delivered over a long distance far faster than a horse and rider could carry them.

Two important discoveries happened in the last decade of the 1800s: The telephone in 1890 and the radio in 1891. Both technologies are still in use today, although the modern versions are much more sophisticated than their predecessors. In 1969, ARPANET, created by Advanced Research Projects Agency (ARPA), a U.S. government agency, was developed. ARPANET was an “early network of time-sharing computers that formed the basis of the internet.” . In 2004, Mark Zuckerberg launched what would soon become the social media giant that would set the bar for all other social media services. Facebook is the number one social media website today and it currently boasts over a billion users. In

2006, the popularity of text messaging or SMS inspired Jack Dorsey, Biz Stone, Noah Glass and Evan Williams to create Twitter. Flickr was one of the earliest and still is one of the most popular photo sharing sites, but others include Photo bucket and Instagram, with Instagram gaining popularity today as one of the top social media sites to include on business cards and other media. Tumblr, a microblogging website started in 2007.

Privacy threats on Social media : Privacy of users on social media is a big threat today. If we take a reference of India every sixth cybercrime in India is committed through social media, according to the National Investigation Agency (NIA). The National Crime Records Bureau (NCRB) show around 70% rise in cybercrimes annually between 2013 and 2015. The number of cybercrime cases reported across India in 2014 was a little more than 9,600, a mere fraction of the estimated three lakh theft cases (that year). But the concern is an annual growth of 70% for the last three years," .Now in India "Lottery and job scams are rampant. It has taken the form of organized crime in India".

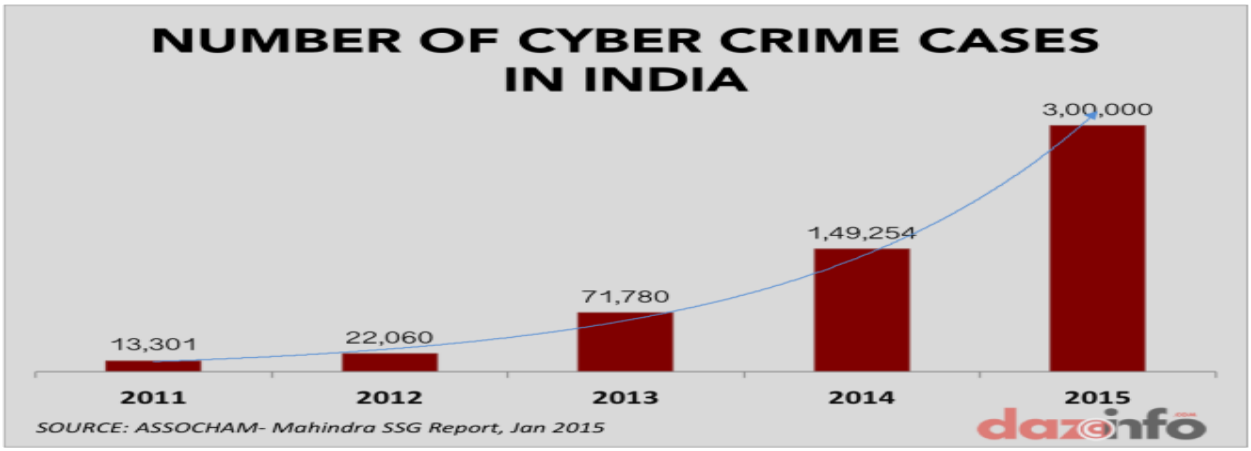

Fig. 1

Organised financial crime was a feature of east European and former USSR countries. But with high internet user density and inadequate knowledge of net users, various cities in India are also becoming locations for perpetrating such crimes. Noida has turned into a hub of cyber attacks in the national capital region.

With 780 cases of cybercrime reported in 2015, Noida saw the setting up of the Centre for Cyber Crime Investigation in 2016.

Most social networks allow applications to have a wide variety of access to user data through different interfaces. Some provide documented APIs that allow specific access to pieces of information. This can also include granular access on a permission basis so that the user can decide which access to grant to the application. Depending on its type, the application can be anchored deep within the social network and melded within the user interface. Alternatively, it could just interact on a loose level, displaying some partial information on a different website. As an example, Facebook has two basic application types. First, there are social plug-ins, which allow the integration of basic Facebook features onto any website. Canvas applications, which do interact with the profile, can send update messages or open a new page, which in turn can contain nearly anything. The "Like" button that allows people to inform others about the existence of a page is an example of a social plug-in.21 The other applications can, to some extent, load code from remote websites and execute it.

Fig. 2.0

Cyber Crimes against Persons:

There are certain offences which affects the personality of individuals can be defined as:

- Harassment via E-Mails: It is very common type of harassment through sending letters, attachments of files & folders i.e. via e-mails. At present harassment is common as usage of social sites i.e. Facebook, Twitter etc. increasing day by day.

- **Cyber-Stalking:** It means expressed or implied a physical threat that creates fear through the use to computer technology such as internet, e-mail, phones, text messages, webcam, websites or videos.
- **Dissemination of Obscene Material:** It includes Indecent exposure/ Pornography (basically child pornography), hosting of web site containing these prohibited materials. These obscene matters may cause harm to the mind of the adolescent and tend to deprave or corrupt their mind.
- **Defamation:** It is an act of imputing any person with intent to lower down the dignity of the person by hacking his mail account and sending some mails with using vulgar language to unknown persons mail account.
- **Hacking:** It means unauthorized control/access over computer system and act of hacking completely destroys the whole data as well as computer programmes. Hackers usually hacks telecommunication and mobile network.
- **Cracking:** It is amongst the gravest cyber crimes known till date. It is a dreadful feeling to know that a stranger has broken into your computer systems without your knowledge and consent and has tampered with precious confidential data and information.
- **E-Mail Spoofing:** A spoofed e-mail may be said to be one, which misrepresents its origin. It shows it's origin to be different from which actually it originates.
- **SMS Spoofing:** Spoofing is a blocking through spam which means the unwanted uninvited messages. Here a offender steals identity of another in the form of mobile phone number and sending SMS via internet and receiver gets the SMS from the mobile phone number of the victim. It is very serious cyber crime against any individual.
- **Carding:** It means false ATM cards i.e. Debit and Credit cards used by criminals for their monetary benefits through withdrawing money from the victim's bank account mala-fidely. There is always unauthorized use of ATM cards in this type of cyber crimes.
- **Cheating & Fraud:** It means the person who is doing the act of cyber crime i.e. stealing password and data storage has done it with having guilty mind which leads to fraud and cheating.
- **Child Pornography:** It involves the use of computer networks to create, distribute, or access materials that sexually exploit underage children.
- **Assault by Threat:** refers to threatening a person with fear for their lives or lives of their families through the use of a computer network i.e. E-mail, videos or phones.

Crimes Against Persons Property:

As there is rapid growth in the international trade where businesses and consumers are increasingly using computers to create, transmit and to store information in the electronic form instead of traditional paper documents. There are certain offences which affects persons property which are as follows:

- **Intellectual Property Crimes:** Intellectual property consists of a bundle of rights. Any unlawful act by which the owner is deprived completely or partially of his rights is an offence. The common form of IPR violation may be said to be software piracy, infringement of copyright, trademark, patents, designs and service mark violation, theft of computer source code, etc.
- **Cyber Squatting:** It means where two persons claim for the same Domain Name either by claiming that they had registered the name first on by right of using it before the other or using something similar to that previously. For example two similar names i.e. www.yahoo.com and www.yaahoo.com.
- **Cyber Vandalism:** Vandalism means deliberately destroying or damaging property of another. Thus cyber vandalism means destroying or damaging the data when a network service is stopped or disrupted. It may include within its purview any kind of physical harm done to the computer of any person. These acts may take the form of the theft of a computer, some part of a computer or a peripheral attached to the computer.
- **Hacking Computer System:** Hacktivism attacks those included Famous Twitter, blogging platform by unauthorized access/control over the computer. Due to the hacking activity there will be loss of data as well as computer. Also research especially indicates that those attacks were not mainly intended for financial gain too and to diminish the reputation of particular person or company.
- **Transmitting Virus:** Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worm attacks plays major role in affecting the computerize system of the individuals.
- **Cyber Trespass:** It means to access someone's computer without the right authorization of the owner and does not disturb, alter, misuse, or damage data or system by using wireless internet connection.
- **Internet Time Thefts:** Basically, Internet time theft comes under hacking. It is the use by an unauthorised person, of the Internet hours paid for by another person. The person who gets access to someone else's ISP user ID and password, either by hacking or by gaining access to it by illegal means,

uses it to access the Internet without the other person's knowledge. You can identify time theft if your Internet time has to be recharged often, despite infrequent usage.

3. **Cybercrimes Against Government:**

There are certain offences done by group of persons intending to threaten the international governments by using internet facilities. It includes:

- **Cyber Terrorism:** Cyber terrorism is a major burning issue in the domestic as well as global concern. The common form of these terrorist attacks on the Internet is by distributed denial of service attacks, hate websites and hate e-mails, attacks on sensitive computer networks etc. Cyber terrorism activities endanger the sovereignty and integrity of the nation.
- **Cyber Warfare:** It refers to politically motivated hacking to conduct sabotage and espionage. It is a form of information warfare sometimes seen as analogous to conventional warfare although this analogy is controversial for both its accuracy and its political motivation.
- **Distribution of pirated software:** It means distributing pirated software from one computer to another intending to destroy the data and official records of the government.
- **Possession of Unauthorized Information:** It is very easy to access any information by the terrorists with the aid of internet and to possess that information for political, religious, social, ideological objectives.

4. Cybercrimes Against Society at large:

An unlawful act done with the intention of causing harm to the cyberspace will affect large number of persons. These offences includes:

- **Child Pornography:** It involves the use of computer networks to create, distribute, or access materials that sexually exploit underage children. It also includes activities concerning indecent exposure and obscenity.
- **Cyber Trafficking:** It may be trafficking in drugs, human beings, arms weapons etc. which affects large number of persons. Trafficking in the cyberspace is also a gravest crime.
- **Online Gambling:** Online fraud and cheating is one of the most lucrative businesses that are growing today in the cyber space. There are many cases that have come to light are those pertaining to credit card crimes, contractual crimes, offering jobs, etc.

- **Financial Crimes:** This type of offence is common as there is rapid growth in the users of networking sites and phone networking where culprit will try to attack by sending bogus mails or messages through internet. Ex: Using credit cards by obtaining password illegally.
- **Forgery:** It means to deceive large number of persons by sending threatening mails as online business transactions are becoming the habitual need of today's life style.

Preventive Measures For Cyber Crimes:

Prevention is always better than cure.

Identification of exposures through education will assist responsible companies and firms to meet these challenges.

- Avoid disclosing any personal information to strangers via e-mail or while chatting.
- Must avoid sending any photograph to strangers by online as misusing of photograph incidents increasing day by day.
- An update Anti-virus software to guard against virus attacks should be used by all the netizens and should also keep back up volumes so that one may not suffer data loss in case of virus contamination.
- A person should never send his credit card number to any site that is not secured, to guard against frauds.
- It is always the parents who have to keep a watch on the sites that your children are accessing, to prevent any kind of harassment or depravation in children.
- Web site owners should watch traffic and check any irregularity on the site. It is the responsibility of the web site owners to adopt some policy for preventing cyber crimes as number of internet users are growing day by day.
- Web servers running public sites must be physically separately protected from internal corporate network.
- It is better to use a security programmes by the body corporate to control information on sites.
- Strict statutory laws need to be passed by the Legislatures keeping in mind the interest of netizens.
- IT department should pass certain guidelines and notifications for the protection of computer system and should also bring out with some more strict laws to breakdown the criminal activities relating to cyberspace.
- As Cyber Crime is the major threat to all the countries worldwide, certain steps should be taken at the international level for preventing the cybercrime.

- A complete justice must be provided to the victims of cyber crimes by way of compensatory remedy and offenders to be punished with highest type of punishment so that it will anticipate the criminals of cyber crime.

Conclusion:

Social networking communities are an inherent part of today's Internet. People love using them to stay in contact with friends, exchange pictures, or just to pass the time when bored. Companies have also discovered social media as a new way of targeting their customers with relevant information. With user groups with hundreds of millions of members, there are always some black sheep with malicious intent. We have seen many worms spread through social networks. In most cases they have used social engineering tricks to post enticing messages on behalf of an infected user. Curious friends who follow the link will also get infected with malware and unwillingly spread the message further. Unfortunately many people will click on nearly any link that they see posted and add anybody to their private network that asks, without knowing who really is behind it. This inherent trust, especially in messages coming from friends that have had their account compromised, makes it easy for attacks to succeed, regardless if it is a phishing attack, a spam run, or a malicious worm spreading through automated scripts.

References

1. https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_risks_of_social_networking.pdf
2. https://www.legalindia.com/cyber-crimes-and-the-law/
3. Sharma Mayank , Elgg Social Networking (From Technologies to Solutions)
4. Robert Siciliano Social Media Privacy and Personal Security Issues
5. Mahadi Anjum,"Internal Security of India Challenges, Threats and Remedial Measures" Jawahar Publisher.
6. Lohit Matani, "Internal Security Concepts. Dynamics. Challenges (2017) " Knowracle Publications; Latest Edition edition (2016)

****