Asian Journal of Managerial Science
ISSN: 2249-6300 Vol. 6 No.2, 2017, pp.42-49

Threats to Security and Privacy of Information Due to Growing Use of Social Media in India

Amishi Arora[1] and Amlesh Mendhekar[2]
[1]Principal, [2]Research Scholar
Central Institute of Business Management Research and Development
Nagpur, India
E-Mail: aroraamishi@yahoo.com

Abstract - **The world is witnessing a rapid rise in the use of Internet by people. With the advancement of technology and increased use of mobile phones/smart phones, people are able to access internet virtually from any part of the globe. Social media is now a very popular means of communication on the internet. The basic idea behind social media concept was to create platform which is user-driven, interactive Web in order to 'bring people closer'.**

In this paper, an attempt has been made to provide an overview of dangers posed by social media platforms to the information security and data privacy of the people. Cybercriminals are using social media platforms to carry out their illegal activities. A large number of people are falling easy prey to cybercriminals everyday on social networking sites. This paper explores the different types of threats which may compromise information security and privacy of people especially the youngsters due to their increased use of social networking platforms. As India has one of the fastest growing social media user base in the world, this paper also explores the various security measures that can be undertaken to become less vulnerable to the threats posed by cybercriminals on social media.

Keywords: **Security and Privacy of Information, Social Media**

I. INTRODUCTION

The twenty first century has seen a lot of new advancement and innovations in the field of telecommunications. Gone are the days when people were mostly dependent on fixed line phones to communicate with one another. Nowadays people mostly prefer using mobile/smart phones and internet for communication. In-fact internet has changed the way people communicate globally. With drop in the prices of smart phones and also the telecom companies offering data/internet access at a very low prices, more and more people now getting connected to internet. Apart from these factors one of the biggest driving factor behind people getting connected to internet is the popularity of social networking sites like Facebook, Twitter and others.

There are millions of people active on social media platforms at any given point of time. Thus cybercriminals are focusing more on social networking sites as they provide virtually correct data to choose and compromise their targets. The risks of using social networking sites are also getting higher by the day as the cybercriminals are devising new methodologies to compromise users. It is therefore necessary to understand the depth of this problem and identify ways and means to minimize the probable dangers to privacy and security of our data.

II. SOCIAL MEDIA

Merriam-Webster dictionary defines Social Media as "forms of electronic communication (as websites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages, and other content (as videos)". In other words social media provides a platform for users to participate in social networking, creating and sharing content using variety of websites and applications. One of the major advantage of social media is that it allows users to communicate with others beyond social or local boundaries. The two key areas of revenue for social media are social advertising and social games.

Some of the common social activities performed by people on social media platforms are:

1.Social Networking

Social networking allows people to make new friends, brings people together where they can interact and share information like their interests, photos, videos, updates, and any other activities. Facebook is one of the most popular social networking site today having more than 1 billion users.

2.Blogging

Blogging is expressing yourself to the world via online personal diary or journal which is called as a blog. The name blog is derived from the term 'web log', is a type of website where the user writes entries or post on which the other users can comment. Blogs needs to be updated frequently to keep the readers engaged. Blogger is one of the most popular blogging site.

3.Micro-blogging and Tweeting

Micro-blogging is a web service that allows the users to post or broadcast short messages to other users of the

service. Twitter is one of the most popular micro-blogging platform in the world. Twitter allows a user to post updates also called as tweets of 140 characters or less. The term tweeting was thus derived meaning frequently posting new updates.

4.Photo Sharing

Photo sharing allows users to upload and share their photos with others. The users can also like or comment on the photos. Instagram is one of the popular photo sharing site.

5.Video Sharing

Similar to photo sharing sites the video sharing sites allows users to share their favorite or homemade videos online. The other users can watch the videos online and can comment or share those videos in their network with other users. YouTube is the most popular video sharing site.

6.File Sharing

File sharing sites allows users to upload files like documents on the online portal which can be shared with other users who in turn can download those files. SlideShare is one such site which allows users to share files mostly the presentations.

7.Instant Messaging

Instant messaging, or simply "IM" is the real time exchange of text messages using a software application. WhatsApp is one the most popular Instant Messaging application for smartphones and desktops.

Some of the most popular social media platforms includes:

1.Facebook

Facebook is the most popular free social networking site which allows its registered members to keep in touch with friends, family and office colleagues. The registered users create their profiles, and can send messages, upload and share photos and video to the other users. Currently there are about 1,871 million active Facebook users worldwide. [1]

2.Twitter

Twitter is one of the most popular micro-blogging site in the world. It allows its registered members to broadcast short messages also known as tweets of up to 140 characters to the other members. Tweeter users may use hashtags to mention or link to other Tweeter users or any other online resources such as videos, photos or webpages. Members use multiple platforms and devices to follow other user's tweets. There are around 317 million registered members of Tweeter worldwide. [1]

3.WhatsApp

WhatsApp is a free instant messaging (IM) software for smartphones which runs on multiple platforms. Users once registered on the application can send messages, share their statuses, photos, videos, documents, location with other registered users. WhatsApp also allows users to make voice and video calls to other users. WhatsApp has more than 1billion users worldwide making it one of the most popular IM application.

4.LinkedIn

LinkedIn is a social networking site designed specifically for professionals. The goal of the site is to allow users to promote themselves and their businesses by making connections with other professionals. The users can send messages to other users, interact in group discussions, apply for jobs, post job openings, publish articles and share content. There are around 106 million active users of LinkedIn worldwide. [1]

5.Instagram

Instagram is a social networking application for sharing real time photos and short videos. It is one the most popular photo sharing media platform that the mobile web has ever seen. There are about 600 million active users of Instagram worldwide.

6.Wikipedia

Wikipedia is a free, open content online encyclopedia that aims to allow anyone to create, publish and edit articles in a collaborative method. The community members are the users registered on the site and are also known as 'Wikipedians'. There are 18 billion average number of monthly page views of Wikipedia. [2]

7.YouTube

YouTube is the largest and most popular video-based social media website which features a wide variety of movie clips, music videos, video blogs, educational videos and short. YouTube content is free to view and the content is mostly generated by users and corporates. YouTube has more than 1 billion active users worldwide. [1]

8.Snapchat

Snapchat is a mobile image messaging, instant messaging, video chat and multimedia sharing application software product. It is one of the most popular social media site among teenagers and young adults. There are more than 300 million Snapchat active users around the world.

9.Google+

Google+ (pronounces as Google plus) which is owned and operated by Google is an interest-based social network. It was designed to replicate the way people interact offline more closely compared to other social networking services. Presently there are about 120 million active users on Google+ worldwide.

III. INTERNET AND SOCIAL MEDIA USERS: SOME STATISTICS

The exponential growth in usage of mobile devices and smart phones along with increased Internet penetration has increased social media user base proportionately. A lot of social media apps have been developed for mobile devices and smart phones. According to statistics accessing social media has become one of the most popular activity for many people worldwide.

A.Internet Users Worldwide

The current world population is 7.5 billion as per the United Nations population data. The estimated Internet users worldwide are 3.6 billion, which is around 49.2 percent of the overall population. The number of Internet users in Asia is 1.8 billion with the penetration rate of 44.7 percent of the overall population. [3]

B.Internet Users in India

The current population of India is around 1.2 billion and the number of Internet users are 462 million, which is around 36.5 percent of the population of the country. The country has seen a 9,142.5 percent exponential growth of internet users since year 2000 [4][5]. The figures indicate that presently, one third of Indian population has access to internet and which growing exponentially at the rate of 30.5% annually (from year 2015 to 2016). This figure is projected to grow to 635.8 million internet users in 2021. Despite the untapped potential, India already is the second-largest online market worldwide. A large number of internet users in India are in the age group 15-24 years [6]. Around 75 percent of the rural internet users in India belong to the age group of 18-30 years and another 11 percent are in the age group of <18 years of age. [7]

C.Social Media Users Worldwide

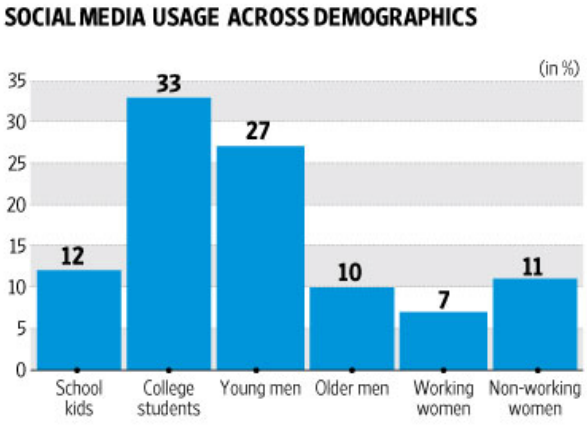
The social media penetration worldwide is growing at a very rapid pace. Currently there are more than 2.34 million media users worldwide, which means around 65 percent of internet users are social media users and these figures are expected to grow in the coming years. The number of social media users is estimated to reach 2.95 billion by the end of year 2020. [8]

D.Social Media Users in India

India has presently around 292 million social media users, The social media user base in India is ever-increasing and it is expected that by year 2021 there will be around 467.9 million social media users which will be second only to China. [9]

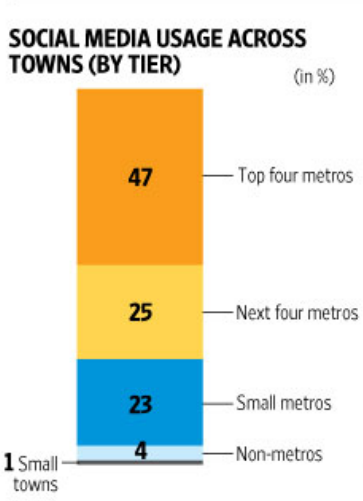
For many Indians users the primary reason to access internet is for accessing the social media networks. As per the report by the Internet and Mobile Association of India (IAMAI), as many as 66% of the 180 million Internet users in urban India regularly access social media platforms. While college students (33%) form the largest demographic of active social media users in India. The most popular activities on social media include maintaining one's own virtual profile on the likes of Facebook and Twitter, posting and sharing an update as well as replying to something a friend has posted. [5] [10]

At the end of 2016, Facebook and YouTube were the most popular social networking sites in India with a 33 percent penetration rate each closely followed by 28 percent reach of WhatsApp. [11]



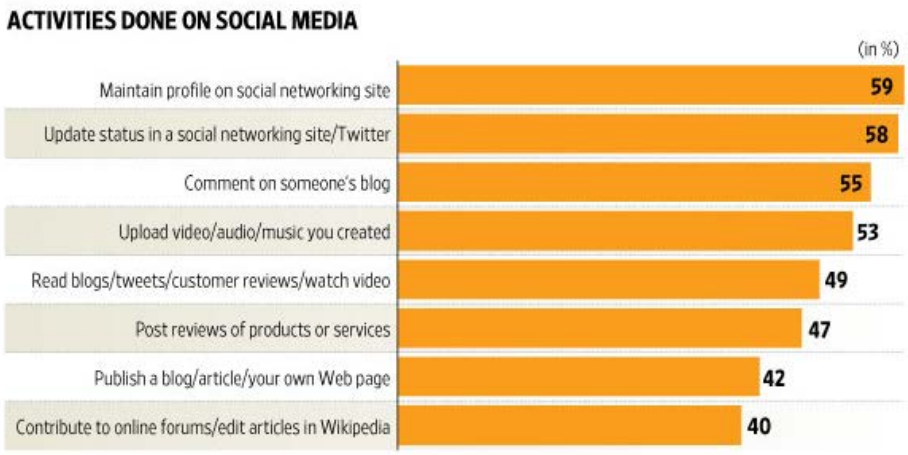
Source: IAMAI

Fig.1 Social Media Usage Across Demographics



Source: IAMAI

Fig.2 Social Media Usage Across Towns



Source: IAMAI

Fig.3 Activities done on social media

IV.UNDERSTANDING INFORMATION SECURITY AND PRIVACY

Information Security is the practice of defending information and information assets from unauthorized access, use, modification, disclosure, disruption, inspection, perusal, inspection, recording or destruction in order to provide confidentiality, integrity and availability. The concept of privacy is depends on one of the core concept of security i.e. confidentiality. Privacy can be defined as confidentiality of the personal information. Meriam-Webster defines privacy as the freedom from unauthorized intrusion. Many countries have developed and enacted special laws for the protection of privacy of individuals against the possible breach by government, corporates and individuals.

Personal information is any piece of information that relates to a living, identifiable human being. It is also referred to as Personally Identifiable Information (PII) or Sensitive Personal Information (SPI). As per National Institute of Standards and Technology (NIST) the following are examples of types of information/data falls under PII [12]

1. Full name
2. Residential address
3. Email address
4. Passport number
5. Mobile/Telephone number
6. Driving license number
7. Date of birth
8. Place of birth
9. Credit card number
10. Genetic information
11. Face, fingerprints, or handwriting
12. Login name, nickname

Apart from the above mentioned types of information the European Union (EU) Privacy Rules define 'sensitive personal data or information' to include the following information relating to: [13]

1. Password
2. Financial information e.g. bank account/credit or debit card or other payment instrument details
3. Physical, physiological and mental health condition
4. Sexual orientation
5. Medical records and history
6. Biometric information
7. Any detail relating to the above clauses as provided to a corporate entity for providing services, and
8. Any of the information received under the above clauses for storing or processing under lawful contract or otherwise

Privacy concerns exist wherever uniquely identifiable data relating to a person or persons are collected and stored, in digital form or otherwise. With the advancement of digital technology the threats and vulnerabilities of personal data is also increasing. Privacy issues mostly arise due to improper or insufficient safeguards on PII or SPI.

A. Threats of Social Media on information security and privacy

There are lot of people who share photos of their new driving license, office or college ID, house number, mobile phone number, new vehicle with number/license plate. Even we have seen many users in India posting photo of their new Aadhaar card (Unique ID or UID by Govt. of India for its citizens) on Facebook and other social networks. All these posts leads to information exposure and also help cybercriminals to steal the privacy information and carry out Identity theft. Geo tagging in photos and videos is one more type of information which the attacker is of attacker's interest. Some of the common types of threats due to social media are:

*1.Social Engineering***:** Social engineering is psychological manipulation of people in revealing sensitive and

confidential information. It is a means of gathering information from individuals by taking advantage of their weaknesses. The attackers make use of social media to carry out social engineering attacks. Some of the types of social engineering attacks includes phishing, impersonation, baiting, etc.

2.Identity Theft: Identity theft involves stealing someone else's identity and committing a fraud. As many users' exposes lot of their personal information on various social media sites, they fell easy prey to identity theft.

3.Online Predators: Online Predators are people who use Internet and social media to target, locate and exploit vulnerable children of all ages for sexual or other abusive purposes.

4.Cyberbullying: Cyberbullying is the use of the social media platforms to harass, bully, threaten, intimidate, or embarrass a young person (a child, preteen or teen) by other young person/s. When an adult is involved in bullying it is termed as cyber-harassment or cyberstalking.

5.Phishing: Phishing is a kind of social engineering attack in which the attacker communicates with victim by disguising as a trustworthy person or organization to solicit their personal information. In this type of attack the victims are tricked to reveal their personal, financial or business or installing malware on their devices.

6.Terrorism: Terrorists are increasingly using social media platforms to spread their ideology, recruiting young people and spreading fear among the masses.

7.Spam: Spamming is sending unwanted and irrelevant messages over the Internet to many users mostly for spreading malware, phishing and advertisements.

8.Malware: Malware or malicious software is used by cybercriminals on social media to infect users' devices to extract confidential and sensitive information of the users.

9.Ransomware: Ransomware also called as 'Rougeware or Scareware" is a type of malware created by scammers which restricts/prevents access to your computer system or your personal files and demands a ransom payment (in form of money, Bitcoins, etc.) in order to regain access. Mostly ransomware is aimed at individuals but nowadays businesses are targeted as well.

10.Internet scams and frauds: Internet scams and frauds (also known as online scams or cyber frauds) refers to using Internet and social media to conduct fraudulent activities in order to scam or take advantage of people. Examples includes lottery scams, Nigerian scam, phishing scams, etc.

11.Website Compromise: Attackers compromise or hack social media sites or applications by taking advantage of vulnerabilities in their software in order to steal user database or user credentials.

12.Clickjacking: Clickjacking (or clickjack attack) is a malicious technique used by the attacker to trick a web user into clicking something different from what they intended to click. The purpose of the attack is to record infected user's clicks on the internet, install malicious content, or to capture sensitive user information like passwords.

13.Social bots: A socialbot or socbot is an automated software program intended to mimic human behavior on social media sites in order to interact with other users, generate messages, supports campaigns, or follow users to collect their personal data.

14.Fake Profiles: Fake profiles are created by attackers to deceive other users on social media sites. Fake profiles can be manual or automated (social bot). A very common example is fake profiles of celebrities on social media sites.

*15.Information leakage***:** Social media users intentionally or un-intentionally share a lot of their personal and sensitive information with others on the network which can be misused by malicious people on the network.

16.Location leakage: Users use geotagging feature to willingly share their location information with their friends and others on social media which may be used by cybercriminals to carry out attack.

17.Inference Attacks: Inference attacks uses data mining techniques on the user's publicly available data on social media to predict his/her personal sensitive information like political view, sexual preference, health issue or religious affiliation.

18.Reconnaissance: Reconnaissance is an act of gathering information on the social media sites about the target (an individual or a company), which may help the attacker to compromise or exploit the target later.

19.Trolling: Trolling or Internet troll means intentionally frustrate or anger someone on the Internet or social media platforms in order to provoke an emotional response.

V.CYBERCRIMES USING SOCIAL MEDIA – A GLOBAL PHENOMENON

Facebook and Twitter alone ontributes to around 81 percent of cybercrimes involving social networking sit. Cybercriminals find these platforms ideal sources for obtaining personal information from unsuspecting people. [14]

A large number of active social media users are youngsters who access the social media platforms using their mobile phones. The Pew Research Center survey on Teens, Social Media, and Privacy indicates that teens are sharing more

information about themselves on social media sites than they did in the past. Teen social media users do not express a high level of concern about third-party access to their data. The information they share on social networking sites might be accessed by third parties like advertisers or businesses without their knowledge. [15]

Most people access Facebook on their mobile phone and for the sake of convenience they do not use user and password option which is a part of the app. In case if the mobile gets stolen, lost or misplaced any person with criminal intent can access the user's Facebook and other social media accounts and can also post some offensive and misleading message. Also, there are chances of exposing the user's other social media platforms if the user has linked his Facebook account login for logging into other apps.

Location tracking is a new security threat which is emerging on social media networks. Location tracking feature allows your friends to know your GPS location and if the privacy settings are not configured properly on the app it can lead to privacy breach as well.

Sometimes simple status information, a message or update can become a serious security threat on social media. When a user posts about his forthcoming vacation tour or his travel like Facebook's 'check-in' feature, he might disclose this information to everyone viewing his profile. This may give some opportunity to break in to the user's house or rob them.

Social media platform has also become useful for criminals, sex offenders, burglars and other crooks. For instance, Google Street View allows these malicious people to study the victim's properties over the internet prior to committing the actual crime. 78 percent of burglars admit that they use social media to seek out their victims. Disabling the geotagging function on the mobile phone while using the social networking apps may prevent lot of crimes. [14]

Social media provides a good platform for reconnaissance if someone wants to target an individual or a company. A lot of information is available on social media like who works in which company, roles of individuals in that company, professional and personal friends, location and other contact information. Any individual who has published a lot of private information which is publicly available on their profiles becomes an easier target of cybercriminals. [16]

Cybercriminals not only steal the information on social media, they also use it to sell the compromised data. As per Gabriel Guzman, head of cyber intelligence at RSA, the security division of tech firm EMC "Anybody is just two clicks away from finding compromised financial data in social media" [16]

Social media is one of the major platform for malware distribution. According to the technology giant Cisco, the most common malware distributed in the year 2015 was Facebook scams. PricewaterhouseCoopers (PWC) found that more than one in eight enterprises were victims of social media related cyber-attacks.

The social media networks sites are themselves not fully secured to protect their own data. As Facebook reported in the year 2015, 31 million accounts on its platform were fake. Other sites like LinkedIn and Twitter also admitted the presence of fake accounts on their networks. [18]

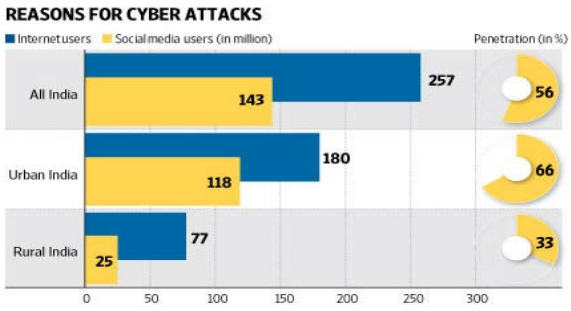
There is a large percentage of young population is active on the social media. On the Facebook alone there are large number of users who are under the age of 10 years and around 40 percent users are under the age of 13 years, which is the minimum age requirement for most of the social networking sites. Most of these minors use social networks without their parents' knowledge and supervision. They become easy targets for the predators as they share a lot of personal and sensitive information such as their photos, place of residence, real age, school they attend, etc. Around 33 percent of all the internet initiated sex crimes are carried out using the social networking sites. In-fact 50 percent of sex crimes committed against minors involve the perpetrator obtaining personal information and photos from the profile of the victim on the social media. [14]

VI.IMPACT OF SOCIAL MEDIA RELATED CYBERCRIMES ON INDIA

The cybercrimes in India has seen rapid growth with the increase in use of mobile phones and the internet penetration in India. The technology adoption is high but the awareness about security and privacy among the citizens is very low. The country is now one of the biggest victim cybercrime in the world. As per the data from the National Crime Records Bureau (NCRB) there was around 70% rise in cybercrimes annually between 2013 and 2015.

Social media contribution towards cybercrime is increasing rapidly in India. As per National Investigation Agency findings "Every sixth cybercrime in India committed through social media" [18]

As most of the social media users in India lack of knowledge and awareness about information security and privacy protection the cybercriminals are targeting their social media accounts. Unless people become aware on protecting their security and privacy it is very difficult to stop the ever increasing cybercrimes throughout the country. According to IAMAI use of social media is one of the major reason for cyber-attacks both in the urban and rural India.



(Source: IAMAI)

Fig.4 Reasons for cyber attacks

As per the Symantec's Internet Security Threat Report 2016, India recorded a 156 percent rise in social media scams and majority of these (94 percent) crimes were spread through sharing of the posts or manual sharing. The report further states that nearly 16 percent social media scams are targeted towards India and every sixth social media scam happening worldwide impacts an Indian. [19]

A.Protecting Information Security and Privacy on Social Media

The best way of dealing with menace of cybercrimes emanating from social media is to make users aware of information security and privacy issues. The users also needs to understand how to how to use of social media platforms responsibly.

Some of the best practices while using social media are:

1.Remove Unnecessary Personal Information: Don't reveal personal information, date of birth, photos, mother's maiden name, etc.

2.Adjust Privacy and Security Settings: Configure the application's security and privacy settings and make best use of all available security features.

3.Do not accept friend requests from strangers: Reject all friend's requests from strangers as criminals may also easy access to your profile and information.

4.Use strong password: Always use strong, lengthy and unique passwords for all social media accounts. This will make the passwords compromise more difficult.

*5.Protect your password***:** Do not share your social media passwords even with your best friends. Where ever possible use multi factor authentication for the accounts.

6.Remove Installed Third-Party Applications: Third party applications access lot of personal information of the users and may also share or sell that information to others.

7.Do Not Publish Your Location: Avoid using geotagging while using social media like the 'check-in' feature in Facebook app as cybercriminals might misuse this information.

*8.Do not trust your online social network friends***:** There are lot of fake users on the social media, so do not share any information with such 'friends' unless their authenticity is properly verified.

9.Monitor your children's online social network activities: Children become easy prey to online predators hence always monitor their activities on social networking sites.

10.Always think twice before posting something: Do not post anything on social media unless you are very sure that the post will not compromise your data security or privacy. Also, always remember that the content in your post is not going to offend anyone.

11.Always update your software: There is nothing like 100 percent secure application and the vendors regularly send updates to the users which tries to mitigate vulnerabilities discovered. Also, apart from applications the users should always update the operating system software (like Android, iOS, etc.)

12.Always use good internet security / antivirussoftware: A good Internet security / antivirus software will enhance the security by preventing compromise of sensitive data of the user on the device. Always the user should update the antivirus software on regular basis.

13.Follow ethics: While using Internet and social media users should follow ethics such as hiding personal information, avoiding bad language, avoid sharing and downloading copyrighted material without proper permission, pretending to be someone else or identity spoofing, spamming, respecting other cultures and religions, trolling others, etc.

VII. ROLE OF EDUCATIONAL INSTITUTIONS OF INDIA IN CREATING INFORMATION SECURITY AWARENESS

As the statistics indicate that maximum number of Internet and social media users in India are youngsters from school children to college students. Most of these people are tech savvy but lack in information security and privacy awareness. This is the primary reason for so many cybercrimes taking place in both urban and rural areas of the country. Educational institutions can play a vital role in reducing the number of cybercrimes in the country by regularly conducting security awareness programs for their students. They can also make the students aware of the process of reporting cybercrime to appropriate authorities and can also counsel victims of cybercrimes.

VIII. CONCLUSION

In the recent years social media has totally revolutionized the way people communicate with others. There many benefits of social media but at the same time it has major

problems with respect to privacy of information and security. Due enormous database of users and their sensitive and personal information, social media has become a potential target of many cybercriminals. As the security and privacy feature on social media platforms are still evolving it becomes very important for every social media user to be aware of all the threats and be careful while using them. The role of educational institutions is very critical in spreading the awareness in protecting privacy of information and security on Internet.

REFERENCES

[1] Robert Allen, Top Social Network sites by number of active users 2017. Retrieved from http://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/attachment/top-social-network-sites-by-number-of-active-users-2017

[2] Craig Smith, By the Numbers: 27 Amazing Wikipedia Statistics (January 2017). Retrieved from http://expandedramblings.com/index.php/wikipedia-statistics

[3] Internet Usage Statistics Retrieved from http://www.internetworldstats.com/stats.htm

[4] Top 20 Countries with the Highest Number of Internet Users. Retrieved from http://www.internetworldstats.com/top20.htm

[5] IAMAI Statistics. Retrieved from http://www.iamai.in

[6] Internet Users by Country (2016). Retrieved from http://www.internetlivestats.com/internet-users-by-country

[7] IAMAI Media Release. Retrieved from http://www.iamai.in/media/details/4486

[8] Number of social media users worldwide from 2010 to 2020 (in billions). Retrieved from https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users

[9] Number of social network users in selected countries in 2016 and 2021 (in millions). Retrieved from https://www.statista.com/statistics/ 278341/number-of-social-network-users-in-selected-countries

[10] Social media in India. Retrieved from http://www.livemint.com/Politics/FqcL24fK5aQ68qC6KzohJO/Social-media-in-India.html

[11] India: social network penetration Q4 2016. Retrieved from https://www.statista.com/statistics/284436/india-social-network-penetration

[12] NIST Special Publication PII 800-122. Retrieved from http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf

[13] Handbook on European Data Protection Law. Retrieved from Handbook on European data protection law EU-2014-handbook-data-protection-law-2nd-ed_en.pdf

[14] Drew Hendricks; The Shocking Truth about Social Networking Crime. Retrieved from http://socialnomics.net/2014/03/04/the-shocking-truth-about-social-networking-crime/

[15] Mary Madden, Amada Lenhart, Sandra Cortesi, Urs Gasser, Maeve Duggan, Aaron Smith and Meredith Beaton; Teens, Social Media, and Privacy. Retrieved from http://www.pewinternet.org/2013/05/21/teens-social-media-and-privacy/

[16] Andreas Illmer; Social Media: A Hunting Ground for Cybercriminals. Retrieved from http://www.bbc.com/news/business-36854285

[17] Nick Hayes; Why Social Media Sites Are The New Cyber Weapons Of Choice. Retrieved from http://www.darkreading.com/attacks-breaches/why-social-media-sites-are-the-new-cyber-weapons-of-choice/a/d-id/1326802

[18] Suchetana Ray and Anirban Ghoshal; Every Sixth Cybercrime in India Committed Through Social Media: NIA. Retrieved from http://www.hindustantimes.com/india-news/every-sixth-cybercrime-in-india-committed-through-social-media-nia/story-KscgnwjcTZ0pzVeVaOiN6M.html

[19] Internet Security Threat Report. Retrieved from https://www.symantec.com/security-center/threat-report