===
Language in India www.languageinindia.com ISSN 1930-2940 18:6 June 2018
Prof. S. Arunraj and Dr. P. Viduthalai, Editors
Portrayal of Social Issues in Literature and Media
Centre for Media and Social Science, Salem, Tamilnadu and
Department of Journalism and Mass Communication, Periyar University, Salem
===

Portrayal of Cyber Security and Laws for Social Media Culture

Dr. M. Malathy and S. Ananda Pragadeeswaran

==

With Social Media Culture (SMC) propagating and distressing our day to day life, our digital addiction level is increasing at a speedy and rapidity. In the urgency to be in this world in the associated globe, users not remember the control over the breathing space to our-self of the information available in the social media. In this paper some of the social media threats and safety measures that would help to keep away from the sufferer of cybercrime.

Keywords: Social Media Culture (SMC), Cybercrimes, Cyber security, Cyber laws

1. Introduction

Nowadays, Social Media Culture (SMC) [1] is involved for high-speed interactions across the world. It channels the public communications using enormously reachable and scalable publishing methods over the Internet. The main objectives of social media consist of linking persons, communities and organizations for exchange of ideas, sharing happiness and relationship. The social media has generated many big business opportunities [2] for enterprises, designed at advertising and running client associations. Popular social media tools include Social Media Culture (SMC) (e.g., Facebook, WhatsApp, and Twitter), shared projects (e.g., Wikipedia), content communities (e.g., YouTube) and blogs (e.g., Blogger). Social media has introduced considerable transform in the way public be in touch. Further, access to social media is increasing from beginning to end portable devices.

Social medium today has integrated skill, content, social contact and revolutionized the system humans communicate. Communication on social media can make enormous viewers organically without any monetary commitment for organization. Social Media Sites (SMS) make easy collaborating, sharing that allow those to construct a public or profile. The type of social media that is the most used in world are sites like Facebook, Twitter and WhatsApp. In particular, we identify numerous advantages of adopting Social Media Sites (SMS) and also establish the related risks; primarily linked to safety, confidentiality and faith.

Similarly, a real moment in time, position bring up to date from users on the Social Media Sites (SMS) may turn out to be a serious threat for their privacy. For these reasons, many individuals as well as organizations are skeptic to endorse them. However, few enterprises chose to design their own Social Media Sites (SMS) [3] limited to their employees.

2. Risks and Challenges

The massive growth of SMS has brought numerous benefits to online communities, but also generated a large number of security concerns. The SMS operates in public domain. Hence, they also provide a vulnerable platform to be exploited by the attackers. Some of the risks and challenges associated with adoption of SMS are as follows.

2.1 Safety Concerns

• *Identity mistreat* – The masquerade of a genuine user by an invader can result in distinctiveness mishandling. The attacker may imprison users' information and damage them consequently. Consider an attacker who creates a forge HR delegate profile on a social networking site. The attacker posts a good-looking occupation opportunity and genuine users may befall the victims by giving out their resumes. The attacker may use these resumes to get together victims' individual information, share it with the third parties or sell to an marketing organization. furthermore, adding together plenty of private information in public profiles may also cause noteworthy spoil to individuals on SMS. The information exposed on the SMS such as full date of birth, mother's name and e-mail can magnetism the attackers since many financial institutes also use this information as a part of user classification. The possibility of such attacks can boost more, if the user accepts needs from strangers. There can be possible data leaks all the way through these *strange* links and entities.

• **Malwares, Viruses and Phishing Attacks**

– Malware and Virus attacks [8, 9] may occur by the use of consumer posts, tweets and email communications. These attacks are also used by intruders to obtain the user's credentials and gain access to the network. After gaining access to the network, the attacker may spread spam mails and steal proprietary or confidential data. The attacker may cache or modify the victim's profile leaving it vulnerable to new attacks.

• Threats from 3rd party applications

– SMS offer the integration with third-party applications. These applications initially seek permission from the user to access personal information present in the user profile. The user clicks on 'Allow' button, potentially losing control over the shared data. Some of these applications, serving the intended purpose in the foreground may also download a malware on the user's machine without their knowledge.

• Legal Aspects - The legal risks associated with the use of SMS for an organization can be broadly summarized as follows.

– Liability due to the breach of organization's security as an outcome of the attack originated from the SMS.

– Legal implications as a result of the leakage of third party confidential information due to the use of SMS.

– Risks associated with attacks against the employees through Social Media Sites (SMS) or associated applications.

– Implications due to posts from employees or outsiders that spread rumours, cause hatred or communal violence.

– Defamation suites due to posts from employees on SMS that caused reputation loss to third parties.

Similarly, SMS may also implicate the individuals. Individuals may face legal charges in the following scenarios.

– Posting offensive content against a particular entity, community or country.

– Anti-legal or anti-national activities of individuals using SMS.

– Leaking confidential information on SMS.

– Invading on someone's privacy.

2.2 Privacy Concerns

Privacy, in Social Media Sites (SMS) remained a complex problem as the concept of social networking and user privacy are quite opposite to each other. The fact that most of the current SMS do not respect the privacy of the user data, is not because of the technical difficulties but rather a design choice made by the providers of SMS. A list of privacy concerns common among SMS users is as follows.

• **Data Privacy** – Users share their personal and sometimes sensitive information on SMS. This may lead to privacy breaches [10] unless appropriate privacy settings are applied for the user's profile. Though SMS provide a range of profile privacy settings, most of the users are either unaware of them or find the mechanism as complex. If the user's profile has the default setting as 'public', then all the information in the profile is visible to everyone. This way, everyone can view the personal information, associations, activities, interests and alumni information which may lead to undesirable consequences. Accepting requests from unknown people may also adversely affect user's privacy. The 'unknown friend' may abuse the user's trust and may try to capture the sensitive information. Besides, users can't control what others can post about them. This way, privacy of both the user and the associated friends is at stake.

• **Tracking Users** – A recent surge of LBSN has invited serious concerns [11] on users' privacy. A real time update on users' location may prove intrusive to the users since the third parties may collect personal information of the roaming users. This way, outsiders probing into the users' personal information can cause them physical security concerns. Likewise, employers may also use SMS as a tool to keep a check on their employees. For example, the HR agency may attach itself to the employees to keep a track on them and monitor their posts.

• Identity Federation Challenges –
Identity Federation is the technique used to share identity across multiple domains. Nowadays, many online websites offer users to login using their Facebook account. The primary purpose here is to add convenience to the users so that they need not to create multiple accounts. But this ability presents tough privacy challenges because users do not have the visibility on how and to what extent their personal information could be shared among third party applications.

2.3 Trust Concerns

Trust, in social networks, plays a vital role for their adoption and is an active area [12] of research. Due to the high susceptibility of Internet, it is necessary to identify with whom we are communicating or dealing online. However, it is very difficult to identify and establish trust for an individual on SMS as there is hardly any direct contact. Considering two entities A and B, entity A is said to trust entity B when entity B behaves exactly in the same way as entity A expects. This 'expected' behavior is often refuted by attackers to exploit the individuals on SMS. Different trust related concerns in SMS are as follows.

• **Online Trust and Reputation Management**– Trust provides a decision support system in SMS. Users often trust their friends, connections and even friend-of-a-friend (FOAF). But attackers use different techniques to abuse user's trust. For example, the attacker creates fake identity of the legitimate user and exploits the user's connections. Similarly, a group of individuals may establish certain behavior among each other and provide unfair ratings such as exaggerated recommendations to each other. In some cases, a disgruntled employee may post some adverse comments which could damage the reputation of the employer.

• Trusting SMS Operators – Whatever users post or upload content in their profile on SMS, the information is usually available with SMS operators. Therefore, users can't trust SMS operators in the first place. SMS operators can retain a copy of the account data even if the original account is deleted by the user. Also, if the data available with SMS operators is in an unencrypted form, it means a direct threat to the user.

• Social Engineering – The technique to persuade the users to disclose their personal and confidential information such as passwords and employment details is known as Social Engineering. Attackers use such a non-technical means to exploit the user's trust on SMS. Moreover, Social media platform can be used for Internet harassment [1] which may cause mental and emotional suffering to the users.

2.4 Impact on Human Relationships

With the creation of SMS, message and contact have pulled out up a new aspect. Even though SMS suggests an efficient way of socialization, its escalating compulsion is building a nation of not-so-social. Citizens have a tendency to use their moment in time on these SMS rather than openly interacting with people and links. as a replacement for of sharing their journey policy with appropriate group, persons have a tendency to post a message on WhatsApp or a Twitter or on Facebook. furthermore, SMS strategy (being an electronic medium) is a reduced way for assigning the emotions. This emotional invisibility can further change the human associations.

2.4.1 Tackling Aggression against Women Online

- In India, the Centre for Cyber Victim Counseling develops educational cyber-awareness programs for schools, for parents and for community members such as the police force.

- Women's Aid in the UK has created a practical guide for victims of online abuse entitled: Digital stalking: a guide to technology risks for victims. "Just five rules for what you can do on the site: Don't spam; Don't ask for votes or engage in vote manipulation; Don't post personal information; No child pornography or sexually suggestive content featuring minors; Don't break the site or do anything that interferes with normal use of the site."

- ***Heartmob*** is a platform that provides real-time support to individuals experiencing online harassment - and gives bystanders concrete actions they can take to step in and save the day [11].

2.5 Information Security

Internet-based threats are not only on the subject of crippling communications and collapse important systems in the world. The world web media information security is a major issue for various web-connected entities. Google faced the important cyberattack to access the Gmail accounts of various Chinese human rights activists in December 2010[12]. The hidden software that contains the PDF file was automatically open the documents and ability to discover some of the Google internal systems.

2.6 Cybercrime of United Nations Office on Drugs and Crime

UNODC in its 2013 Comprehensive Study on Cybercrime proposes 14 acts that can represent cybercrime, structured in those similar three categories [13]

Acts against the privacy, reliability and accessibility of computer data or systems:

- Illegal entrée to a computer system
- Illegal contact, interception or gaining of computer data
- Illegal interference with a computer system or computer data
- Production, allocation or possession of computer abuse tools
- Breach of privacy or data protection measures

An interrelated act for individual or economic gain or harm in the computer:

- An interrelated fraud or counterfeit in the computer
- Interrelated self-offences in the computer

- Interrelated patent or brand offences in the computer

- Distributing or controlling sending of Spam

- Interrelated acts causing personal harm in the computer

- Interrelated solicitation or 'grooming' of children in the computer

Computer content-related acts:

- Interrelated acts involving hate speech in the computer

- An interrelated production, distribution or possession of child pornography in the computer

- Interrelated acts in support of terrorism offences in the computer

The basic security breach tools with which the enumerated crimes are committed are backdoors, botnets, denial-of-service attacks, keyloggers, logic bombs, malware, pharming, phishing, rootkits, smurfing, spoofing, spyware, Trojan horses, viruses, worms, and many more, [14] the reach variety and the definition of which can be found elsewhere. [15]

2.7 *Mobile legal policy and cyber law for SMS in India*

Now-a-days Indians are using mobile phone equivalent to their large population. Communicating Social Media Sites (SMS) via mobile phone is more popular than the PC communications. So mobile manufacture and world business peoples are targeting the Indian customers. Large number of mobile user needs cyber legal policy and cyber law to access Social Media Sites (SMS). India is a right place to put Information Technology Act 2000 for information security in the usage of mobile phones.

2.8 Conclusion

The potential of social media sites and strong-minded are linked risks. We also offered various parameters based on which social media sites can be evaluated. However, the security challenges posed by Social Media Sites (SMS) need a united effort from the Users, Organizations and the Social Media Sites(SMS) operators. Users should protect their personal information prudently to avoid any identity misuse or theft. Organizations and Social Media Sites (SMS) operators should create a balance by enforcing adequate security measures to reap the best results. Despite of the inherent risks, social media possibly will remain as a powerful communications channel, acting as a dynamic source for information, talent and customers. The Digital and Network technologies have taken us from the industrial era to the information era. This information era created cyberspace which is never a secure space. As an interconnected society, we are committed to building this Better-Connected World. Social media is here to stay and become more powerful. The organization need to put in policy of usage and make the employees aware of the policies as the use of social media brings challenges for organizations, because it is a new communication tool that needs to be implemented in the already existing communication goals, strategies and daily activities of the organization. Be a responsible netizen, extend it to the society and make cyberworld a safe and secure place to digitally coexist.

==

References

[1] The Complete guide to Social Media from the Social Media Guys, http: //www. thesocialmediaguys.co.uk / wpcontent/ uploads /downloads/2011/03/ Complete Guide to Social Media.pdf

[2] The Social Economy: Unlocking value and productivity through social technologies, McKinsey GlobalInstitute, July 2012. http://www.mckinsey.com/insights/mgi/research/ technology_ and_innovation/the_social_economy

[3] IBM Beehive, http://www-01.ibm.com/software/ucd/gallery/beehive_research.html

[4] 1 Billion Facebook Users on Earth, http://www.forbes.com/sites /limyunghui/2012/09/30/1-billionfacebook-users-on-earth-are-wethere-yet/

[5] A Social Collaboration Platform for Enterprise Social Networking. Minbo Li, Guangyu Chen, Zhe Zhang, Yi Fu.IEEE, 16th International Conference on Computer Supported CooperativeWork in Design (CSCWD), June 2012.DOI -10.1109/CSCWD.2012.6221890

[6] https://foursquare.com/

[7] http://en.wikipedia.org/wiki/Gowalla

[8] An Analysis of Security in Social Networks. Weimin Luo, Jingbo Liu, JingLiu, Chengyu Fan. IEEE, International Conference on Dependable, Autonomic and Secure Computing, December 2009. DOI -10.1109/DASC.2009.100

[9] Friend-in-the-Middle Attacks:Exploiting Social Media Sites (SMS) for Spam. Markus Huber, Martin Mulazzani, Edgar Weippl, Gerhard Kitzler, Sigrun Goluch. IEEE, Internet Computing, pp. 28-34, 2011. DOI -10.1109/MIC.2011.24

[10] Exploiting Vulnerability to Secure User Privacy on a Social Networking Site. Pritam Gundecha, Geoff rey Barbier, Huan Lui. ACM, SIGKDD International Conference on Knowledge Discovery and Data Mining, August 2011. DOI -10.1145/2020408.2020489

[11] West, Jessica. (2014). Cyber-Violence Against Women. Prepared for Battered Women Support Services, Vancouver,May 2014.

[12] Thompson, TEXAS LAW REVIEW, 474 (2011).

[13] Comprehensive Study on Cybercrime 16. 2013. For substantive elements of each proposed group please refer to the Study at 17-21.

[14] Thompson, TEXAS LAW REVIEW, 469 (2011); BRENNER, Cybercrime and the Law: Challenges, Issues, and Outcomes 36-56, 121-126. 2012.

[15] There are numerous publicly available sources on the technical nature of cybercrime tools. See for example Yvonne Jewkes & Majid Yar, Handbook of Internet Crime (Routledge 2010).
[16] http://goo.gl/y7HQw9

Dr. M. Malathy
Professor
VTHT, Avadi
Chennai

S.Ananda Pragadeeswaran
Asst. Prof,
BPA College of Education
Vamban