Technology Challenges in Social Networking and Cyber Security

ISBN: 978-1-943295-14-2

Praveen Gujjar J
T Manjunatha
Visvesvaraya Technological University
(gujjarpraveen@gmail.com)
(tmmanju87@gmail.com)

Cyber-Ethics, Cyber-Safety, and Cyber-Security issues need to be integrated in the educational process beginning at an early age. These trends are posing a threat to human security, and there is a need for greater Government security and awareness amongst citizens to safeguard their information on the World Wide Web. This paper focus on social media and social network challenges and risk involved in the social network because of the increasing number of user. The paper also describes the recommendation to secure the personal information of the user safe.

Keywords: Cyber Safety, Cyber Security, Cyber Risk, Social Media, Social Networking

1. Introduction

The Internet has changed the manner in which individuals express their perspectives, by the introduction of web 3.0 user's can have conversation about the product or service with manufacturer or service, ers expressing their views, emotions and sentiment through social network sites like Google Plus, Twitter, Facebook etc. Social network is producing a huge volume of notion rich information as tweets, reviews, comments, discussion, blog entries, and so forth. Social media network gives a chance to businesses by giving a stage to interface with their target customer for advertisement. A user on the most of the cases depends widely on other user's generated content for decision making about the product available in the online. Because of the huge content generated by the users in a daily basis it becomes a difficult job for the ordinary users to analyze the content. Hence there is a great demand to automate the users review. In information technology data protection or information security is one of the great challenges for the world. Sharma (2012) analyzed that in IT industries data security is one of the serious issue. In whole world internet is one of the important and faster growing things for business development as well as in different private and government organization. Internet use varies in different sector like government department, banking, national defense, ecommerce, communications, finance firm, entertainment, and private organization for various functions. Sofaer et al (2012) said that the most use of internet for all above functions in our life chances of the attack from attacker on our information are higher priority. Cyber security is one of the most important terms in computer and information technology. Protection of our data or critical information is very essential for everyone. This is technology age, everybody wants technology in their hand to solve his/her problem or increase efficiency of work. But because of the tremendous use of internet in every field the protection and privacy also get affected. Rajaretnam (2012) shown that for the protection of privacy and data from attacker and different techniques and software may used to increase the level of public concern. Burtescu (2009) analyses that there is lot of challenges for data protection in the information age because of the social media and social network and there may a chance of database may go through different level of attacks. The attacks may be classified as indirect attack or direct attack. These attacks can also be called as passive attack and active attack. Kulkarni et al (2012) shows that attacker or hacker are plays their role to attack or hack the information. Regularly they attack on network as well as hack all information or available on sites. Gujjar and T Manjunatha (2016) analyzed that an Innovation taking place in technology incorporates certain ethical standards into law. E-marketing enables new business practices it has many advantages, in the same way it also brings certain risk. Manjunatha and Gujjar (2018) analyzed nature of the Indian Information Technology companies. The paper is organized in four parts. Part 1 is the introduction; Part 2 presents objectives; Part 3 Social media and social network challenges; Part 4 presents the cyber security in India; Part 5 presents Summary and conclusions. References are given after Part 5.

2. Objectives

2.1 We have set following objectives based on the evidence Kulkarni et al (2012) and Gujjar and T Manjunatha (2016)

- To analyze the risk in using social network for the citizens of the country.
- To Suggest safety tips for using social media and social networking

3. Social Media Challenges and Risk

Social media is explained by a number of tools, which includes social networking sites blogs, Facebook, micro-blogs, Wikis, twitter and discussion forums. It has been observed that Facebook, twitter and other discussion forms are initiating a negative publicity about the person, place or event. Everyday social media users are increasing exponentially because of the internet users. It was uncovered that Social networking sites allow data to spread rapidly among people in general. Social media and social networking sites empower clients to trade thoughts, to post updates and remarks, share their interest, talk about activities and events etc. social networking are used for various purpose by different communities like from general chit-chat may end up proliferating into breaking news, from gentle humor into serious discussion, coordinating disaster response etc.

At same time, social media and social network make secret data even more insecure. Social media and social network like Facebook, LinkedIn, Twitter has surprised the world. With the steady want to cooperate with each other and be associated, the capacity and reliance on web to convey this systems administration ability becomes more grounded. Social media and social network enable individuals to make an public and semi public profile on the web, associate with various clients with whom they share a typical association on the equivalent/distinctive stage normally called "Companions or Friends". Social media and social network empowers users to see their friend's conversations, their personal and social life details and interests etc. Social networking sites are an online platform that attracts a community of users and enables them to create their personal and social profile. The users share their profile with people who share common interests, goals or causes. The profile or perceived impression of self will enable users to connect with different people or so called friends. They communicate in their social group through forums, emails, instant messaging etc. Issues as the growth of social networking sites has brought various benefits it also has brought various security concerns. It also provides a vulnerable platform to be exploited by the attackers. Garg et al (2015) and Das et al (2017) analyzed some issues associated are as follows.

1. **Misusing Identity**: The attacker imitate the identity of any user results in misusing identity. The attacker at that point may access all the data and that data can be abused without the knowledge of the actual user.
2. **Threats from using 3rd Party Applications**: These applications seek permission from the user to access personal information for all the various games and apps (especially in mobile apps). The user grants the app a certain level of permission concerning user's information. Further some of these applications which are playing at the foreground may download a malware on the user's computer or phone without their consent.
3. **Trusting Social Networking Sites Operators**: The contents that user uploads or posts on social networking sites, the information are available with the networking operators. The operators can save account data even after the deletion.
4. **Viruses, Phishing Attacks and Malwares**: Viruses and malware often find their way onto your computer through those annoying ads. After gaining access to the network, the attacker can access or steal confidential data by spreading spam mails.
5. **Legal Issues**: Posting contents that is offensive to any individual or community or country. There are legal risks associated with the use of social networking sites like leaking confidential information on sites or invading on someone's privacy.
6. **Tracking Users**: It can cause physical security concerns for the user, as the third parties may access the roaming information of the user by collecting the real time update on user's location.
7. **Privacy of Data**: Users share their information on social networking sites. For example everyone can see the information of a user, if the user's default setting is 'public'. Accepting requests from unknown people can also create a security threat.

Risks and Challenges

Risk and challenges Garg et al (2015) analyzed that, with the increase in the number of users accessing social networking sites, has opened new routes for the attackers to gain access to the accounts of the individuals. The more Information that is posted creates a new threat on the privacy. Social Sites are growing rapidly posing new risks for individuals and organizations in this modern world of technology. And some of the challenges are as follows

1. **Phishing Attacks**: Phishing is the form of stealing vital sensitive information of the user by means of electronic communication. In this method attacker gain confidential data such as password, credit or debit card information etc.,
2. **Identity Federation Challenges**: It is a technique used to share user credentials across multiple domains. For example many sites offer users to login by their Facebook Account, google account etc., so that it is more convenient to the user and the user does not have to make multiple accounts across different sites. It may seem convenient but the user does not have the knowledge about on how and to what extent their personal information can be shared among third party applications.
3. **Malwares**: Malwares are the programs which are installed in the user's devices without the knowledge and consent of the user. This spreads fast and infects the devices or software.
4. **Click Jacking Attacks**: In this attack the Trojan in web pages asks the user to click on the malicious link, and a malware is planted onto the system. This is common in Facebook with the name like jacking that is when a user likes a page, a picture or a video the user is trapped by the attackers. This type of attacks are done to do malicious attack or to make some page popular.

4. Cyber Security in India

Garg et al (2015) and Das et al (2017) explain that internet usage has increased in India; cyber-crimes have also increased respectively. Das et al (2017) shows More than 32000 cyber-crimes were reported between 2011 and 2015, across India and more than 24000 of these cases have been registered under the IT Act and the remaining cases under the different sections of IPC and other State Level Legislations (SLL).Cyber-crimes are registered under three broad heads in India, the Indian Penal Code (IPC), the IT Act and other State Level Legislations (SLL). The cases registered under the IT Act include

- Tampering with computer source documents (Section 65 IT Act)
- Loss /damage to computer resources(Section 66 (1) IT Act)
- Attempt Hacking (Section 66 (2) IT Act)
- Accessing Digital Signature Certificate by misrepresentation of facts (Section 71 IT Act)

- Publishing false Digital Signature Certificates (Section 73 IT Act)
- Fraud Digital Signature Certificate (Section 74 IT Act)
- Breaking of confidentiality or privacy (Section 72 IT Act)
- Failure to aid in decrypting the information intercepted by Government Agency (Section 69 IT Act)

5. Suggestions to Keep Safe

Dwivedi (2018) shows that in the present world of digitalization masses have welcomed the mobile solutions that speed up daily transactions, such as online shopping and banking, for the reason that it can be accessed anywhere and anytime. Such users generally fall prey to the cyber criminals who always try to device new ways to rob the innocent users by taking edge of unsecured wireless networks, third-party applications, and texting to acquire personal information. At this technologically advanced stage, to protect yourself and your information, it is important to take these following steps

- Allow only authorized user to access wifi service.
- Use password with the combination of lower case letter, upper case letter, numerical and some special characters to keep your password safe.
- Keep your anti-virus software updated to protect against viruses, spyware, and malware.
- Don't download or click on the unknown link for unwanted ads.
- Keep personal information secure to avoid identity theft.
- Transfer personal vital information to trusted sites.
- Don't disclose the more personal information in social network and in social network profile
- Depending on the need user must set display of profile information as public or only to the contact list.
- Be attentive when interactive with chat rooms, social network or in any other platform, don't disclose any credit card or debit card details.
- Parents should monitor their children activity in the internet in order to avoid any dangerous situation and parents should educate their children about the safety tips to be followed while using any social networking sites.

In this section, some recommendations are given to secure the information of the user

- Avoid responding to spam or phishing mails in un-trusted network.
- Don't use any pirated operating system or cracked version of the operating system use only genuine operating system.
- Update the antivirus software regularly to avoid malwares.
- Use multi level authenticating system to avoid the attacker from unauthorized access.
- Before using the internet user must ask this question to themselves whether internet is free or they are free, to avoid unwanted destructions.
- Switch off the mobile data when cell phone is ideal.
- Training and educational programs should be done by the government to spread the awareness about cyber security. The Government should conduct publicity campaigns and programs which includes seminars, contests, and exhibitions about cyber Security.
- Social Networking Sites which has the privacy security setting discusses the tools which available to make the account more secure.

Privacy security in social network are subdivided as

1. Who-can-see-my-stuff: This is priority setting for the Facebook users where the user can limit the audience who can see the posts from the user. Public posts should be avoided for security
2. Login-Alerts: This setting allows the user to get a notification when anyone logs into their account from an unrecognized device or browser.
3. Third-party-authenticator: This is the new setting added to the Facebook which enables to generate Facebook security code to authenticate any third party app.
4. How others interact with the user: This helps user to manage how other people's activity affect the user's profile. And the user can manage tags, 'unfriend' or 'block' someone.

6. Summary and Conclusion

In the present era of cyber revolution and globalization, the entire world is witnessing the novel problem for human security. The prime test is to ensure the human security. The most widely recognized and well known utilization of web is for person to person communication. Taking a gander at its prevalence it has even turned into a well known spot for digital assaults by programmers/digital offenders. The social media and social media network is most preferable site by the attacker to gain the personal and private information of the user. The education institution, the government and other private sector should create the awareness on protecting the necessary information of the user from the attacker. It is very easy to find crime but at the same time it is bit challenging to link that crime towards criminal. Hence it is the duty of education institution and government to spread the awareness among the user about the cyber security and cyber ethics. It is also the responsibility of the education institute; government sector and other private sector devise a way for youth to put them in the right path. To avoid the cybercrime global efforts are required because attackers may attack not only from the local national it could be from foreign countries too. Every user must know and must understand IT act before using the social network. As the utilization of

social network increases, odds of falling prey to digital violations are likewise getting roots. It is relevant for the clients to be progressively alarm and ready to perceive the strategies like digital stalking and cyber bullying posing presenting risk to individual security. Strategies, for example, hacking and phishing are utilized to fool individuals into uncovering individual data. Emails tricks are a typical type of extortion that attacker use to exploit individuals. This paper focused more on challenges in social media and risk involved in usage of social media is outlined. Recommendation may follow to preserve the user vital information.

7. References

1. D. Sofaer, David Clark, and W. Diffie (2012), 'Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy', http://www.nap.edu/catalog/12997.html, 'Cyber Security and International Agreements, Internet Corporation for Assigned Names and Numbers', pp.185-205.
2. Divya Dwivedi (2018) Technological challenges to Human Security in the Age of Information and Cyber Wars, INTERNATIONAL JOURNAL OF BASIC AND APPLIED RESEARCH, Volume 8, Issue 2, pp 40 – 48.
3. Emil Burtescu, (2009) 'Database Security-attack and control method's', Journal of Applied Quantitative Methods, Vol. 4, Issue 4.
4. Praveen Gujjar and T.Manjunatha (2016), 'A Study of Ethical and Legal Issues in E-Marketing in India', AIMS International conference proceedings, Vol 1, Issue 1, pp. 1-6.
5. Pritam Gunecha, Geoffrey Barbier, Huan Lui, (2011) Exploiting Vulnerability to secure user Privacy on a social networking site, ACM, SIGKDD International conference on knowledge Discovery and Data Mining, Volume 1 , Issue 1.
6. Ravi Sharma (2012), 'Study of Latest Emerging Trends on Cyber Security and its challenges to Society', International Journal of Scientific & Engineering Research, Vol. 3, Issue 6, pp. 240 - 248
7. Richa Garg, Ravi Shankar Veerubhotla, Ashutosh Saxena (2015), Security, Privacy and Trust in Social Networking Sites. CSI Communications ISSN 0970-647X, Volume 39, Issue 2.
8. Rituparna Das and Mayank Patel (2017) Cyber Security for Social Networking Sites: Issues, Challenges and Solutions, International Journal for Research in Applied Science & Engineering Technology (IJRASET), Volume 5, Issue 4, pp 833 – 838.
9. S. Kulkarni, S. Urolagin, (2012) 'Review of Attacks on Databases and Database Security Techniques', International Journal of Emerging Technology and Advanced Engineering, Vol. 2, Issue 11.
10. T. Manjunatha and Praveen Gujjar J (2018), 'Profitability Analysis of Indian Information Technology Companies using DuPont Model' , Asian journal of Management, Vol 9, Issue 3, pp. 1105-1108
11. T. Rajaretnam, (2012) 'The Society of Digital Information and Wireless Communications (SDIWC), International Journal of Cyber-Security and Digital Forensics', Vol.1, Issue 3, pp. 232-240.