An Assessment Cram on Security Issue of Fake Identity Behavior in Social Media

Deepak Dashora[1], Dr. Manish Shrimali[2]
[1]Research Scholar, JRN Rajasthan Vidyapeeth University, Udaipur, Rajasthan, India
[2]Research Supervisor, JRN Rajasthan Vidyapeeth University, Udaipur, Rajasthan, India

Abstract: *In the present era the role of social media is very important in respect of making world a global village. People who are connected with these media are sharing their professional and social life information and updates. But some antisocial elements are misusing such social media and it becomes threat for innocent people. The present review or assessment paper tries to provide an outline concern to fake identity and behaviors available on social media.*

Key Words: *Social media, Identity, Information, Security, Facebook, Privacy.*

1. INTRODUCTION:

In general, Social media is concern from the group of groups of people at various levels and countries which are connect through the internet and sharing their information, photographs, videos and data. Behind the social media, the basic purpose is to keep up or convey the far-away people collectively and providing a platform to share their opinion and outlook as well as their current information. The information updates in social media in existing situation plays a fundamental function in keeping people together independent of the geographical boundaries.

As we know that each coin has two sides, in the same way social media also has several affirmative and pessimistic characteristic too. There are people sharing abusive information and fake material or socially restricted data to the sites and creating an unnecessary confusion and sometimes it also harms the image of people in the social media. Hence, for such activity there are least number of safety parameters available which are unable to identify the user at their best. Information regarding Name, Age, Gender, Location, email address and contact numbers are purposively provided wrong to fool the other user on the sites or media.

2. ISSUE OF FAKE IDENTITY AND SOCIAL MEDIA:

In the present day, it is essential for a person to stay connected with the internet as well as its diverse media tools. It is a need of the hour to do so for successful growth and development of a person concern. Fooling people and taking correct information out from the users is not only limited to the social sites but also applies to the corporate. For their mere benefits of marketing and advertising their own products, asking the user information and then sharing it to the mass marketers for an amount of profit is also one of the critical security aspects of social and online media.

At the similar point in time as a person were busy answering questions there were teams of people assessing questions and assisting in the background. There are many security issues to avoid a fake identity on social media such as persons' email id and their passwords and many more.

Social Media is internet based communication platform providing enhanced facilities to the one to ensure variety of data and information to be transmitted and shared.

Varieties of forms have been developed by these social media sites to share the information among the friends and relatives of one. Such activities of social media increases the attraction of using and connecting to these social sites in the user and ultimately, the user in the sake of sharing of information to his/her friends, shares personal data and information unknowingly to the person who is not at all concerned about. Such people are called hackers, who manipulate the information shared on these sites and exploit the user thereof which is being a major security issue for the user. Creating fake identity over the social media through internet is nowadays is very often and hence needs to be handled such issues very seriously and carefully.

The varying aged groups including children, adults, women and middle-aged people are the core users of the internet and social media sites. Hence, large number of variety of data and information are shared and transmitted via internet network. So, there is a vital importance to catch hold such internet hackers and to restrict their illegal use of the information.

3. ISSUES MATERIALIZE:

The issues concerned from the study refer to the inconsistency among the two variables at different point of time and knowing the positive and negative effects. What went before assessment of the prose of the research work finished before now shows that there is immobile plentiful span? As there is increasing demand for the social media, fast update of the electronic communication technology has led to arising of more online security issues in the social media day by day. So, it is of vital call for to be acquainted with the fissure in the effect of online security issues of fake identity behavior in social media and their technological solutions. There are the varieties of issues in the field in the present scenario of social media. The main focus would consist on knowing the security issues, technical issues and fake identity behavioral aspect in social media.

3. AN ASSESSMENT OF FAKE IDENTITY BEHAVIOR:

An assessment is a study of past research work on the given topic. It simply refers to study and understand the past researches. It acts as an outline as suitable directions to the framed research.

3.1 Impact of Online Social Networking

Online social networks make easy connections between people based on shared interests, values, membership in the groups (i.e., friends, professional colleagues). They make it easy for people to find and talk with individuals who are in their networks using the web as the interface. For instance LinkedIn is strong in identity and also chains relationships and reputation. On the other hand, Facebook is strong in relationships and also chains presence, identity, conversations and reputation. Ning is strong in groups and also chains sharing and conversations.

3.2 Fake Identity on Social Networks

Social networks altogether have absorbed worldwide responsiveness these days because of their possibility to address masses and probable future customers. Social networks such as Facebook, Twitter and Google+ have captivated masses in the back years considerably. The potential of social networks is often distorted by malevolent users who extract the delicate private material of ignorant users. The most common ways of carrying out a large-scale data harvesting attack is the use of bogus profiles, where malicious users present themselves in profiles imitating fictitious or real persons.

3.3 Role of Technical Literacy in Social Media Networks

Education department of Colorado describes the technology literacy as the ability to correctly select and responsibly use skill & technology. Students who have reached technological literacy are able to:

- Problem-solve
- Connect
- Locate, use and synthesize info & found using technology
- Advance skills necessary to task in the 21st century

3.4 Mobile Social Networking Applications

Mobile social networking is the social networking where persons with similar interests converse and attach with one another through their mobile phone and/or tablet. More like web-based social networking, mobile social networking occurs in virtual groups. Numbers of web-based SNSs, such as Facebook and Twitter have shaped mobile applications to give their users prompt and real-time access from anyplace they have access to the Internet. Moreover, native MSNs have been shaped, such as Instagram, Foursquare and Strava, to let communities to be built around mobile functionality.

3.5 Social Media in Communication

Social media simply refers to interactions among people in which they generate, share or exchange information and ideas in virtual groups and networks. The Office of Infrastructures and Marketing manages the main Facebook, Twitter, Instagram, Snapchat, YouTube and Vimeo accounts. An array of tools with one-on-one consults with schools, divisions and offices looking to form or uphold an existing social media presence to discuss social media goals and plan, as well as offer visions and ideas.

3.6 Impact of Profile Cloning

Where someone other than the genuine owner of a profile creates a new profile in the same or dissimilar social network in which he copies the original info. By doing so, he makes a fake profile impersonating the genuine owner using the cloned info. Since users may uphold profiles in more than one social networks, their associates, especially

the more distant ones, have no way of knowing if a profile encountered in a SNS has been shaped by the same person who shaped the profile in the other site.

3.7 Privacy and Security of User Information

Information privacy, or data privacy (or data protection), is the connotation between pool and dissemination of data, technology, the public expectation of privacy and the legal and political issues nearby them.

Privacy alarms exist wherever personally identifiable info or other sensitive information is collected, stored, used, and finally demolished or deleted – in digital form or otherwise. Unsuitable or non-existent disclosure control can be the root cause for privacy issues. Data privacy subjects may arise in reply to information from a wide range of sources. The task of data privacy is to use data while protecting individual's privacy predilections and their personally recognizable information. The fields of computer security, data security and information security design and use software, hardware, and human resources to address this issue. Since the laws and guidelines related to Privacy and Data Defense are constantly changing, it is significant to keep abreast of any changes in the law and to repeatedly reassess obedience with data privacy and security rules.

3.8 Taboo Contents

A **taboo** is a fervent prevention of an action based on the certainty that such behavior is either too sacred or too accursed for normal individuals to undertake. Such exclusions are current in almost all societies. The word has been rather expanded in the social sciences to strong exclusions relating to any area of human activity or custom that is sacred or prohibited based on moral judgment and sacred beliefs. "Breaking a taboo" is typically measured objectionable by society in all-purpose, not just a subset of an ethos.

3.9 Hackers and Predators in Online Social Media Networking

Hackers object social sites like LinkedIn and even Facebook to obtain tons of info about potential targets. As a matter of fact, Social Engineers have formed bogus LinkedIn users and used a programming boundary to easily search for users at a specific place of business and pull a lot of info from their account that could be used in a Social Engineering occurrence.

Unfortunately there is also an alarming trend of stalkers and predators possibly using social media sites to track or find possible victims. For over a year and a half, the community consciousness website ICanStalkU.com presented internet users how easy it was to pull geotag info from pictures posted on social media sites. They would post a picture pulled from a social site along with the pictures user name and… Their Site!

4. CONCLUSION OF ASSESSMENT:

Nowadays up to date developments of inclined uses of social media and increasingly connecting users regularly have go in front to materialization of online security issues of the personal information over the internet. In support of the same issues, research is essential in the direction to identify such fake behavior over the internet related to identity, information and security. Present assessment is not just confined with studying the issues in online social media security, but it will concentrate on various aspects on how to reduce such issues. Further research will throw light on how to identify a fake identity over the social media and what steps can be taken to restrict or reduce such behavior of the user.

REFERENCES:

1. Alhajj, Reda, Rokne, Jon: “Encyclopedia of Social Network Analysis and Mining”, Springer-Verlag New York, Vol. 1, No. 1, pp. 1-2437, (2014)
2. Ali, A. and Hudaib, Z: “Comprehensive Social Media Security Analysis & XKeyscore Espionage Technology”, International Journal of Computer Science and Security, Vol. 8, No. 1, pp. 97-158, . (2014)
3. Altshuler, Y., Fire, M., Aharony, N., Volkovich, N., Elovici, Y. and Pentland, A. (2013), “Trade-Offs in Social and Behavioral Modeling in Mobile Networks”, Springer Berlin Heidelberg, Vol. 7812, pp. 412-423.
4. Baruahm, T. : “Effectiveness of Social media as a tool of communication its potential for Technology enabled connection : A micro-level study”, International Journal of Scientific and Research Publications, Vol. 2, No. 5, pp. 1-10, (2012)
5. Das, B. and Sahoo, J. : “Social Networking Sites – A Critical Analysis of Its Impact on Personal and Social Life”, International Journal of Business and Social Science, Vol. 2, No. 14, pp. 222-228, (2015)

6. Elangovan E. and Chandrakala D.: "Identification and Prevention of Multiple Account in Social Media", International Journal of Advanced Technology in Engineering and Science, Vol. 03, No. 01, pp. 80-88, (2015)
7. Griffin, C. and Squicciarini, A. : "Toward a Game Theoretic Model of Information Release in Social Media with Experimental Results", IEEE Symposium on Security and Privacy Workshop, Vol. 1, No. 1, pp. 113-116, (2012)
8. Jin, L., Chen, Y., Wang, T., Hui, P. and Athanasios V. : "Understanding User Behavior in Online Social Networks", IEEE Communications Magazine, Vol. 1, No. 1, pp. 144-150, (2013)
9. Livingstone, Sonia and Brake, David R. : "On the rapid rise of social networking sites: new findings and policy implications", Children & society, Vol. 24, No. 1, pp. 75-83, (2010)
10. Suhial, A. : "Privacy & Security a Concern in Social Networks", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS),Vol. 4, No. 1, pp. 75-83, (2015)
11. Tariq, W., Mehboob, M., Khan, M. and Ullah, F: "The Impact of Social Media and Social Networks on Education and Students of Pakistan", International Journal of Computer Science Issues, Vol. 9, No. 4, pp. 407-411, . (2012)
12. Tsikerdekis, M., Zeadally, S. : "Online Deception in Social Media", Library and Information Science Faculty Publications, Vol. 57, No. 9, pp. 1-16, (2014)
13. Verma, A., Kshirsagar, D. and Khan, S. (2013), "Privacy and Security: Online Social Networking", International Journal of Advanced Computer Research, Vol. 3, No. 1, pp. 310-315.
14. Young, K. : "Managing online identity and diverse social networks on Facebook", Webology, Vol. 10, No. 2, pp. 1-18, (2013)