Social Media Security Threats Investigation and Mitigation Methods: A Preliminary Review

Mandeep Singh¹, Chaman Verma² and Pamela Juneja³

¹Department of Comp. Science and Engineering, Chandigarh University, Chandigarh, India.
²Department of Media and Educational Informatics, Eötvös Loránd University, Budapest, Hungary.
³Department of Comp. Sci. and Engg., Chandigarh Group of Colleges, Chandigarh, India.

E-mail: mandeep.cse@cumail.in, chaman@inf.elte.hu, pamela.4081@cgc.edu.in

Abstract. Recent advancement of data collection and coupled statistics, big data became a significant issue in various research areas like: Machine learning, data mining, social networks, artificial intelligence, etc. Social networking is used as a platform for various applications like: government, business, educational, political, dating and matrimonial, etc. Like each and every platform, social networking too has its own set of pros and cons. We examine the types of posting on social media websites and influence of posting data and privacy concerns of Facebook and twitter users. This study indicates the different concerns of users regarding posting information and its influences of user voiced privacy concerns. It is beneficial in fields like: education, advertisements, online shopping but people get addicted to social networking, its time consuming in various issues and can be misused for cybercrimes. We’ve discussed the e-government objectives of using social media. Social networking is also vulnerable at different stages and attacked in several ways that includes evil twin attack, virus attack, phishing attack, account hijacking, data breach attack, fraud and scams. Site monitoring, developing security policies, educating users and training programs, updating software, archiving, media contents are several mitigation techniques are used to reduce the effects of cyber-attacks.

1. Introduction

Big data is a numerous amount of data consists of structured, semi-structured and unstructured data that are increasing massively from various internal or external data sources. The data size can be measured in terabytes, petabytes and Exabytes. Big data is conceptualised on 3Vs: (i) Volume – Includes large amount of data, i.e. data generated by organizations, social media, etc. (ii) Variety – Data exists in wide variety of heterogeneous data available in different formats like text, audio, video, image, database, etc. (iii) Velocity – it’s the rate of generation of data depending on sensors, internet to analyse big data in effective manner.

Several individuals and organizations proposed to expand the original concept of 3Vs. Some common additions are:

Veracity – The complexity and variety of sources to evaluate the quality of data [1].

Variability – variation of data cause contrast in quality and variety of sources required to process, identify and filter data.
Big data has been implemented for business optimization, medicine and health care, financial services, fighting cybercrime, etc. Big data faces several challenges like: security and privacy, breaching sensitive data, data quality/integrity, lack of transparency, ethical and social challenges, surveillance, unfair discrimination, etc. [2]

Basically, Social network is a group of individual or organizations that share a social class that share interests and idea and making new friends, like networking groups. It helps people to stay connected with family and friends. Unlike regular media generally created by a few people, social media websites consist of unlimited users. Several social networks commonly used now-a-days are like: (i) Facebook – most popular website on the internet. It’s user’s destination to connect with family and friends’ online and sharing images, movies, etc. (ii) Classmates – website used for connecting high school graduated individuals and be in touch for future reunions. (iii) Instagram – a flexible photo sharing service available for all platforms. (iv) Google – It’s a recent social networking application from Google. (v) Pinterest – a sharing service allows everyone to share their creations and collections.

2. Related Work

Wajeb Gharibi et al., (2012) [3] investigated the cyber threats in website that related to social media. Social network consists of organizations or individuals known as nodes, connected by relations like: common interest, friendship, exchange of finance, connection of opinions, knowledge or reputation. Threats can be intentional or unintentional, targeted or non-targeted and come from a several sources such as: intelligence and information warfare, hackers, virus writers, criminals, existing contractors or unsatisfied employees in an organization. Other than interacting or communicating Social networking websites flourishes business promotions. They have studied the history of online social websites, classified their types, discussed cyber threats, and suggested anti-threats methods for future. Yongick Jeong, et al., (2017) [4] examined the influence of the different posts, statistics, and privacy issues regarding users of different websites like Facebook and Twitter. The study indicates the preferences of young users’ postings individually on Facebook and Twitter. The content of posts variably influence the privacy concerns created by users on the basis of user type (authoritative, marketer and distant relations). Rakesh Singh Kunwar, et al., (2016) [5] reviewed the details of security risks, threats and different attacks using social media. Social media and Internet generated different ways to communicate in originated world. Tweets, sharing images, likes and comments are several ways to communicate among friend and families all over the world. In the past several years, social networking sites played a vital role to connect via Twitter, YouTube, My Space, Facebook, LinkedIn, etc. Social media helps to create network with people, but social media websites possess several security risks to users and organizations. This paper provides an in-depth detail of threats, security risks and different types of attacks using social media. Gabrielle G. Groth, et al., (2017) [6] summarized the latest updates related to alliance among college students use of social media and risk behaviors. Social media is widely and frequently used among students. Risky behavior of posting photos and text on social media is common and linked to personal use and its negative results. Reviewed challenges and its impact on current literature. Finally, discussed the prevention methods and recommendations regarding future research in social media and risk behaviors of college student. Jaroslav Bukovina, (2016) [7] examined economical and technical point of view of social media data. They presented an overview of research related to the connection between capital markets and social media. Theoretical reasoning of such connection is mainly defined to be a behavior, finances which enlarge the standard model of well-planned marketings and observes less rational factors like sentiments of investors as powerful pricing assets. Additionally the theoretical construction of communication mechanism and social media. They have summarized the main discovery in such field and defined the future challenges. Zhang, Zhiyong et al., (2016) [8] surveyed futurist network security of social media and reliability for an increased complication and variety of attacks and intelligence applications. The security and dependability issues became serious and need to be addressed urgently. The lack of examining an effective measurement for reliability and security of tools and applications of social media influences its evolution and improvement. They highlighted new direction for measuring fundamental platforms, hierarchical architectures based on crowd computing.
and signalling theory that is important for the social media ecosystem. Aizhan Tursunbayeva, (2017) [9] classified, appraised and captured an applicable proof from gray literature and 4 research databases. Out of 2441 effectively applicable results just 22 studies met inclusion criteria completely. The crossing in between health and social media received appreciable observation, without knowing how the health organizations of public sector utilize social media for e-Government. The humble evident is generally expressive and related to single field have a shortage of theoretical depth in segments of the e-Government research. A unique category of evaluation also emerged. The absence of strong proof makes it hard to extract results related to effectiveness of techniques in the health sector and additional research are required. The study of papers is summarized by defining the research gap of methods and techniques used for improvement and future work shown in table 1.

**Table 1. Summary of Literature Survey**

| Author               | Year | Technique | Gap                      |
|----------------------|------|-----------|--------------------------|
| Wajeb Gharibi        | 2012 | Use antivirus tools, Security tools, Strong authentication, Spreading awareness [3] | Security Threats Privacy Threats |
| Yongick Jeong        | 2017 | Structural Equation Modeling [4] | Generation Gap |
| Rakesh Singh Kunwar  | 2016 | Spamming Technique | Spamming Clickjacking Malicious Application |
| Gabrielle G. Groth   | 2017 | Investigation with social media, Using mixed methods, Experimental designs | Identifying Issues Self-reporting A privacy setting |
| Jaroslav Bukovina    | 2016 | Analysing Technique | Unstructured Data |
| Zhiyong Zhang        | 2016 | Network Security Methods | Security /Privacy Issue |
| Aizhan Tursunbayeva  | 2017 | Systematic Approach | Unstructured Data[9] |

The users are concerned with others’ posting than their own posting. The detailed description of major variables is shown in table 2.

**Table 2. Analysis of variables by SNS type [4]**

| Privacy concerns of posting types on facebook (n=216) | Mean | SD | Max | Min | Kurtosis | Skewness |
|------------------------------------------------------|------|----|-----|-----|----------|----------|
| Posting own timeline                                   | 4.43 | 2.19 | 7   | 1   | -1.31    | -.38     |
| Posting on other’s timeline                           | 4.26 | 2.04 | 7   | 1   | -1.15    | -.30     |
| Others posting on own timeline                        | 4.91 | 1.94 | 7   | 1   | -.54     | -.75     |
| Privacy concern My Tweets                             | 3.30 | 2.32 | 7   | 1   | 1.40     | .42      |
The table 3 indicates the remarkable difference between posting types on Facebook [4].

**Table 3.** Difference in perceived privacy concerns for Facebook posting activities

| SNS Format | Facebook** |
|------------|------------|
| My posting on own timeline Mean (SD) | 4.44 (2.20)\textsubscript{A} |
| My posting on others’ timeline Mean (SD) | 4.26 (2.05)\textsubscript{A} |
| Others’ posts on my timeline Mean (SD) | 4.91 (1.94)\textsubscript{B} |
| Wilks | .83 |
| F-value | 18.19 |
| Partial $n^2$ | .18 |

The table 4 indicates the notable difference among posting types on Facebook [4].

**Table 4.** The difference in perceived privacy concerns for twitter postings [4]

| SNS Format | Twitter*** |
|------------|------------|
| My tweets Mean (SD) | 3.29 (2.32)\textsubscript{B} |
| My retweets Mean (SD) | 3.17 (2.19)\textsubscript{AB} |
| Others’ retweets on my tweets Mean (SD) | 2.95 (2.16)\textsubscript{A} |
| Wilks | .95 |
| F-value | 4.66 |
| Partial $n^2$ | .05 |
3. Cyber Threats in Social Networking Websites

Social networking has changed the interaction manner in person and on the way to change professional life. It plays an important role in business, although it’s high at risk with unlimited users, more attackers get attracted in recent times [10]. Several social network risks considered in enterprises:

3.1 Social Networking Worms
As per researchers, Koobface is considered as “largest web 2.0 botnet”. The worm is particularly designed to grow beyond the social network (e.g., my space, hi5, Facebook, twitter, etc.) to engage more machine and seize more accounts for spamming.

3.2 Phishing bait
An e-mail attracts users to sign-in Facebook without picking on fbaction.net URL in browser. Several users had compromised their accounts in such act, but a significant number of users still exist. Facebook quickly acted to blacklist that domain, ensuing many copying efforts like fbstarter.com.

3.3 Trojans
Social networks are great carriers for Trojans like “click here” and you get a Zeus - a famous banking Trojan, responsible for high profile thefts and URL Zone – is smarter, that calculate the amount of victim’s accounts and decide the priority of theft.

3.4 Data leaks
Sharing is a major concept social networks work on. Several user shares a lot about projects, finances, scandals, product or other fragile information about organizations that leads to embarrassments or legal damages.

3.5 Shortened links
URL shortening services like: bit.ly or tinyurl to fit the lengthy URLs to short spaces. Obfuscated links are so apparent that it never dawns on victims that they’re clicking on malware install instead of their required link.

3.6 Advanced persistent threats
Key elements of APTs is to gather the knowledge of character like officers, executives for whom social networks is a stash of data. The offenders of APTs use knowledge to expand their threats and acquiring entry to fragile systems.

3.7 Cross-Site Request Forgery
It’s not a particular type of threat – like a method used to distribute an experienced worm, CSRF assault and utilizes the trust of the user in its browser. As long as the application does not examine the referrer header, it’s easy to attack “share” image in the event of the user to spread / catch the attack.

3.8 Impersonation
A different account of the individual with a number of followers were hacked. Various imitators gather a huge number of followers on twitter and later humiliate the individuals they are imitating. Twitter is now shutting down the imitators who attempts to defame their victims.

3.9 Privacy threats
Data from personal accounts are accessible for advertising targets, few users are active only exploits someone’s reputation with gossips and some concerns related to Facebook includes hacking, unnecessary contacts, stalking, id-theft and 3rd party accessing Facebook accounts [11]. Another confusing concept of disclosing the personal data, despite of being aware of the consequences [12].
Individuals may endanger their privacy, concerned to be left alone that is also known as FOMO (fear of missing out).

Social networks are a turning point, helping big or small businesses to locate and connect to their aiming markets. It has several pros and cons as discussed in table 5.

| Merits                                                                 | Demerits                                                                 |
|------------------------------------------------------------------------|--------------------------------------------------------------------------|
| Social networks are free to use and also useful for freelancers.        | It’s time consuming, as 2-way communication is required.                  |
| Online shopping makes lives easier and time saving.                    | It’s quick, scatter like wildfire. An inappropriate declaration can damage the reputation online. |
| It helps to be more responsive to clients, businesses.                  | Outputs take time to be obvious as social networks is not about advertising. |
| Social networks are useful in education, as students can explore the topics in detail | Cybercrime, proposes an increased threat to users.                         |
| It is accessible to everyone and replaces the modes of communication, almost everything is possible online. | Addiction to social network is a negative impact. People loose physical communication and interaction with the real world. |

The various benefits of social networking websites motivates the users to be spirited eg. A group of students disclosed that 5 basic requirements of internet user: building relationship, communication, interest, comfort and reputation can be satisfied with Facebook [13] and researchers observed that entertainment is a key motivator among students to use social networking [14] social connectivity is a motivation to use Facebook [15].

Privacy is considered as a power to be free from unnecessary disturbance and to maintain privacy, individuals follow synchronizing process to set the privacy levels [16]. Maintaining the privacy of relations can be fulfilled with control over access.

4. Application in Social Networking

Social networking has become a wide area for both social and business purposes. Social networking has become remarkable target in several fields as discussed below:

4.1 Social Networking Websites
These are internet based social media applications to stay in touch with family, friends, classmates, clients, etc. People used to share pictures, sending messages, videos to stay connected.

4.2 Business Applications
It is used in enterprises to connect with people at low cost. This could be useful for small businesses and entrepreneurs looking forward to expand their business. Since it is operated globally its latest trend of socializing with the public through advertisements and reviewing their opinions to improvise quality of products.
4.3 Dating Applications
Individuals communicate and sharing personal details internally to make relations, that can be long term, short term or one time relation. Using that information several dating apps as well as matrimonial site is available online, where users create their profile to communicate and meet the person of interest.

4.4 Finance Applications
Using virtual currency promotes the financial trades globally. Online sale, purchase of commodities is possible due to social networking.

4.5 Educational Applications
The majority of students explore the details of their relative topic online. Social networking supports the foster relationship between student and teacher by providing online classrooms, educational blogs, chat and discussion threads, etc. Content sharing and rating feature is available to these applications.

4.6 Medical and Health Applications
Social networking is also embraced by health care professionals to manage the institutional knowledge and highlight individual physician and practitioners. These applications appear to help its members with several mental and physical ailments. Sober Circles are created to help persons in recovery from addictions habits by communicating with each other which leads to the encouragement of others related to humans. Several groups concentrate on exercising and share their workout videos for others.

4.7 Political Applications
Currently social networking websites are used for social and political movements. Facebook, twitter plays a pivotal role in connecting people to the Egyptian evolution, where social websites used as a platform to people featuring related updates. In 2008, in Barrack Obama’s election campaign, social media was incorporated as a winning strategy.

4.8 Crowdsourcing Applications
It’s a platform for crowdsourcing like contests, charity functions, professional freelancing, fund raising startups which occurs offline also.

4.9 Reasons for using Social Media
Bertot et al.(2010) [17] framework used to classify the interactions of social media. By overlapping the types of crowdsourcing solution and co-produced along with public health services via comment, feedback suggestions on social media.

- **Transparency and accountability**
  It mainly includes Twitter, Facebook or YouTube to post data about the organization like: staff members, services, etc. to give updates of current activities, i.e. job openings, news, events, etc. to increase awareness of Open Data resources.

- **Democratic participation**
  It’s cited because public health organizations use social media as e-government. In Japanese studies it’s found that maximum number of online signatures for campaign to oppose reforms to reimbursement of regular medicines.

5. Mitigation Techniques to Address Social Media Security Threats
Risk mitigation is a technique of minimizing the influence of risk by deploying particular measures [18]. The number of unknown risks exists with usage of social media in organizations. Several methods can be used to prevent and minimize the security risks are as follows:
5.1 Developing social media acceptable use and security policy
To minimize the security risks in social media, some organizations have officially proposed a policy to guide the usage of social media sites. The policy consists of instructions which specifies the acceptable and objectionable consequences, regulatory or legal demands as per social media content, password policy, privacy settings, etc. [19, 20] Personal and professional profiles of employees should be separate and update passwords on a regular basis and should be unique for each platform.

5.2 Routine social media site monitoring
Monitoring social media existence of the organization is important. It’s necessary to track his conversations about organizing on the internet and respond appropriately. The corporation must scan the internet to locate the misuse of enterprise brand regularly. Site monitoring tools like: Google Alerts, social mention is able to track malicious activities against corporations. Such tools usually give RSS feeds and e-mail alerts to update corporation.

5.3 Monitoring employee internet activity
To ensure the acceptable use of social media and security policy, several companies monitor the login activity of employees. A research [21] disclosed that 68 percent companies scans the internet activities of employees out of which 56 percent blocks access to particular sites. Few restricted the login to famous websites at the work place. Intrusion detection system filter mischievous content, hinder the bad websites, prevents discharge of private data.

5.4 User education and training program
The security’s weakest link is human [22]. Accurate training and education raises the security awareness and responsibility against malware and data breaching. Detailed security awareness training is must that explains the company’s acceptable use of social media and security policy, genuine safety measures mitigates the threats and risks.

5.5 Software Update
Updated antivirus, firewalls and antispyware software must be deployed on every device used by employees. It’s important to perform regular scan for all devices as well as the downloaded file from e-mail, website or flash drive. Updating of operating system and applications (like pdf or flash) associated is required [23].

5.6 Archiving social media content
Several organizations work to preserve and capture the social media content for legal purpose. Certain tools like Symantec’s Enterprise Vault archiving software was created for companies to extract, capture and store the data posted by employees on social media. Archiving minimizes the risks in highly disputed or regulated firms like finance industry or health care [24].

5.7 Challenges and Limitations
The challenges involve defining scope of public health sector and differences between finance and health system structures to notify the purpose of exclusion and inclusion format. The variety of health organizations, out which some existing as such evident e.g., the study of food standards based on different definitions of different agencies. Study conducted in developed countries despite of international databases, like WHO, a unique review of social media use aspects of e-government exists in public, although they don’t classify as research [25]. Ample use of students is another limitation. Considering more approaches to capture evidence like reviews of innovative programs and expert consultations are necessary for further research.
6. Conclusion

The social network is a group of individual or organizations that share interests and ideas and making new friends, like networking groups. It helps people to stay connected with family and friends. Social networking has changed the interaction manner in person and on the way to change professional life. It plays an important role in business, although it’s high at risk with unlimited users, more attackers get attracted in recent times. Several social networks commonly used these days are Facebook, Twitter, Instagrams, etc. The study examined the multi-dimensional methods to explore the privacy concerns of posting behavior of one’s own network, expanding statistics to others’ network and general internet users. The study explored and suggested that privacy setting can be improved on the basis of users. Various cyber threats like social networking worms, phishing, trojans, data leaks, shortened links, impersonation, etc. To minimize the risk of such threats and attacks mitigating techniques like: site monitoring, security policies, educating users and software updates are the measures taken. Several future work includes extending current study and using non-students sample with different posting types and contributes to understanding the privacy on SNSs and various other factor effects privacy concerns. Users can determine the levels of concern and finally, survey of adult users shows the similarity awareness of observation techniques and privacy controls on the internet.

References

[1] Ellingwood, J. 2016 An introduction to big data concepts and terminology. Digital Ocean. Sep, 28.
[2] Fhom, H.S., 2015. Big Data: Opportunities and privacy challenges. arXiv preprint arXiv:1502.00823.
[3] Gharibi, W. and Shaabi, M., 2012. Cyber threats in social networking websites. arXiv preprint arXiv:1202.2420.
[4] Jeong, Y. and Kim, Y., 2017. Privacy concerns on social networking sites: Interplay among posting types, content, and audiences. Computers in Human Behavior, 69, pp.302-310.
[5] Kunwar, R.S. and Sharma, P., 2016, April. Social media: A new vector for cyber attack. In 2016 International Conference on Advances in Computing, Communication, & Automation (ICACCA)(Spring) (pp. 1-5). IEEE.
[6] Groth, G.G., Longo, L.M. and Martin, J.L., 2017. Social media and college student risk behaviors: A mini-review. Addictive behaviors, 65, pp.87-91.
[7] Bukovina, J., 2016. Social media big data and capital markets—An overview. Journal of Behavioral and Experimental Finance, 11, pp.18-26.
[8] Zhang, Z. and Gupta, B.B., 2018. Social media security and trustworthiness: overview and new direction. Future Generation Computer Systems, 86, pp.914-925.
[9] Tursunbayeva, A., Franco, M. and Pagliari, C., 2017. Use of social media for e-Government in the public health sector: A systematic review of published studies. Government Information Quarterly, 34(2), pp.270-282.
[10] Networks, Palo. 2017. "Top 10 Social Networking Threats". Network World. https://www.networkworld.com/article/2213704/collaboration-social/top-10-social-networking-threats.html.
[11] Debatin, B., Lovejoy, J.P., Horn, A.K. and Hughes, B.N., 2009. Facebook and online privacy: Attitudes, behaviors, and unintended consequences. Journal of computer-mediated communication, 15(1), pp.83-108.
[12] Blatterer, H., 2010. Social networking, privacy, and the pursuit of visibility. In Modern Privacy (pp. 73-87). Palgrave Macmillan, London.
[13] Urista, M.A., Dong, Q. and Day, K.D., 2009. Explaining why young adults use MySpace and Facebook through uses and gratifications theory. Human Communication, 12(2), pp.215-229.
[14] Ezumah, B.A., 2013. College students' use of social media: Site preferences, uses and gratifications theory revisited. *International Journal of Business and Social Science*, 4(5).

[15] Alloway, T.P. and Alloway, R.G., 2012. The impact of engagement with social networking sites (SNSs) on cognitive skills. *Computers in Human Behavior*, 28(5), pp.1748-1754.

[16] Zlatolas, L.N., Welzer, T., Heričko, M. and Hölbl, M., 2015. Privacy antecedents for SNS self-disclosure: The case of Facebook. *Computers in Human Behavior*, 45, pp.158-167.

[17] Jaeger, P.T. and Munson, S., 2010. Engaging the public in open government: Social media technology and policy for government transparency. *Federal register*, 1, pp.1-18.

[18] Saha, I. and Paul, B., 2019. Private sector involvement envisaged in the National Strategic Plan for Tuberculosis Elimination 2017–2025: Can Tuberculosis Health Action Learning Initiative model act as a road map?. *medical journal armed forces india*, 75(1), pp.25-27.

[19] Chi, M. and Wanner, R., 2011. Security policy and social media use. *Reducing the Risk of Social Media to Your Organizations*. Retrieved January, 18, p.88.

[20] Delerue, H. and He, W., 2012. A review of social media security risks and mitigation techniques. *Journal of Systems and Information Technology*.

[21] Boorsma, B. and Mitchell, S., 2011. Work-Life Innovation. *Smart Work–A Paradigm Shift Transforming: How, Where, and When Work Gets Done*, Cisco Internet Business Solutions Group (IBSG) on https://www.cisco.com/web/about/ac79/docs/ps/Work-Life_Innovation_Smart_Work.pdf.

[22] Vroom, C. and Von Solms, R., 2004. Towards information security behavioural compliance. *Computers & security*, 23(3), pp.191-198.

[23] Patel, N. and Jasani, H., 2010. Social media security policies: Guidelines for organizations. *Issues in Information Systems*, 11(1), pp.628-634.

[24] “Symantec enterprise vault 10 reduces the risks of using social media tools for business”, available at: www.symantec.com/about/news/release/article.jsp?prid¼20110801_02.

[25] Holeman, I., Cookson, T.P. and Pagliari, C., 2016. Digital technology for health sector governance in low and middle income countries: a scoping review. *Journal of global health*, 6(2).