Research Paper: Social Media- Security Risks and Mitigation Techniques -MSc-Cyber Security

SRI LANKA INSTITUE OF INFROMATION TECHNOLOGY Malabe, Sri Lanka
ms19802640@my.sliit.lk

Bakeer Hassan

April 22 2020

1 Abstract

In today's digital and socio- economic development one of the leading and fastest that taking place in the modern world is the "Internet". The continual grow of cyber-attacks to the digital world has been past decade which poses serious threat to the Digital technology of the world. The assignment/research will focus on threats of cyber security for Social Media/Social Networking sites (SNS), however the social medial assumption among the business and individuals play a significant role or sky rocketing. Social medial sites include many areas such as social brandings, digital marketing and e-commerce and the real scenarios is that most of the users are unaware of the risks and lack of knowledge which may be still potential risks ,where it could lead further for cyber-crime. Following issues and risks will be addressed in the paper. Security issues and challenges in the SNS (such as third-party application-threat, identity theft, phishing attacks, and Malware) will be addressed/discussed and this chapter gives summary of the privacy and social media security issues and also demonstrates the different types of security risks and proper mechanisms to protect those risks .In addition, the chapter explains common technique or strategy, where attacker used most often and security measure against the risks. Emphasizing the government's efforts to curb this serious problem, the document also proposes appropriate solutions that can be recognized by individual users and the digital cybernetic world of government and private sector cooperation to have Cyber Safe digital world (Rituparna Das1, 2017).

2 Introduction

Online social media has become one of significant among the world where it has been used nearly millions of people in order to get to know each other online on social networking sites. However, on social network sites, people's daily tasks, real market connections, backgrounds. Many people in the most popular social network sites like Instagram, Google+, Facebook, and Twitter are concerned about the social networking sites. (L.S.Y. Dehigaspege, 2016).In modern era of computers and Smartphones the internet made the remarkable changes to the communication. Due to absence of security, numerous cyber-crimes have occurred during the past era. Cyber security involves an important role in the present growth of services and information technology. Cyber security is consequently user try keep the professional and personals information from attack on the social media/internet. The importance of cyber security is to protect computers, network, losses and programs/tools to be used as unauthorized access. Many users are lack of knowledge about the risks related to internet and use to share the information that makes more vulnerable for cyber-attack. (Rituparna Das1, Cyber Security for Social Networking Sites: Issues,, 2017).

3 Literature Review

Social network sites are growing and more research paper are published.Some include links to social security issues known to social networking sites, cybercrime on social networking sites and potentials risks."M.Shaabi and W.Gharibi (2015)", mentioned various social network sites to investigate cyber -bullying on social network sites. Some of the discussions on paper on social networking sites such as Facebook, Classmate, Myspace, and Flicker and so on have been discussed. Additionally, the impact of social networking websites, privacy and security issues also have been aggravated/highlighted with the privacy and safety risks they encounter on social network sites, the strategy on anti- disasters and with development of the tools which can be used to deal with spies, Trojan horse, hijackers, viruses and other malicious software. So, the research is about the nature of future development for cybercrime [1] (Singh*2, 2017).

A.Alam and R.Jabe, (2016), Done a survey for identifying end user's awareness for security and privacy issues which used to take place in the social network sites. The research/survey will mainly focus on primarily on Facebook social networking platform and the study will not only focus or discuss the user's perception that relates to security and privacy issues but also presented the perception of enhancing the default privacy setting which has been presented by the Facebook, therefore the prevention and reduction in the cybercrime/attacks can be succeeded. It has been noticed that users are not aware about the privacy setting and do not like to modify the default settings. However, it has been decided that users should aware about the default settings and must change/modify, where the users would not be fallen as a prey for security breaches and moreover preventing from security breaches the Facebook must

pay an attention regarding safety settings[2]. (Singh*2, 2017).

A.Verma et al. [22], recommend a distributed/circulated and decentralized architecture which provide security and privacy for social networking users and it is an enhanced security and privacy by the technique of cryptography RSA-"Random Sequence Algorithm" and digital signature."Yabing Liu,et al(2011)", brought up suggestion to improve the default and to provide advanced tools in order to protects and privacy. However, the full scope of the privacy requirement is unknown, and there are times when privacy issues are encountered or problems faced by users.(Roshan Jabee, 2016).

L.S.Y. Dehigaspege, et al. [2016], discussed highly secured mechanisms methods which used to prevent users from cyber-attacks and threats on social networking platform. But this method is entirely different from above suggested research paper where this researcher has done based on algorithm which uses a recognition of voice system for end users where it permits users to login based on the voice. The system location identification system and also it includes CAPTCHA program as well in the algorithm, therefore the main advantage among users and the bots is possible and main theme of the study is to provide the secure verification algorithm in order to secure the social networking platform [8]. (Singh*2, 2017). Gunatilaka et al. [8], has done a research and distributed a report which mentioned about the rapid growing site of people towards social networking sites and it has become a significant target for cyber-attacks and also no any social bridge or relation among end users, but still users used share sensitive and personal information on social sites, therefore this becomes vulnerable for attacker to get more easy to do attack on target end user based on information collected. But various sites try to avoid this kind of misuses or attacks; however the attackers still has the potential to overcome the security measure even accomplished and contains threats and issues which include investigation on different security and privacy issues in social networking platform. The issues accomplished such as identity theft, privacy risks, phishing, hacking, physical threat malware attacks and spamming. (Roshan Jabee, 2016).

Warren and Leitch [12], presented in the report that personal and privacy information can be attained any time if there is any sort of weakness that vulnerable through internet, where user used to share feelings, massage and any sensitive information and it also has many security problems within the online platform based security vulnerabilities which are associated to the domain. (Roshan Jabee, 2016)."Cases ad Pesce [9]", stated that end user of social platform used to share the information knowing and unknowingly which can be personal and sensitive information, where it could lead to major disaster of cyber-crime and information such as photos, private information and every action of life activities are being post to the social networking sites, therefore this becomes of one the privacy concern. New privacy setting to keep secret to confidential users' secret and to set up tagging on social networks. (Roshan Jabee, 2016).

Chewe et al. [1], paid more attention towards personal information and how it is being affected in terms of social media and internet, however further,

discussed on how the privacy leads to risks and what are the security strategy measures can be implemented in order to prevent security breaches and but further, it has been highlighted security risk on social platform and the threats which make the user vulnerable for cyber -crime. Therefore, finally suggested some of security measure and best practices to stay away from cyber-attacks on Social network. (Roshan Jabee, 2016). Dhar and Gangopdhyay [7], have distributed survey which states that social network platform targeting towards teenagers and make an opportunities to stay connected with known and strange people, therefore this make friends with people with strange people and adding details to their friends can be a spectacular or visible subject. But have to consider about the sort of extent level the personal information is secured or disclosure to other party and further, focused on security perimeter which has been setup by social networking platform such as Twitter, Facebook, MySpace and Orkut etc. (Roshan Jabee, 2016).

Security Risks:

Social Network worms: includes the social network Koobface, which researchers say is the "largest Web 2.0 botnet." Although it contradicts the idea of a multi-faceted "worm" such as Koobface, it is specifically premeditated to spread across social networks (eg Facebook, MySpace, Twitter, Hi5 and Bebo), machines to attract and steal more and more robots. More accounts to create more spam mail. Always make money through regular robots, including Russian intelligence and dating services.

Phishing: Remember the FB action? Would please not receive an email that will reach your browser's Facebook, fbaction.net URL? Most Facebook users' accounts are down, this is only a "small percentage" and when you realize that there are over 350 million Facebook users, there are still a large number left. According to Credit, Facebook tried to get a list of this domain quickly, but tried hard (for example, fbstarter.com). Since then, Facebook has had a lot of experience.

Data Leaks: All social networks are connected. Unluckily, many users share a lot about the business - projects, products, financing, organizational changes, stigma, or other sensitive information. Even husbands sometimes share how long they have worked for another secret plan and many details about this plan are being discussed. The problems that arise are shameful, harmful, and legal.

Advanced persistent threats: One of the main aspects of APT is the collection of data from stakeholders (for example, managers, supervisors and veterans). Because social networks can be an information store. APT criminals use this information to increase their risk - to gather more intelligence (e.g., malware and Trojans) and then access sensitive systems. So while not directly involved in APT, social networks are a source of information. Less nonsense, but less important for an individual, so more active criminals may be given a chance.

Cross-Site Request Forgery (CSRF): This is not a specific threat - it is similar to the technology used to propagate advanced social network worms and uses the trust of a social network application in a user's browser, as evidenced

by CSRF attacks. If the router title is not checked by the social networking app, it is easy for the attacker to "share" a picture of an event that other users can click on.

Mitigation techniques:

Security Policy-(Social Medial Acceptable Policy and Security): Many organizations have been set up to guide employees on social security risks, how to use social media. Official policies typically apply to social media, data processing, distribution, the results of a mint agreement, legal or regulatory requirements for social media content, browser and company support configurations, privacy settings, password policy, and more. . (Ch, 20; Sophos, 23; Klavitt et al., 20).

Social Media Monitoring: It is important to be a social media monitoring company. It is important to know that the companies they designate and the organizations associated with them must constantly verify the use and research of the brand of the enterprise. (CDC, 2009).

User Education and training: Studies have shown that human communication is the weakest line of security (Curry, 23; Var and Aun Souls, 23). There should be proper consumer education and training to increase security awareness and increase personal responsibility to prevent security incidents on social media, such as leaking malicious programs and data breaches (Chi, 2011; Federal CIO Council, 2009).

Developing Social Medial Incident notification and Response Plan: Whatever the security measures, there are still threats on social media. Thus, in order to reduce or mitigate the negative impact of an accident, the organization must be informed of the social media event and the response plan for its development. A good report on a social media event and response plan includes information about the event, passwords, data leaks, data breaches, lending, viruses / malware, and more.

Software Update: Companies must ensure that the latest antivirus and antivirus software is installed on employees computers and all devices used by them (Chi, 2011). It is important for employees to understand the importance of constantly reviewing any work that you download from not only their computer / device, but also their website, email, or gray drive.

Conclusion It is an essential to consider about the growing site of Social medial/Networking sites however, it has become a significant target for Cyber-attack. Cyber-crime taking widespread and posturing biggest threats to the economic security and national levels such as public and private institutions, defense, telecommunication and technology and financial factors are under risks of cyber-attack. Therefore it very important for the organization takes right security mechanisms to protect from cyber-crime and user should aware in order to protect personal.In all studies, social networks are a security risk and privacy concerns. These disasters, in fact, are in their central architecture, and the hijacker can use it with all their personal information, and how to use the privacy settings appropriately to improve the community online. Additionally, many people, especially in their teens, have a great deal of confidence in other people and seeing a great deal about their identity on the Internet. This can only

be achieved by technical means or guidance has to investigate any information that is not secure by social media, and it should tell that what should not transfer any sensitive information through social networks. The load is often wise for what the user is doing online. But more advanced education and some structural changes can be used more securely for social networks. Education is a big, big part. Sometimes people need to remember things when they start to be negligent. Finally, the Research found that the survey was needed to make users more secure on social networks and some of security measure and best practices have mentioned on this paper to keep safe away from cyber-crime while online.

References

[1] Das, R. (2017). Cyber Security for Social Networking Sites: Issues, Challenges and Solutions. International Journal for Research in Applied Science and Engineering Technology, [online] V (IV), pp.833-838. Available at: https://www.researchgate.net/publication/316497540$_{C}yber_{S}ecurity_{f}or_{S}ocial_{N}etworking_{S}ites_{I}ssues_{C}hal$

[2] Ijsrp.org. (2016). Secure Authentication: Defending Social Networks from Cyber Attacks Using Voice Recognition. [online] Available at: http://www.ijsrp.org/research-paper-1016/ijsrp-p5820.pdf

[3] Jabee, R. and Afshar, M. (2016). Issues and Challenges of Cyber Security for Social Networking Sites (Facebook). International Journal of Computer Applications, [online] 144(3), pp.36-40. Available at: https://pdfs.semanticscholar.org/b501/886f966f8cd7e471

[4] kundoc.com. (2017). Social network security: Issues, challenges, threats, and solutions - PDF Free Download. [online] Available at: https://kundoc.com/pdf-social-network-security-issues-challenges-threats-and-solutions-.html .

[6] M. Sreenu1, Dr V, Krishna, A. and Nayak.N3, D. (2017). A General Study on Cyber-Attacks on Social Networks. [online] Iosrjournals.org. Available at: http://www.iosrjournals.org/iosr-jce/papers/Vol19-issue5/Version-5/A1905050104.pdf

[7] Microfocus.com. (2017). Best Practices for Social Media Archiving and Security. [online] Available at: https://www.microfocus.com/media/white-paper/best$_{p}ractices_{f}or_{s}ocial_{m}edia_{a}rchiving_{a}nd_{s}ecurity_{w}p.pdf$

[8] Norman, A., Hamid, S., Hanifa, M. and Tamrin, S. (2017). Security Threats and Techniques in Social Networking Sites: A Systematic Literature Review. In: Future Technologies Conference (FTC). Vancouver, Canada: Future Technologies Conference (FTC), p.20.

[9] The Social Side of 'Cyber Power'? Social Media and Cyber Operations. (2016). In: 2016 8th International Conference on Cyber Conflict Cyber Power. 2016: The Social Side of 'Cyber Power'? Social Media and Cyber Operations, p.13.

[10] Thesai.org. (2016). Role of Security in Social Networking. [online] Available at: http://thesai.org/Downloads/Volume7No2/Paper$_{2}-Role_{o}f_{S}ecurity_{i}n_{S}ocial_{N}etworking.pdf$

[11] Jabee, R. and Alam, M. (2016). Issues and Challenges of Cyber Security for Social Networking Sites (Facebook). International Journal of Computer Applications (0975 – 8887), 144(3), p.5.

[12] Norman, A., Hamid, S., Hanifa, M. and Tamrin, S. (2017). Security Threats and Techniques in Social Networking Sites. Future Technologies Conference (FTC), p.20.

[13] Singh, A. and Singh, A. (2017). Review of Cyber Threats in Social Networking Websites. International Journal of Advanced Research in Computer Science, 8(5), p.5.

[14] Suleman, M. and Anees, T. (2018). Threats All Around –An approach towards enhancing User Privacy on Online Social Networks. [Online] Paper.ijcsns.org. Available at:http://paper.ijcsns.org/07$_b$*ook*/201809/20180903.*pdf*

[15] Wani, M. and Jabin, S. (2017). Online Social Networks - Representation and Analysis. International Journal of Innovations Advancement in Computer Science IJIACS, 6(7), p.7.