International Journal of Enhanced Research in Management & Computer Applications, ISSN: 2319-7471
Vol. 3 Issue 12, December-2014, pp: (1-4), Impact Factor: 1.296, Available online at: www.erpublications.com

Security Threats of Social Networking Sites: An Analytical Approach

Arpita Banerjee[1], C. Banerjee[2], Dr. Ajeet Singh Poonia[3]
[1]Assistant Professor, St. Xavier's College, Jaipur, Rajasthan, India
[2]Assistant Professor, Amity Institute of Info. Technology, Amity University, Rajasthan, India
[3]Associate Professor, Govt. College of Engineering & Technology, Rajasthan, India

Abstract: Social networking is gaining prevalence in our society. Popularity of some of the social networking sites like facebook, twitter, skype etc. has increased at astounding level. It is not only popular in young generation but can be used by all the section of the society to fulfill their need like job searches, sources to increase their revenue, tool to make the users aware of safety rules and security policies. Most importantly, they are being used as a way to relink with old and distant friends. But, as with any new application, it is always important to keep a thorough understanding of its security impact. Each of these networking sites consist of their own security mechanism which if not followed properly can lead to personal data or information and resource at risk thereby resulting in financial loses. In the new age, identity theft, spamming, eavesdropping, malware attacks, viruses, phishing, information leakage, etc. are threats to the privacy of people. Because of such privacy issues interest of a lot of users turns down towards these social networking giants. These challenges impose several new research questions to the research community with regards to security. The purpose of this research paper is to make people aware about breaches on social networking websites. This research paper states a comparative study on the security issues being faced by various social networking websites.

Keywords: Social Networking, Security, Breaches, Security Threats, Software Security, Security Awareness.

I. INTRODUCTION

The commencement of the Internet has given rise to many forms of online sociality, including e-mail, Usenet, news groups, instant messaging, blogging, and online dating services, etc. among all these one thing that is gaining popularity with a rapid speed is the use of Social Networking Sites (SNSs). SNSs are eminent sources of recreation primarily for the youth. In fact these social networks have become an inherent part of today's Internet [1].

They allow sharing of the information (whether personal or professional) with people who may be, old friends or strangers. Some of the popular social networking sites are facebook, twitter, skype in India, Orkut in Brazil, VKontakte in Russia, or Mixi in Japan etc. among them Facebook is the most causal website. As many friends as one wish to have can be created using these social networking sites [2].

It helps one to be in touch with some of the old friends from high school, etc.In a similar fashion, Twitter and LinkedIn are generally used for networking with professional commitments. These social networking sites provides a good platform for exchange of ideas, professional commitment etc. They further allow the user to add connections and create followers. It has become a part of one's daily life as it is aneconomical and easy way to beconnected with friends and relatives and even unknown persons [3].

It helps one not only to facilitate data sharing but also sharing of emotions[4].The online networks deliver substantial advantages to both the individuals and the business sectors. As one of the main aims of social networks is to find people of similar taste and likes, it is almost provided by all major networking sites. SNSs allow the users to search for local friends by restricting the query to a single town, for co-workers by searching for a company name, or for like-minded people [5].

Some of the remarkable benefits of online social networks are as follows:

- Assist the people to stay linked with each other very easily and efficiently, even on a universal level.
- It helps the people of similar interest to virtually interact among each other.
- Provide an environment and medium for new approaches and channels of online relationship, education, experience-sharing and formation of mutual trust.

- In the business sector, a well-made SNS can boost the company's communal knowledge and can enhance the goodwill of the company in the market engaging a broad range of people to be the part and parcel of the company's strategic planning process [6].

In spite of having many advantages of SNSs, some companies are thinking of blocking the access to social networks completely instead of conversing with their employees and making them aware of the risks.The reason being the security and the access control mechanisms of SNSs are relatively weak. Instead of adopting negative thinking patterns, organization should develop effective awareness [7] and training program [8] to educate their employees about the various threats, risks, counter measures associated with security risk [9]. Further they should also be made aware about the security policies, standards and protocols that they need to know related to cyber security [10] [11].

The security of these sites is weak because they are not designed keeping security and privacy as the prime facet of SNSs. So it becomes difficult for the administrator to check users from visiting social networks from laptops or smart phone while they are in office, home or anywhere else. Therefore along with benefits some security and privacy issues are also being included in many SNSs [6]. Further, 21 rules of software security need to be followed while designing and developing SNSs as it ensures implementation of adequate security [12].

The rest of the paper is organized as follows: ThThe section II describes some of the social networking sites threats, whereas in Section III, states the security measures. Conclusion and future work is drawn and reported in Section IV.

II. THREATS OF SOCIAL NETWORKING SITES

There are a wide variety of threats causing harm to social network a brief description of some of these threats are stated below:

A. Baits: Image destroying can also be done through many search engine optimization techniques. In this mechanism keywords are used to make links and on this basis ranking of sites are done. Maximum social networks permit people to see what is stylish and hot at the moment. For example, Twitter lists the top trending topics on its home page which makes it easily available for attackers, who automatically take hot keywords and include them in their spam messages to get a better listing. Some attackers even started manipulating Twitter messages before forwarding. The attackers generally search for those messages that contain hot keywords [5] [16].

B. Follower scams: With the rapid growth of importance of social networks people are more stressed to get people as more friends or followers as possible. In some social groups, acceptance of any person as a member of that group generally depends on his or her number of social connections. Generally school going students and college students are fascinated about it —the more online friends you have, the more popular you are.

Some fake websites also offers the visitor free services like providing new followers to themfor which you need to give them your user id and password.Obviously it is a bad idea to share your password with strangers, since you cannot control what will be done with your account. In most cases it is also against the terms and conditions of the social network [13] [16].

C. Impersonation of celebrities and friends: Many times, fake profiles of celebrities are seen on various social networks. Unfortunately there is no policy for stopping someone from registering a new account under the name of a celebrity or any one and similarly there are no policies for using a publicly available photo as a profile picture. In fact there arenot real authentication that links a virtual profile to a real-life identity. Thus as long as the posted messages sound reliable people will think it is the official account.

This type of fake account can then be used to spread fabricated information and rumors or to attract new followers that can later be spammed. Sometimes phishing attacks and local information-stealing Trojans are currently the most common causes of stealing personal information. Once an attacker obtains the password of any account he can manipulate the personal and professional information of that account holder and update the profile status.

These update messages often include links to other malicious sites in order to get more account passwords. As the message seems to come from a friend's account people tend to trust it. This inherent trust, and the usual curiosity, leads to a high click rate on those malicious links, making the attacks very successful [14] [16].

D. Koobface: The W32.Koobface worm has been one of the first large malware attacks, targeting social networks for years, and it is still wide-spread and active today. It is very successful as it uses clever social engineering attacks and counts on the link-opening behavior of social media users [15] 16].

E. Phishing: It should come as no surprise that since social networking sites use user name and passwords for logging in, those services are also susceptible to phishing attacks. Just like with phishing attacks on banks, social networking phishing comes in many different flavors. Currently the amount of phishing lures for community sites is relatively low at 3%, when compared to 78% targeting the financial sector.

This clearly is because the profits for phished bank accounts are much higher. In addition, the creation of dummy accounts on social networks is rather simple and can be used to generate accounts for spamming [15] [16].

F. Advanced fee scams: By design, social communities are an interesting target field for advanced fee scams, also referred to as 419 scams. Since people willingly disclose a lot of private information, a scammer can easy identify possible victims that will fall for the scam and adjust the motives that the chosen social engineering trick will exploit.

These types of scams typically come with a nice matching story that will present the victim some enormous benefit with apparently no strings attached. Later the scammer will inform the user about some unforeseen problem and will need a small amount to be paid up front. After the money is paid the attacker disappears, along with the promised benefits [16].

III. SECURITY MEASURES RECOMMENDATIONS

Some of the recommended key take-away strategies for avoiding the threats associated with the online social networks are described below [6][17][19]:

- Awareness about disclosing personal information on social networks.Users need to be more conscious about the information they reveal through their personal profiles in online social networks.
- Role of Government in raising awareness: Government should initiate different educational and awareness-raising campaigns to inform the users to make the rational usage of the Social Networking Sites as well as to encourage the providers to develop and practice security conscious corporate policies [6].
- Restructuring and reframing security policies and framework: The existing legislation may need to be modified or extended due to the introduction of some issues like the legal position of image tagging by the third person which are not addressed by the current version. As a result, the regulatory framework governing SNSs should be reviewed and revised as itrequires.
- Strong and dedicated membership: The strength of authentication method varies from SNS to SNS. However, in order to avoid fake and troublesome memberships, the authentication mechanism need to be further strengthen.
- The people who are regular visitors of these SNSs should be good users of the most powerful antivirus tools with regular updates and must keep the appropriate default setting, so that the antivirus tools could work more effectively**.**
- Information of setting default privacy and security preferences: Since most of the users are not aware of the necessity for changing the default privacy preference [6] [17] it is essential to set the default setting as safe as possible.
- Making available proper and authenticated security tools: Providers also need to offer the following strategies for better user control on different privacy and security related issues [17].
- Government with support of educational institution can provide various security awareness raising programs [18].
- Cyber security should be made a part of school and college syllabus [18].
- The prevailing security policies needs to be rebuild and re constituted according to the current types of attacks and threat [18].

IV CONCLUSION

While SNSs offer progressive tools of interaction and communication, they also promote new challenges regarding privacy and security concerns. In this paper, we have briefly defined some major characteristics and benefits of social networking sites that have made internet as one of the most popular technology of present era. Our paper also did a comparative analysis of critical security threats of these social networking sites.

Finally, some recommendations are being made for enhancing the security issues and aspects of SNSs' to ensure user benefits from the social network sites rather than dissatisfaction from its downsides. If these sites are not cautiously and vigilantly used with their security aspects, they can become the most dangerous and powerful tools for the hacker to interrupt the personal as well as professional life of the users. A well-informed user will not only help to maintain security, but will also educate others on these issues and establish best practices which can be standardized and updated as applications mature or as new applications come along.

REFERENCES

[1]. Dinerman, B. (2011).Social networking and security risks. white paper, GFI software.
[2]. Giles Hogben, Social Networking - Security at The Digital Cocktail Party, Terena Network Conference 2008 [Online] retrieved on 26th Nov, 2014 from http://tnc2008.terena.org/schedule/presentations/show00ae.html?pres_id=7
[3]. Next Generation Electronic Identity - eID beyond PKI. [Online] http://www. enisa.europa.eu/pages/ eID/ eID_ws2007.htm.
[4]. Stan Schroeder, 20 Ways To Aggregate Your Social Networking Profiles. [Online] http://mashable.com/2007/07/17/social-network- aggregators
[5]. Acquisti, A., & Gross, R. (2006, January). Imagined communities: Awareness, information sharing, and privacy on the Facebook. In Privacy enhancing technologies (pp. 36-58).Springer Berlin Heidelberg.
[6]. Al Hasib, A. (2009).Threats of online social networks. IJCSNS International Journal of Computer Science and Network Security, 9(11), 288-93.
[7]. Banerjee, C., &Pandey, S. K. (2010). Research on software security awareness: problems and prospects. ACM SIGSOFT Software Engineering Notes, 35(5), 1-5.
[8]. Banerjee C., Banerjee Arpita, PandeyS. K. (2013): Software Security Awareness: Comparison of Artifacts Based Awareness Tools and Techniques.SGVU Journal of Engineering & Technology, 1(1), 33-38
[9]. Banerjee, A. B., &Murarka, P. D. (2013). An Improvised Software Security Awareness Model. International Journal of Information, Communication and Computing Technology, 1(2), 43-48.
[10]. Banerjee C., MurarkaP D, Banerjee Arpita (2013). IT Security Practices in an Organisation: Balancing Technology and Management Perspective.IMPETUS an Interdisciplinary Research Journal.2(1).1-6.
[11]. Banerjee Arpita, Banerjee C. (2014). Cyber Security Awareness Through Education: Problems and Prospects. IMPETUS an Interdisciplinary Research Journal.2(1).
[12]. Banerjee, C., &Pandey, S. K. (2009). Software Security Rules, SDLC Perspective. arXiv preprint arXiv:0911.0494.
[13]. Boyd, D. (2003, October). Reflections on friendster, trust and intimacy.InIntimate (Ubiquitous) Computing Workshop-Ubicomp (pp. 12-15).
[14]. Boyd, D. M. (2004).Friendster and publicly articulated social networking.
[15]. Chen, Y., Roussev, V., Richard III, G., &Gao, Y. (2005). Content-based image retrieval for digital forensics.In Advances in Digital Forensics (pp. 271-282).Springer US.
[16]. Candid Wüest. The Risks of Social Networking. Symantec [Online] http://www.symantec.com/ content/en/us/ enterprise /media/ security_response/whitepapers/the_risks_of_social_networking.pdf
[17]. Ellison, N. B., Steinfield, C., & Lampe, C. (2007). The benefits of Facebook "friends:" Social capital and college students' use of online social network sites.Journal of Computer-Mediated Communication, 12(4), 1143-1168.
[18]. Al Mushayt, O. S. (2013). Threats and Anti-threats Strategies for Social Networking Websites. International Journal of Computer Networks and Communications (IJCNC)Vol, 5.[19] Kim, W., Jeong, O. R., & Lee, S. W. (2010). On social Web sites. Information Systems, 35(2), 215-236.