Comparative Study of Security Risk in Social Networking and Awareness to Individual

Tosal Bhalodia, Chandani Kathad and Keyur Zala

Abstract Nowadays, social networking sites are very greatly used and are continuously growing at its peak. The extraordinary use of all the social networking sites mainly Facebook, Twitter, LinkedIn, and Google Plus involve huge amount of data transferred to public daily. This data transfer involves public information such as personal information, education, professional, etc. which leads to security at personal level. Let us see the comparative study of Facebook, Twitter, LinkedIn, and Google Plus for security risk and how effective it is for well-being to society.

Keywords Social · Facebook · Twitter · Gplus · Linkedin · Security
Public · Private · Government regulation · Information · Security
Optimization security measures · Vulnerability

1 Introduction

Social networking implementation explores the way to communicate in public, and this leads to sharing of information to known and unknowns. Implementation of any tool to live involves great amount of security involvement and needs to concern about risk of personal/company data. Of above four social networking sites mentioned, Facebook and Gplus are very informal and easy to use for all the public. Linkedin and Twitter are very professional and generally used for connection to CEO's and other related professional users. Twitter creates followers and makes connection through users following.

T. Bhalodia (✉)
Atmiya Institute of Technology & Science, Rajkot, India
e-mail: tosalbhalodia@gmail.com

C. Kathad · K. Zala
Ilaxo.Com, Rajkot, India
e-mail: kathadchandni@gmail.com

K. Zala
e-mail: keyurzala2010@gmail.com

M. U. Bokhari et al. (eds.), *Cyber Security*, Advances in Intelligent Systems
and Computing 729, https://doi.org/10.1007/978-981-10-8536-9_21

Business nowadays depends on information system. But due to vulnerability, the enterprise information system is under the attack of viruses and hackers which causes great loss to organization on reputation, information leakage, etc. Information security awareness is very important for each and every individual [5]. This awareness mainly needs to implement in all the universities in form of information security subject. This leads to educate the individual about the threat occurred due to social networking attacks. Malicious software, hacking tutorials, and other resources intended to help conduct cybercrime can be commonly found within hacker communities, often available for free or traded within black markets [9].

1.1 Facebook/GPlus

There are main three usual features for Facebook like capability to adding friends, to change or modify status, and last one is implement application for execution applications such as games and quizzes. A "Friend" means anyone on the Facebook system whom you allow to see very different levels of personal and public information, such as comments, birth date, jobs, photos, member of groups, and list of other friends and relatives. An individual can play games online and update others in day-to-day life.

Everyone can also notice friend's friend, i.e., individuals, whom you have officially became friend and may not met before, may have visualization keen on everyone's private situations and information.

There is update field which is at the pinnacle of the everyone's Facebook, but the main use of that field is that it allows the abuser to place anything similar to snippet as regards several topics at any point. It has very parallel field, although it does not agree to extra passage, and LinkedIn is not allowed for connecting associations/images/videos with the keep posted. A little example of every user's update is posted by your any social networking site like Facebook friend. These all are extremely classic:

- "Presently established a plane ticket proffer."
- "Someone is tired of every one this cold winter."

Even though that strength looks comparatively undamaging, the third position could raise a little be anxious. Every user can tell all their friends and connected links, i.e., all of your friends, which we do not be there at home used for a half year [12]. This is like to attaching an indication on the main road and infusing something.

Although the applications on social network may seem to be safe, along with in actuality a good number probably it is safe and harmless, it is forever something that can send harmful content to your computer/laptops. It is not right just to Facebook, but there are same as like Facebook, additional social networking sites which are associated with the Internet in universal situation, when you start downloading the web form or opening documents in email communications. So, you need to make sure that every user's computer has a correct and efficient antivirus or firewall, which means updated antivirus and install or run antivirus software if all are starting from a trust resource or accepted by the admin or group of IT department.

1.2 Twitter

It is a live application like to Facebook and LinkedIn which allows you to post comments which we say these days to tweet on some topics. Special users on the network of Twitter can grow to be supporters of someone's tweets related, like everyone can receive the updates regarding the data or information which are sent by them.

Study over the business ecosystems in Hungary by monitoring 6000 out of 20,000 Facebook users who publically displayed their employers. Then, they represented the complexity of connections graphically through a simulator. Also, they transformed the overall graphical network into a relationship graph of employers. If individuals are very related to each other in the network, then there is strong bonding in relationship with each other. Making progress to the same framework, Neunerdt et al. [3] proposed two algorithms for collecting and processing web comments in context of social blogging. Agarwal [1] proposed his extraordinary research work on "Prediction of Trends in Online Social Networks". He expended the "directed links of following" in the social media of Twitter to determine the flow of information. This approach directed a user's influence on others users that could decide if the topic is stylish or viral in the social networking world.

1.3 LinkedIn

If user can utilize Facebook, LinkedIn, Gplus, Twitter, or else some other online site for social networking, Internet banking or daily purchases, you must be responsive of messages and emails which are argued to be since these sites but actually the tricks may contain nasty content. I have received many emails that claim to be from my personal bank, but they are actually sent by a spammer. Spammers are there in the hopes of obtaining my users user id and password. Claiming of emails of Twitter and Facebook invitations is now most common. Emails and messages may still contain an attach RAR file or ZIP file that recipients may use to unlock to observe which user is invited them and made a flow to open the file. The attachment actually contains a worm; it may destroy the entire user's computer and user's reputation on personal and organizational level.

2 Research Background

The paper refers to the definition of information security as given by IMS for information security. It defines "securing the information from different threats in order to ensure business confidentiality, reducing business risk, and increase ROI and business opportunities" [4].

2.1 *Finding from Short Survey*

Information security is a technical problem but nowadays it is management problem as organizations are facing real financial losses and threat of reputation [7, 11]. Recent survey by CSI—Computer Security Institute—found that there are various risk levels to security (Table 1).

2.2 *Finding from short survey chart*

See Fig. 1.

3 Discussion and Conclusion

It is very important to keep awareness of social media among the employees and within the organization. There are many negative consequences for such exploring to social media. Due to such study and effect of information leakage and by previous studies, we have concluded that employees and other individuals are very

Table 1 The percentage of threat in real world when exploring personal information to social networking sites [6]

Social site	Uses	Risk percentage (%)
Facebook	Facebook allows posting of personal data	61
Twitter	Twitter creates business relations and connections	17
LinkedIn	Creates followers	4
Google Plus	Same as Facebook but with low risk due to its usability …	40
Myspace	User's space	18

There are biggest risk of security Facebook (61%), Twitter (17%), LinkedIn (4%), Google Plus (40%), and Myspace (18%)

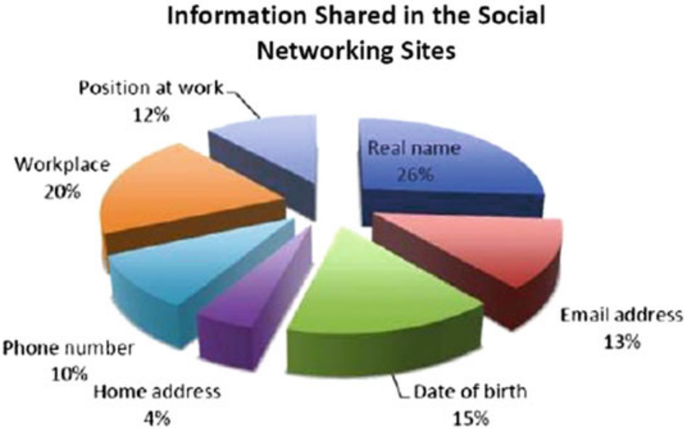

Fig. 1 The types and percentage of information shared on social media

well aware about the threat by leakage of organizational and personal information to the outer world, as mentioned issues and percentage of sharing information might lead to serious damages.

By considering the security problem caused by social networking sites, the suggestions must be implemented by organizations and individuals. Such considerations are more distinguished by SETA programs, with organizational policies [2, 12].

Based on above discussions, it can be said that many users are aware of the use of social media that is directly concerned with the security issues. However, organizations and many awareness programs in the society play important role to install this awareness to individual in order to protect them from leakage of valuable information of personal and professional information, which may cause serious security disaster.

References

1. Abdul Molok NN, Ahmad A, Chang S (2011) Disclosure of organizational information by employees on Facebook: looking at the potential for information security risks. In: 22nd Australasian Conference on Information Systems (ACIS2011), Sydney, Australia
2. Abdul Molok NN, Chang S, Ahmad A (2013) Discolsure of organizational information on social media: perspectives from security managers. In: 17th Pacific Asia Conference on Information Systems (PACIS2013), Jeju Island, South Korea
3. Agarwal P (2013) Department of Computer Science and Engineering, IIT Delhi. Prediction of trends in online social network
4. CSI (2007) 12th annual computer crime and security survey. Computer Security Institute
5. Eminagaoglu M, Uçar E, Eren S (2009) The positive outcomes of information security consciousness training in companies-A case study. Inf Secur Tech Rep 14:223–229

6. Neunerdt M, Niermann M, Mathar R, Trevisan B (2013) Focused crawling for building web comment corpora. In: The 10th Annual IEEE CCNC- Work-in-Progress, pp 761–765
7. Olsik J (2011) The ESG information security management maturity model. Enterprise Strategy Group, Milford, Massachusetts
8. PricewaterhouseCoopers (2010) Security for social networking. pwc.com.au, Australia
9. Radianti J, Gonzalez JJ (2007) A preliminary model of the vulnerability black market. Society
10. Rowe FM, Ciravegna F (2010) Harnessing the social web: the science of identity disambiguation. In: Web Science Conference
11. Sophos (2011) Security threat report: 2010. Sophos Group, Boston, Massachusetts
12. Star T (2012) Don't become an 'accidental' outlaw. In the Star Online