ISSN: 2321-8169
5663 - 5665

Security on the Abusive Social Network Sites- A Survey

J.Adamkani
Research Scholar,
Quaid-E-Millath,
Govt College for Women,
University of Madras

Dr.K.Nirmala
Research Supervisor,
Dept. of Computer Science,
Quaid-E-Millath,
Govt College for Women

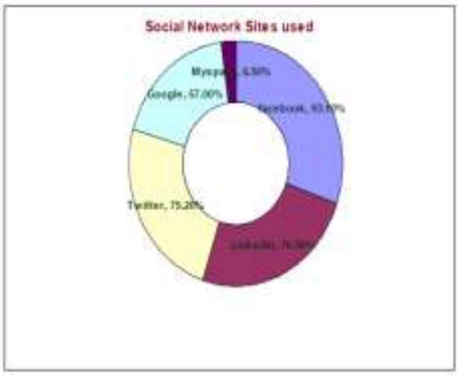
Abstract-To share business interests, the internet social network have become the common platform where users communicate through which My Space, Second Life and similar web2.0 sites can pose malicious security hazards. The social networking sites are viewed as a kind of online cocktail party in business view as a friendly comfortable place to establish contacts, associate buyers or sellers and raise personal or corporate file. To the maxim, cocktail party metaphor is not pure, obviously in the content of a load glass house for social network serves, the users are served in with care and endless visibility through a highly amplified bullhorn. The social network sites are accessed from the comfort and privacy by maximum users, there is a possibility of false sense of anonymity where the users natural defences can too devasted due to the lack of physical contact on social network site by which there is an endanger of disclosing the information of individuals which would never think of revealing to another at a cocktail partys.

Keywords *– Social Networks, MySpace, Web 2.0, Cocktail party*

*****

I. INTRODUCTION

In the materialistic world of nuisance, social networks have become part of the business and personal fabric. To conduct business and personal relationships there are about a billion users using social networks around the globe by which the risks of attackers targeting the users as well as user concern has grown to personal privacy.



1.1 Security Threats

Business enterprises the communicating with customers, build their brands and reveal information favour social media platforms viz Facebook, twitter and LinkedIn are increasing at large to the rest of the world. Does not mean social media are exclusively for linking, friending, up-voting or digging. The mere fact emphasis on risks to use social media ranging from damming the brand to exposing proprietary information to inviting law suits for organisations.

II. MOBILE APPLICATIONS

In mobile application developments the rise of social media has inextricably linked with the revolting spanning the industry. The employees in industry typically download huge application but not concerning about using their own company issued mobile devices. To the extent they download more than they bargained for hence malware is designed to reveal the users private information to a third party replicate itself on other devices, destroy user data or even impersonate the device owner.

2.1 Social Engineering

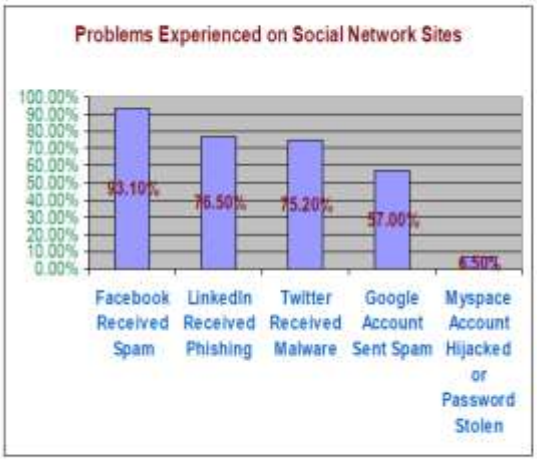
Social Engineering has been the choice of smooth talking scammers before computer networks. But the potential victim who have the soft spot in hearts were forced for grifters and flimflam artists due to the rise of the internet this has taken to a new level by social media through face book, twitter, foursquare and my space where users share personal information about themselves than ever in which assumed trust of dangerous level is encouraged by social media platforms.

2.2 social networking sites

Through third party apps by way of advertisement there found malicious code into the social networking site which go right to the source in the form of hackers .In a work computer by visiting malicious sites can extract personal information where shortened URLs are used to trick users by twitter it is easy to retweet a post by twitter which is especially vulnerable so that eventually could be seen by hundreds of thousands of people.

2.3 Our employees

There can be lapses in judgment even by the most responsible employees by making mistakes or behaving emotionally. All the occasions could not be perfect by everybody. If the comment is made on a work related social media account in the office then it is out there and cannot be retrieved by a high level communication executive by whom the brand is damaged and endangered an account which was not tuned is to the corporate mission in contrast imagine what a disgruntled low-level employee wish out as much invested in job might be able to do with social media tools and a chip on the shoulder.



2.4 Lack of the social media policy

The organization just turn employee loose on social networking platform and are to represent without a social media policy for a enterprise by inviting disaster the goals and parameter of the enterprises social media initiative are to be spell out contrary one will get exactly what they are inviting will be problems.

III. BUSINESS PROTECTION

The business protection can be enhance by the extend threats.

Discrect: The unwanted visitors can be protected through the identity theft or malicious threats. It is advisable to refrain by typing anything into a profile page, bulletin board, instant message or other type of online electronic form which can includes personal and business names and addresses, contact numbers, job title, date of birth, schedule details, daily routines and business or family information, unscrupulous individuals may use against us, it's far better to communicate in generalities than to reveal information.

Skeptical: with a high degree of scepticism viz, stock tips, advance news, personal gossip and so on, social network sites are full of useful business information as well as to substantial amount of useless disinformation. Where users will lie in order to boost their own agenda while others spout unsubstantiated rubbish out of stupidly of ignorance.

Thoughtful: Though the release of personal inhibitions the internet has a curious way like a loudmouth is not favoured by many. It is advisablenot to be a victim of byte by typing anything online which include outrageous, claims, sender, obscenity and so. Thus through thought one can be cool and professional by thinking twice before typing.

To be Professional: To present a video or picture to a social network site, one must make sure it presents in the best possible light by dressing professional and avoiding to wear a funny hat.

Wary: Mostly users always are not the same what they are on the internet, the 14 year old kid in Milwaukee or prisoner in Romania may be a CEO to chat with others in Denver until they are identified independently. Sometimes may turn to screen a new hire or confirming a prospective business partner by using the same business tools to ascertain the business or financial information.

Ensuring of privacy policies: Privacy guidelines are ensured by major social network services published on their websites which include the type of information to sell to other parties where due care should taken to read and understand by spending an amount of time .Presumably if the terms are not liked ,the better not to use the service.

IV. SECURE SCOCIAL NETWORK IDENTIFICATION.

The services incorporated through secure social network include the websites Myspace, Facebook, twitter and windows live spaces where information's are exchanged but the users viz photos videos personal messages and so on .The more the usage ,the more risk occur in using them where the traffic is enrooted by hackers ,spammers, various writers, identity thieves and other criminals. It is advisable to protect through the tips.

4.1 Links through caution

Avoidance of treat links in the received mails should be strictly flowed.

4.2 Posting of self pass word

The click "forgot your pass word " on the account log in page is what the hackers break into financial or other accounts where the security questions viz your birthday, hometown, high school class, mother middle name etc search for the answers by breaking into account It is advisable to use own password questions by hot drawing from anyone materialistically.

4.3 Negligence of users in trust of messages from whom it is from

Oftenly messages code like they are from known ones break into accounts through hackers but the case is not so. By this anonymous method is to be used to track the known ones where it is suspected whether a message is fraudulent. New social networks are inhibited in the process.

4.4 Protection of giving ones email address

Synonymously it is advisable to safeguard the scan of one's email address book from social networking services. Commonly if ones contacts are on the network an offer to enter the email address and password is encountered when one joins a new social network. This will function when a user has sent an email message with a social network and the site may use information except a few social network sites. Many sites are bound to explain what they does.

4.5 Use of social network site directly into user browser

There is high risk of losing one's personal information when the user click to their site through email or another website when entering ones account name and password into a fake site.

4.6 Ascertain of who the user accept as a friend on a social network

There is high possibility of creation of fake profiles from unknown users in order to access information.

4.7 Ascertain and preference of social network carefully

It is advised to know the privacy policy by evaluating the site what the user plan to use and monitors the content that people post on the site. The same criteria is to be maintained when using the credit card to a site where the user's personal information is provided.

4.8 Ascertain of information revealed on the social network site is permanent

There is a provision of evacuation of print photos or text or images and videos when users remove account on the internet. Due attention is to be rendered when excess information is installed on ones site. It is a general phenomena of allowing users to download third party applications on dues personal page where high possibility of stolen of personal information occurs by sedatives. Ensuring of safety precautions is to be taken with any other program or file while extracting from the web through the third party applications. Thus ascertain and favour of social networking sit e is predominantly to be think many times before use.

CONCLUSION

With much attention and precaution by users, social network sites are potentially more useful and worth full business tools with excepted behaviours, personal and company impacts there arise a powerful persuasive communication plan to educate the user communicating about social media risks with an adequate amount of caution and common sense in business. More advice is pertained to organisations to support the communicating plan with targeted protection in order to mitigate risks of social networking as the phenomena which exists to gain momentum.

REFERENCES

Dr. Paul Judge, 2011, Social Networking Security and Privacy Study. [2] http://www.networkworld.com/news/2011/053111-socialmedia-security.html?page=2 [3] http://www.microsoft.com/security/onlineprivacy/social-networking.aspx [4] http://www.networkworld.com/news/2011/053111-socialmedia-security.html?page=1 [5] Gary Loveland, , May 2009,Secure Enterprise 2.0 Forum, Q1 2009 Web 2.0 Hacking Security Report.