# Assessing the Risks of Plymouth's Presence on Social Networks- A Case Study of Bebo

O.Shodiya and A.Phippen

Centre for Information Security and Network Research,
University of Plymouth, Plymouth, United Kingdom
e-mail: info@cscan.org

## Abstract

This research paper considers the sorts of risks associated with the posting of personal information on social networking sites, using Plymouths presence on the social networking site Bebo as a case study. It also considers the data that users provide, that makes them more vulnerable to these risks. The paper then concludes that there is a low level of awareness of internet protection amongst the Plymouth community on Bebo, and user education is needed in order to mitigate against the risks that Bebo users in Plymouth expose themselves to when they post their personal information online.

## Keywords

Risk, Social Networking, Bebo, Personal Information, Plymouth.

## 1 Introduction

Social networks play a crucial role in our everyday lives, as most of us have integrated social networking sites into our everyday living, as we see them as a way to network with people and connect to friends. In today's world there are so many social networking sites, with most of them continuing to see an increase in their user base, in a recent report posted on the social networking site Facebook, it stated it just crossed the 90 million user mark (Facebook website, 2008). Social networks has described by Boyd et al (2007) are "*web based services that allowed individuals to (1) construct a public or semi public profile within a bounded system (2) articulate a list of other users with whom they share a connection (3) view and traverse their list of connections and those held by others within the system"* (Boyd et al, 2007).

Despite the benefits provided by the social networking sites there have been growing concerns about the safety of personal information provided on these sites. Personal information comprises of information such as our names, date of birth, e-mail address, residential address, workplaces and photos and they usually serve as identification information. In a recent report published in the BBC, the child exploitation and online exploitation centre said it was concerned about the posting of personal information by children on social networking sites, as one in twelve children met up with someone encountered first online (BBC website, 2006). The various concerns raised about the safety of personal information on social networks have brought about the need for the assessment of the risks associated with the

posting of personal information on social networking sites using Plymouths presence on Bebo as a case study.

## 2 Previous Study

Research carried out by Sameer Hinduja and Justin Patchin in the area of "*personal information of adolescents on the internet, a case study of my space"* showed that youths are posting and identifying personal information, but not to the extent to which they are supposed to. They based their conclusions on a online survey they carried out on the SNS Myspace which revealed that 81.25% of adolescents profile pages viewed revealed their current cities, 38.4% provided their first names, 27.8% provided their school names, 14.5 provided their birth date, 8.8 provided their full names, 4.2% provided their IM names, 1.1% provided their e mail address, and 0.3% provided their phone numbers. The research was designed to extract data that will determine the validity of the media's claims about whether My Space deserved all of the antagonistic attention and stain it had received from many adults in administrative capacities. The research also wanted to confirm if the numbers support the high volume of reports received. As such, the researchers embarked on an inclusive content analysis of representative sample of pages of my space profiles. The researchers as a measure of caution, in order for the research to be representative, made sure that profiles to be studied had to have a balanced and random chance of being selected for analysis from the entire collection of My Space pages. This they accomplished using a random number generator, as each profile page created on the SNS my space is uniquely assigned a numeric identifier within the site upon its creation. The research further investigated the possibility of cyber bullying and online contact by sexual predators in SNS, and its results revealed that the possibility of been contacted online by sexual predators online is extremely low, but there are possibilities that children could be bullied online (Hinduja et al, 2008).

## 3 Research Methodology

This research in arriving at its result, used a combination of quantitative methods which include that adopted in researches carried out by Sophos, and Hinduja et al, 2008. Sophos in its Facebook ID probe study created a fake Facebook profile page called "Fraudi Staur" (Sophos website, 2007) and used this profile to send out friend requests to random profiles on face book. "Fraudi Staur" (Sophos website, 2007) was a green plastic frog profile on face book that gave out less information about itself (Sophos website, 2007). In order for the research to find and determine the number of people in the Plymouth network on Bebo, a domain specific search for the hometown Plymouth was conducted using the following parameters (Age – Null, Sex- Male and Female, Relationship Status – Any, Hometown –Plymouth). Then in order for this research to carry out a balanced comprehensive content analysis of the profile pages of people in the Plymouth network, it used a random number generator similar to that used in the research carried out by Hinduja et al, 2008, to determine the profile pages to be viewed. This made it possible for the profile pages to have a balanced chance of been selected among profile pages of people in the Plymouth.

An excel data sheet was then designed to collect the data provided on 200 profile pages of people in the Plymouth network. Due to the fact that the profile pages were

sampled randomly, the Bebo pages that were identified could have been that of a child or an adult, although Bebo does not allow the ages of those less than 16 to be displayed on their profile pages. Additionally data could not be extracted from some profile pages, as a result of them restricting access to their profile pages; Bebo provides its users with the ability to enable privacy settings. The research then looked at all publicly accessible information on the Bebo profile pages identified and this information included the basic profile information provided by the users and comments left by friends. Most of the information was found on the basic profile pages of the users. Additional information was also discovered on the comment portions of the profile pages. Then in order for this research to further investigate the attitudes of the Plymouth community to divulging sensitive information such as identity data on the social networking site Bebo, a fake profile page was created to see the possibility of obtaining sensitive information from users. The fake profile pages then sent out friend requests to 50 users identified from the earlier data collection phase.

## 4 Results

A domain specific search for people in Plymouth turned up a figure of 25,169, this value represents those who put up Plymouth as their hometown, as there are some others who would have specified United Kingdom as their hometown, but this research would ignore such as we are only interested in those who set Plymouth as their hometown. Among the profile pages selected by the random number generator for content analysis, were some profiles which enabled privacy settings, thus these profiles could not be viewed unless you are a friend. This finding indicates that some users might be aware of the risks of posting personal information online as this information could compromised, thus in this regard they have enabled privacy settings as a safeguard. Additionally, some profile page searched for, returned errors and this might be attributed to their accounts been inactive or been deleted.183 of the profile pages people had an age displayed on their basic profile pages, which represents of the profile pages sampled. Among the 200 people sampled, 74 of them could be termed minors (less than 18 years old).This finding shows that there are good numbers of minors that use the social networking site Bebo, thus there might be a possibility of cyber bullying or cyber stalking occurring to this class of users.

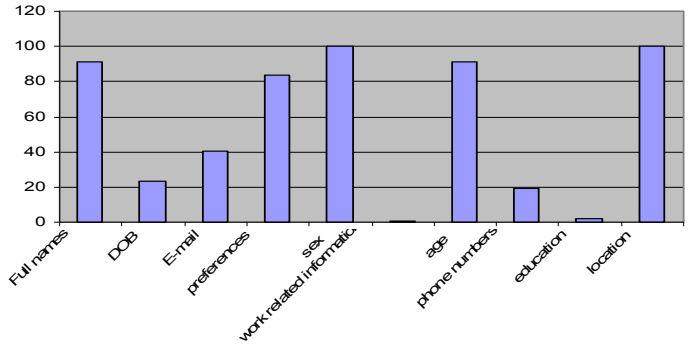


**Figure 1: Information posted by people on the Plymouth network on Bebo (%)**

46 of the users put up their dates of birth on their profile pages, although we noted earlier that Bebo does not allow ages less than 16 to be displayed on profile pages. The putting of sensitive data such as date of birth which is used in identification of persons, on this profile pages can be due to the insensitivity of the owners of this profiles to internet protection, or the fact that they are not aware of the risks of posting sensitive personal information on social networks. Among the 200 profile pages 182 provided their full names on their profile page, The posting of full names in combination with dates of birth on social networking sites has been identified as a major source for online identity theft in the past, and it will be a source for identity thieves obtaining information about potential targets in the years to come. 168 of the profile pages analyzed provided preferences on the profile pages and this information is also usually used by computer users as password to their systems, as they see them as easy to remember secrets for which they can not forget. The provision of preferences on these profile pages can be said to be no harm to the owners of these profiles until this information is used to compromise items such as their E- mail accounts. All of the profile pages sampled provided the sex of the owners of the profile page, this is so because the SNS Bebo requires users to provide their sex before joining the sites. The display of sex on the profile page of users on the SNS Bebo is a default, which users cannot control, thus they are bounded by this default setting. Among the profile pages sampled, 172 provided their photos on their profile pages and this can be attributed to the interactivity of the web technologies that are used by SNS which enable users to make statements about themselves in form of photos. The posting of personal information such as photos is no risk to users of the Plymouth community on Bebo, but if this photos are used in combination with other data such as date of birth, full names, sex then it maybe a potential risk to the users who posted this information, as this information can be used to make clone passports of the users. In all the profile pages analyzed 81 users had their E- mail address or chat IM displayed on their profile pages and of this number are 26 minors (less than 18). The posting of this information is of no harm to the posters of such information, until the information is either used to stalk or bully the person who posts the information. Among the 200 profile pages analyzed, 183 provided their ages on their profile pages, as this might be attributed to the focus group that Bebo attracts. Adolescents tend to provide their ages on their profile pages so as to show they are young and can be networked. The posting of the users age is not a source for concern until this information is used by some someone such as a cyber stalker or online predators to identify potential target that they are going to stalk. In all of the profile pages analyzed 4 provided education related information, while another 2 provided work related information. The posting of work or education related information is no requirement when joining Bebo, but an additional feature on these sites. The posting of sensitive data such as work and education related information cannot be explained, as this information can be can be acquired by cyber stalkers or online identity thieves in identifying targets.

The second part of this research which involved an Identity probe turned up mind bugging results. This fake profile page was able obtain response from 18 people, in form of confirmation of friend request, and among the people that confirmed friend request, the fake profile was able to obtain the phone numbers of 5 of them on their profile pages. In other to further investigate the possibility of me obtaining the contact details of the 13 who did not put up their contact detail on their profile pages,

6 of those who accepted friend requests from the fake profile were added to live messenger accounts using the live messenger ID they provided on their profile pages, although not all provided live messenger IDs.

In other to further investigate the possibility of me obtaining the contact details of the 13 who did not put up their contact detail on their profile pages, 6 of those who accepted friend requests from the fake profile were added to live messenger accounts using the live messenger ID they provided on their profile pages, although not all provided live messenger IDs. The purpose of this is to see the possibility of them divulging sensitive information such as their contact details and workplace to me. The results were astonishing as the fake profile was able to get the contact details of 2 of them within a week of meeting online, although 3 others refused to reply to chat messages but they confirmed the friend requests on their live messenger accounts, and one is yet to reply to my friend request on live messenger as of the time of writing this report.

## 5 Recommendations and conclusion

Social networking sites (SNS) such as Bebo will continue to thrive as long as they continue to adapt themselves to the dynamics of meeting user social needs. The users will also continue to provide personal information on SNS as them see it as an opportunity to network themselves. If users cannot be prevented from providing personal information, it will become imperative to educate users on the attendant risks that go with posting personal information such as Full names, Date of birth and E- mail address on SNS. This measure will go a long way in increasing the level of awareness of internet protection in the Plymouth community, which is our case study. And in light of the above mentioned points this research will also summarize the protection measures that can be taken by users in Plymouth on Bebo to protect themselves against the risks that go with posting personal information on social networking sites which include Cyber stalking, Cyber bullying, and Online identity theft. Additionally the summary of measures will also consider the measures that can also be taken by SNS service providers to protect user information, without undermining the purpose for which SNS where designed for, which is networking.

- Social networking sites should consider investing more money in increasing user education on the potential for harm in posting sensitive personal information online.
- Privacy settings should be enabled by users of social networking sites.
- Read the privacy policy that social networking sites provides its users.
- Parents of Minors should monitor their children when using social networking sites.
- Users should limit the amount of personal information they post on social networking sites.
- Users should avoid the temptation of adding strangers to their list of buddies or friends.
- Users should avoid posting information which can be described as revealing.

- Users should make use of covert channels of communication in reaching out to friends rather than using social networks.
- Social networking sites should consider investing more money in increasing user education on the potential for harm in posting sensitive personal information online.

# 6 References

BBC website, 2006. "*Child online safety card unveiled*". (BBC.co.uk). Available at http://news.bbc.co.uk/1/hi/technology/5238992.stm [accessed 11th May, 2008]

D Boyd et al, 2007. Social networking sites: Definition, History and scholarship. Journal of computer mediated communication. Page (210-230) Available at http://www.blackwell-synergy.com/doi/pdf/10.1111/j.1083-6101.2007.00393.x Social Network Sites: Definition, History, and Scholarship [accessed 21 April 2008]

ENISA (European network and information security agency) (2007). "*Security issues and recommendations for online social networks"*. Available at http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf [accessed 2nd June 2008].

Parry, 2008. "*Parrys guide to cyber bullying"*. (Bebo.com). Available at http://www.bebo.com/CyberBullying.jsp [Accessed 23 November, 2008]

Ralph Gross, Alessandro Acquisti. 2005 "*Information Revelation and Privacy in Online Social Networks (The Facebook case)*". (Heinz college.edu) Available at http://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf [Accessed 31st December, 2008

Smith p, Madhavi J, Carvahlo M, Tippet N. "cyber *bullying, its forms, awareness and impact, and the relationship between age and gender in cyber bullying"* (Anti- bullying.org) Available at http://www.anti-bullyingalliance.org.uk/downloads/pdf/cyberbullyingreportfinal230106_000.pdf

Sophos website, 2007. *Sophos facebook probe shows 41% of users happy to reveal all to potential ID thieves.* (Sophos.com). Available at http://www.sophos.com/pressoffice/news/articles/2007/08/facebook.html [Accessed 1st January 2008].