Educating Social Networking Users

P.Nair and M.Papadaki

Centre for Security, Communications and Network Research,
Plymouth University, Plymouth, UK
e-mail: info@cscan.org

Abstract

"*Privacy is dead, and social media hold the smoking gun." – Pete Cashmore, Mashable CEO*
"Social networks aren't about Web sites. They're about experiences." – Mike DiLorenzo, NHL social media marketing director.
Since the turn of the 21st century, there have been many developments in the technological world, developments and findings that may not have necessarily improved the way the world lives, but definitely have changed and revolutionised the way it works . The Internet itself has changed so much from being a service designed for CERN scientists to communicate amongst themselves to a global phenomenon (Anderson, 2007). And now with the rise of Web 2.0 or simply a second much better version of the Web, people are getting more and more dependent on the Web for everything that they do. The participatory nature of Web 2.0 along with its user friendly design and outlook meant that it became an endless repository of dynamic information and information exchange into which anybody can both add to as well as take from (Sharma, 2011). Many services like blogging, interactive and target centric advertisements and product placements, e-commerce soon started to blossom due to the advent of Web 2.0 however none of them could profit as much as social networking sites did during the last half a decade.
In this project an effort will be made to educate users about the potential threats involved on social networking sites by creating a Flash based game designed in the format of a quiz. The users will be put in make believe situations where they will have to answer questions based on their existing knowledge of social networking sites and its functionalities. The users through the game will also be made aware of additional facts that can further help their security measures against the threats on social networking sites. The game will be sent to a selected group of participants and the results will be collected for analysis purpose. The results will be studied in depth to evaluate the success of the game and whether creating awareness by using interactive medium is a good choice over other means like designing posters, making videos, lectures, seminars etc. Based on some of the scenarios a few solutions and changes will be suggested to the already existing precautions and measures. The results of the game shows there is a scope for more user responsibility in creating awareness and users are open to similar awareness based initiatives instead of the tried and testing ones like video and seminars. Users were also seen to better react to situations if they were able to co-relate it with similar situations.

Keywords

Social networking sites, SNS, security, Awareness, game, educating

1 Introduction

Social networking sites or SNS have been expanding the most amongst all Web 2.0 services (Leitner and Grechenig, 2008), however the threats involved in SNS have

also been expanding at the same phenomenal rate, with cyber criminals making SNS as one of their preferred targets. Social networking sites on their part know that it is essential to keep hold of the users and provide for their safety, making sure that they improve security and devise new methods to keep away the cyber criminals. But the fact remains that the main reason that cyber criminals thrive so much on social networking sites is due to the fact that the efforts put in to protect the users by the sites is not been reciprocated by the users themselves. Lax security measures combined with not adhering to the proper social networking etiquettes with regards to sharing of personal information has meant that it is the end user that is the weak link when it comes to the fight against cyber criminals. The digital age of today comes with a paradox, that of accepting wholesome changes and getting the latest developments with just a mouse click, however it comes at the expense of losing the identity and privacy of oneself, besides opening oneself to a multitude of attacks (John, 2010) It is this internal conflict and chaos that the cyber criminals are exploiting to good effect for their own good

The aim of the paper is three-fold, i) getting a clear picture of the existing scenario with respect to areas like privacy and security issues and the extent of the problem, studying out the factors that are hindering the area and developing a solution ii) designing and developing an interactive game that will bring awareness to the scenario and lastly iii) evaluating the success of the game.

2 Existing Scenario

Users are very careless with their personally identifiable information (PII), nearly 40 per cent of users had displayed information such as birth date, while a quarter of users with children had posted some information about their children on social networking sites(Consumer Report, 2010).Acquisti and Gross(2009) have shown with the help of a few details it is possible to guess someone's social security number(SSN). The popularity of social networking sites with people all over the world has made it a favored spot for cyber criminals to spread their chaos (Walsh, 2011). Oversharing(of information and content) and weak privacy settings are rampant amongst users on social networking sites with users at risk against threats like phishing, identity theft, data breaches, loss of locational privacy, real life threats like stalking, paedophilia, robbery etc.

User is under threat from all sides, i) including his own known contacts/friends, ii) from third party applications and policy changes of social networking like Facebook photo tagging (Cluley, 2011) and iii) lastly from his/her ignorance and neglect. There are other types of threat on social networking sites XSS (cross site scripting) attacks, facial recognition technology related threats. Threats on SNS can be divided into the vectors that they target and attack, like privacy related attacks , drive-by download/payload related threats like malware, spyware etc., identity related threats and real life threats. A table charting the type of threats and the solutions that can be implemented to stop those threats from occuring can be as seen in Figure 1.

Solutions

Threats	Avoid oversharing	Tweak privacy settings	Anti-virus/ user system changes	Changes in site policy, design etc.
XSS			**X**	**X**
Phishing			**X**	**X**
Location tagging	**X**	**X**		**X**
Identity theft	**X**	**X**		**X**
Facial recognition	**X**	**X**		
Real life threats	**X**	**X**		**X**

Figure 1: Threats versus solutions

3 Game Design and Results

The game is designed in the format of a quiz-based game where the user's knowledge will be put to test by social networking sites based scenarios. The scenarios have been developed keeping in mind the various scenarios and threats aggregated from the section Existing Scenario. As such the game will have 8 questions of different formats and divided into 5 scenarios.

Scenario 1: Importance of passwords and and the need for password awareness

The top 5 most commonly used passwords that were revealed during the hack attack on Gawker websites included passwords like 123456, password, 12345678, lifehack and qwerty (Broida, 2010). Passwords like these could mean that even the best privacy and security settings wouldn't be able to save a user from getting his account hacked and all of his information stolen.

Scenario 1 contains 3 questions which are questions which basically tests the user's knowledge on password strength, password reusability and having unique passwords.

Scenario creates awareness on threats like dictionary attacks and brute force attacks, which can lead to the user's password being guessed or cracked and could lead to the user's account getting compromised and misused for a wide variety of purposes.

Scenario 2: Phishing and identity theft protection

Scenario 2 touches on the topic of phishing based emails and sites. There is only one question in this scenario in which given a situation, the user is asked to judge whether the mail originating in the situation is a phishing mail or not. Users are advised and warned about the dangers of phishing sites as well that look very much like the original site exceot for a few unnoticeable changes which sometimes is enough for a naïve or a new user to become a victim of an identity theft.

Scenario 3: Oversharing and privacy settings

Scenario 3 has two questions that concerns oversharing and privacy settings, the two questions were clubbed into one scenario because one can prove that if sharing information and privacy settings are considered two entities then it is enough for one the entity to exist such that the other entity can be neglected and thus limiting the damage that can be caused as well.

For example : If Alice has set her privacy settings such that no one but her trusted friends and contact can only see her information then it means she can share any information she wants without being in too much risk as no one else but her friends can see those information.

The two questions in this scenario tests the user's knowledge of what should be shared with only friends and contacts and what should be shared with everyone (public view)

Scenario 4: Privacy Policy

Scenario 4 containing just only one question tests the user's knowledge of the privacy policy document often found on SNS' that tells the users of the way in which the user's personal information is used by the site, where it is stored, what to do if the user wants his personal information taken back etc.

Being aware of privacy policy and its contents can save a user from data breach and data being viewed and used by third party apps which can then cause all sorts of problem

Scenario 5: Child Protection on Social Networking Websites

The last and final scenario judges a user's knowledge of child protection mechanisms and measures in existence on SNS'. Livingstone, Olafsson and Staksrud (2011) have only surveyed kids in European countries and found that an unusually high number of kids are on social networking sites flouting age restrictions and often end up sharing too much information on the sites. Although many users won't have kids, the sheer number of people on the Internet means that the user will atleast know some people in his contact list who will have kids and it is important to be aware of the threats that can happen on SNS these days.

The question tests the user by asking him/her if they can spot whether in a made up situation, an underage kid is lying about his age online

At the end of the game, there are some questionnaire that is used for the purpose of demographical analysis besides getting feedback on the game and some background information on the user.

4 Results

Total of 30 people played the game and the age and gender wise break up is as follows (the numbers in bracket denote the percentage of the total):

Men : 17 (56.66%), Women : 13 (43.33%)

18-24 age group : 18 (60%)
25-34 age group: 4 (13.33%)
35-44 age group: 6 (20%)
45-54 age group: 2 (6.66%)

The scenario wise break down of the results is as seen in Table 2.

Scenario	Right Answer	Wrong Answer	Need for awareness
Scenario 1	50%	50%	Moderate
Scenario 2	86.66%	13.33%	Very less
Scenario 3	66.66%	33.33%	Less
Scenario 4	33.33%	66.66%	Definite need for awareness
Scenario 5	80%	20%	Less

Table 2: The table is tabulated as the percentage of total users out of 30 who gave the right and wrong answers

From the results one can see that there is a definite need for awareness in Scenario 4 where the user needs to be made aware of the privacy policy.

The high percentage of people who got questions 5 and 6 in Scenario 3 were able to do so because the questions were such that there were related to each other. In fact a high percentage of users who got Question 5 also managed to get Question 6 right.

This proves that it becomes easier to create awareness if situations can be co-related and the user is made aware of it.

4.1 Questionnaire analysis

The users were asked whether they have come across before such awareness based games on the same topic and 80 per cent of the users said they have never across such a game before, while the 20 per cent who had come across such a concept were among the highest scorers. **This proves that those who had come across such a content before were perhaps well informed of the threats and hence were able to score high marks**

The game manages to create some awareness and something new for the users when asked in a question 50 per cent of the users agreed to the fact that games like this were a better concept and more effective in creating awareness than watching a video or a seminar on the same topic. In terms of evaluating the success of the game this statistic says a lot.

It came as no surprise that people who agreed or strongly agreed that they have good knowledge of the way computers and social networking sites work were some of the higher scorers in the quiz with an average score of 69.64 %

This proves that people who have a technical background or a general idea of the way computers and the Internet works are less at risk online than say someone who isn't so good with computers and Internet.

In the next question as well, it doesn't come as too much of a surprise that users who said that they find it difficult to find information on the Internet related to such security threats were in fact some of the low scorers in the game.

5 Conclusion

The game showed that there are certain areas where user awareness is still not as good as one would want it to be, for example areas like password protection and usage. The paper also proved that users must be given more responsibility when it comes to creating awareness amongst each others. Users who had come across a similar awareness related game were some of the high scorers in the game, hence proving that not only being aware of a threat makes you more knowledgeable but also you tend to be in a position to teach others the same. A positive response was received with regards to the concept of using a game to create awareness as half of the users taking part in the game felt that the idea was a better one than creating awareness on the same issue using a seminar or video.

6 Future Work

There is definitely a lot of potential for future work on this particular thesis and the development of the game. The users through the questionnaire have accepted the game as a new and novel way of creating awareness better than some of the existing means like watching a video or attending a seminar on the same topic.

7 References

Acquisti, A., Gross, R.(2009). Predicting social security numbers from public data. *Proceedings of the National Academy of Sciences of the United States of America,* 106(27) pp.10975-109780

Anderson, P. (2007). What is Web 2.0? Ideas, technologies and implications for education. *Proceedings of the JISC Technology and Standards Watch, Feb 2007.* [online] Available at: http://www.jisc.ac.uk/media/documents/techwatch/tsw0701b.pdf [Accessed on 16 June 2011]

Broida, R.(2010). Password Choices [online] Available at : http://www.bnet.com/blog/businesstips/the-gawker-leak-how-to-protect-your-business-from-poor-password-choices/9976 [Accessed on July 16 2011]

Cluley, G.(2011). Facebook changes privacy settings for millions of users - facial recognition is enabled [online] Available at: http://nakedsecurity.sophos.com/2011/06/07/facebook-privacy-settings-facial-recognition-enabled/ [Accessed on 29 June 2011]

Consumer Reports (2010). Social insecurity. What millions of online users don't know can hurt them [online] Available : http://www.consumerreports.org/cro/magazine-archive /2010/june/electronics-computers/social-insecurity/overview/index.htm [Accessed on 24 June 2011]

John,N.(2010). Does WikiLeaks have any privacy issues? [online] Available at: http://privacy.sociothink.com/?p=110 [Accessed on 16 July 2011]

Leitner, P., Grechenig, T. (2008). Social Networking Sphere: A Snapshot Of Trends, Functionalities and Revenue Models. *Proceedings of the IADIS International Conference on Web based communities 2008.* Amsterdam, The Netherlands, 24-26 July 2008.

Livingstone, S., Ólafsson, K., Staksrud, E. (2011) *Social networking, age and privacy.* EU Kids Online, London, UK.

Sharma, P. (2011). Core Characteristics of Web 2.0 services [online] Available at : http://www.techpluto.com/web-20-services/ [Accessed on 10 July 2011]

Walsh, S. (2011). Top 5 Reasons Why Spammers Love Social Networking [online] Available: http://www.allspammedup.com/2011/08/top-5-reasons-why-spammers-love-social-networking/ [Accessed on 5 August 2011]