Journal of Modern Science and Technology
Vol. 2. No. 2. September 2014 Issue. Pp.87-98

Social Networking Sites: Threat to Security

Mohammad Jabed Morshed Chowdhury[1] and
Narayan Ranjan Chakraborty[2]

Popularity of social networking sites has dramatically increased in recent years. Social networking sites like Facebook, Google Plus, and LinkedIn allow millions of individuals to create online profiles and share personal information with vast networks of friends and, often, unknown numbers of strangers. In this paper, patterns of information revelation in online social networks and their security implications have been studied. These security implications are named as social security attacks in this paper. We survey online behavior of more than 50 University students. The amount and type of information they disclose has been evaluated. We also perform an extensive analysis on disclosed information from different perspectives of the users. At the end, we demonstrate how this information may lead to security breaches. This will help to create security awareness about the usage of social networking sites among the users.

Keywords: Social network sites, Security attack, Social Attack, Risk.

1. Introduction

Millions of users are flocking daily to social networking sites like Facebook or Twitter etc. Enormous popularity of these web-sites has its roots in the unique opportunities social network has to offer: possibility to manage one's identity and context in the desired way by allowing users to consciously self-present and control the image they project to others (Ellison et al, 2006 and Krasnova et al, 2009). In addition, by allowing users to efficiently keep in touch and develop relationships, social networking sites promise to create social capital – an important contribution to the modern society and a source of their public value (Ellison et al, 2007). The popularity of social networking sites has increased rapidly in recent years. But the concept dates back to the 1960s. Viral growth and commercial interest only arose well after the advent of the Internet. The rapid increase in participation in very recent years has been accompanied by a progressive diversification and sophistication of purposes and usage patterns across a multitude of different sites. The social networking sites can be grouped mainly into seven categories, including business, common interests, dating, face-to-face facilitation, friends, pets, and photos.

Though there are differences between different social networking sites but they also share a core feature: "profile" - a representation of their sel[ves] and, often, of their own social networks) - to others to peruse, with the intention of contacting or being contacted by others, to meet new friends or dates (Friendster, Orkut), find new jobs (LinkedIn), receive or provide recommendations (Tribe), and much more.

---

[1]Mohammad Jabed Morshed Chowdhury, Department of Computer Science and Engineering, Daffodil International University, Bangladesh, E-mail: jabedmorshed@gmail.com
[2]Narayan Ranjan Chakraborty, Department of Computer Science and Engineering, Daffodil International University, Bangladesh, E-mail: narayan@daffodilvarsity.edu.bd.com

The success of these sites has attracted the attention of the media (Ellison et al, 2007) and researchers. The latter have often built upon the existing literature on

social network theory (Joshua et al, 2009, Mohamed et al, 2012 and Sadie et al, 2012) to discuss its online incarnations. In particular, (Boyd, 2003) discusses issues of trust and intimacy in online networking; (Donath and Boyd, 2004) focused on participants' strategic representation of their selves to others; and (Liu and Maes, 2005) focus on harvesting online social network profiles to obtain a distributed recommender system.

In this paper, we focus on patterns of personal information revelation and different security based on that information. We are relying on the amount and type of information people freely reveal in social networking sites. Category-based representations of a person's broad interests are a recurrent feature across most networking sites (Liu and Maes, 2005). Such categories may include indications of a person's literary or entertainment interests, as well as political and sexual ones. In addition, personally identified or identifiable data (as well as contact information) are often provided, together with intimate portraits of a person's social or inner life.

In this paper, we focus on patterns of personal information revelation and different security based on that information. We are relying on the amount and type of information people freely reveal in social networking sites. Category-based representations of a person's broad interests are a recurrent feature across most networking sites (Liu and Maes, 2005). Such categories may include indications of a person's literary or entertainment interests, as well as political and sexual ones. In addition, personally identified or identifiable data (as well as contact information) are often provided, together with intimate portraits of a person's social or inner life.

Such apparent openness to reveal personal information to vast networks of loosely defined acquaintances and complete strangers calls for attention. We investigate information revelation behavior in online networking using actual field data about the usage and the inferred privacy preferences of around 500 students. We have run an experiment among these students based on the information they have reveled in the Facebook. Our results provide a preliminary but detailed picture of personal information revelation and different security attacks based on this information.

The remainder of this paper is organized as follows. We first elaborate types of information revel in online social networking in Section 2. Next, we present the different security attacks based on the publicly revealed user information Section 3. Then, we discuss about our experimental procedure to measure the effect of these types of security attacks in Section 4. In section 5, we demonstrate a social phishing attack and its implication. Finally, we conclude in Section 6.

2. Information Revelation on Social Networking Sites

While social networking sites share the basic purpose of online interaction and communication, specific goals and patterns of usage vary significantly across different services. The most common model is based on the presentation of the

participant's profile and the visualization of her network of relations to others. This model can stretch towards different directions. In matchmaking sites, the profile is critical and the network of relations is absent. In diary/online journal sites like LiveJournal, profiles become secondary, networks may or may not be visible, while participants' online journal entries take a central role. Online social networking thus can morph into online classified in one direction and blogging in another.

Patterns of personal information revelation are, therefore, quite variable. First, the pretense of identifiability changes across different types of sites. The use of real names to (re)present an account profile to the rest of the online community may be encouraged (through technical specifications, registration requirements, or social norms) in social networking websites like the Facebook, that aspire to connect participants' profiles to their public identities. The use of real names may be tolerated but filtered in dating/connecting sites like Friendster, that create a thin shield of weak pseudonymity between the public identity of a person and her online persona by making only the first name of a participant visible to others, and not her last name. Or, the use of real names and personal contact information could be openly discouraged, as in pseudonymous-based dating websites like Match.com, that attempt to protect the public identity of a person by making its linkage to the online persona more difficult. However, notwithstanding the different approaches to identifiability, most sites encourage the publication of personal and identifiable personal photos (such as clear shots of a person's face).

Second, the type of information revealed or elicited often orbits around hobbies and interests, but can stride from there in different directions. These include: semi-public information such as current and previous schools and employers (as in Friendster); private information such as drinking and drug habits and sexual preferences and orientation (as in Nerve Personals); and open-ended entries (as in LiveJournal).

Third, visibility of information is highly variable. In certain sites (especially the ostensibly pseudonymous ones) any member may view any other member's profile. On weakerpseudonym sites, access to personal information may be limited to participants that are part of the direct or extended network of the profile owner. Such visibility tuning controls become even more refined on sites which make no pretense of pseudonymity, like the Facebook. And yet, across different sites, anecdotal evidence suggests that participants are happy to disclose as much information as possible to as many people as possible. It is not unusual to find profiles on sites like Friendster or Salon Personals that list their owners' personal email addresses (or link to their personal websites), in violation of the recommendation or requirements of the hosting service itself.

3. Different Security (Social) Attack

People usually share information about their identity, educational institutions, career related information and their likings in their profile. They also share photos and videos about them. These types of information reveal the psychology, interest and personality about any individual. Malicious people can use this information to prepare and launch security attacks. We call them social security attacks. There can

be many types of social attack. We have indentified and experimented with the following social security attacks.

3.1. Social Phishing

Phishing is a form of an attacker which attempts to fraudulently acquire sensitive information from a victim by impersonating a trustworthy third party. Phishing attacks today typically employ generalized “lures.” For instance, a phisher misrepresenting himself as a large banking corporation or popular on-line auction site will have a reasonable yield, despite knowing little to nothing about the recipient. In a study by Gartner (Gartner, 2004) about 19% of all those surveyed reported having clicked on a link in a phishing email, and 3% admitted to giving up financial or personal information.

It is worth noting that phishers are getting smarter. Following trends in other online crimes, it is inevitable that future generations of phishing attacks will incorporate greater elements of context to become more effective and thus more dangerous for society. For instance, suppose a phisher were able to induce an interruption of service to a frequently used resource, e.g., to cause a victim’s password to be locked by generating excessive authentication failures.

The phisher could then notify the victim of a “security threat.” Such a message may be welcome or expected by the victim, who would then be easily induced into disclosing personal information. In other forms of so-called context aware phishing (Markus, 2005) an attacker would gain the trust of victims by obtaining information about their bidding history or shopping preferences (freely available from eBay), their banking institutions (discoverable through their Web browser history, made available via cascading style sheets or their mothers’ maiden names which can be inferred from data required by law to be public (Virgil et al, 2006).

Given that phishing attacks take advantage of both technical and social vulnerabilities, there is a large number of different attacks; an excellent overview of the most commonly occurring attacks and countermeasures can be found in (Emigh, 2005). The idea of using people’s social contacts to increase the power of an attack is analogous to the way in which the “ILOVEYOU” virus (Ellison et al, 2007) used email address books to propagate itself. The question we ask here is how easily and how effectively a phisher can exploit social network data found on the Internet to increase the yield of a phishing attack.

The answer, as it turns out, is: very easily and very effectively. Our study suggests that Internet users may be over four times as likely to become victims if they are solicited by someone appearing to be a known acquaintance.

3.2 Social Spam

Users usually share the email address and their contact numbers in the social networking sites. These facilitate the spammer to collect the email address of their

victims. They use the interest of the user victim and put that kind of spam mail to the victim. Our experiment shows that victim usually show more interest in this kind of email which align with their personal interest.

3.3 Identity Theft and Impersonation

Identity theft happens when fraudsters access enough information about someone's identity (such as their name, date of birth, current or previous addresses) to commit identity fraud. Identity theft can take place whether the fraud victim is alive or deceased. Attacker can data mine different t information about a person from the different social networking sites (e;g., Facebook, LinkedIN etc). The attacker can then impersonate this person in his working place or educational institution and can revel much confidential information about the victim or about the institution.

3.4 Dictionary Attack on Password

The use of passwords is a major point of vulnerability in computer security, as passwords are often easy to guess by automated programs running dictionary attacks. Passwords remain the most widely used authentication method despite their well known security weaknesses. User authentication is clearly a practical problem.
People usually put the password which they can remember easily. For that sometimes they use password associated to themselves, for example, their phone number, car number, pet name, favorite book etc. Please +use to share this kind of information in their social networking profiles. Attackers can harvest this information and can successfully break their password.

3.5 Information Leakage

Social networking site is established as a new vehicle for public messaging. In the past, forums for public communication were either controlled, like television or radio programming, or limited, like a public protest that is physically limited to a geographical area. Social network now allows individuals to broadcast their messages to particular individuals or the public at large at no cost, with no special equipment, and with no oversight or filters. This ability can have a serious impact on an individual or organization and its brand, and its reputation. Any person can intentionally or unintentionally leaks confidential information which can be used by the attacker for malicious activities. Sometime even personal photo, information about being any place in a specified time can reveal much secret information.

4. Experiment and Result New

To access online social activities of users, a session has been organized with 50 students from different departments of Daffodil International University. We have analyzed the result from different perspective, namely technical, gender and age.

4.1 Technical perspective

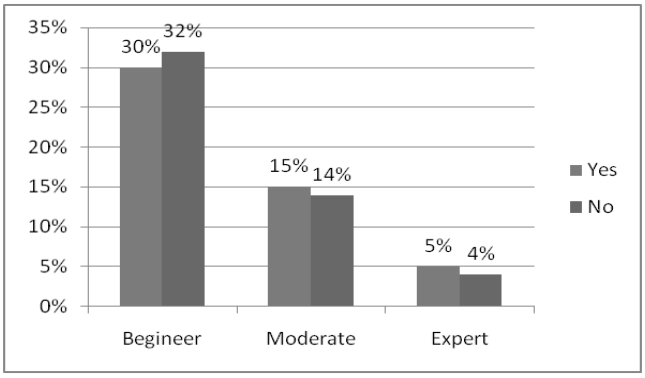
First of all we have focused on the technical aspect of the user's background. We divided the users into three groups, beginner, moderate and expert. The level of

expertise is very subjective and we leave this for users' own judgment. In this survey, out of the 50 participants, 54% are moderate users, 40% are the beginner and 6% expert user. From our survey, it reveals that it is a greater threat for beginner and moderate users than the expert users. As maximum of users of social networking sites fall into beginner and moderate category, the overall risk is very high.

First question asked to the participants, whether they shared their email address in Social Network or not? All participants give positive reply. It clearly indicates that e-mail address is public to all and it is the window to an attacker to communicate directly to their personal email address and lure them for spamming and phishing mails.

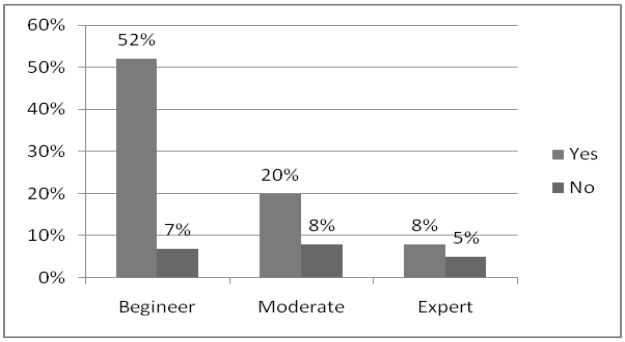
Next question was "Do you use your name or any personal information which you share in social network as your password?" The replies are alarming as 50% said yes they shared such kind of information in social network. Figure 1 shows the opinion. Now a day's password is the prime way to enter into any system. If someone shares this type of sensitive information to the public then s/he will be in great danger.

Figure 1: Personal Information as Password



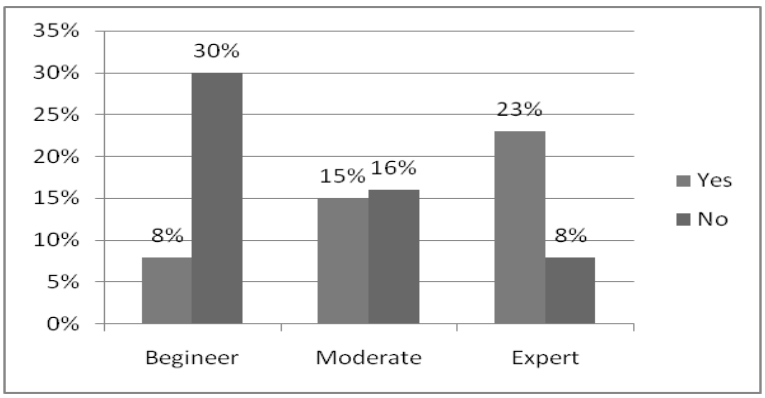
Do you want to get email about your favorite movie/shopping/book in your email? This was the next question. 80% of the total participants said yes they want this kind of information to their email inbox. This is an opportunity for the spammer or attackers to send more targeted mails.

Figure 2: Email Notification of Favorite Things



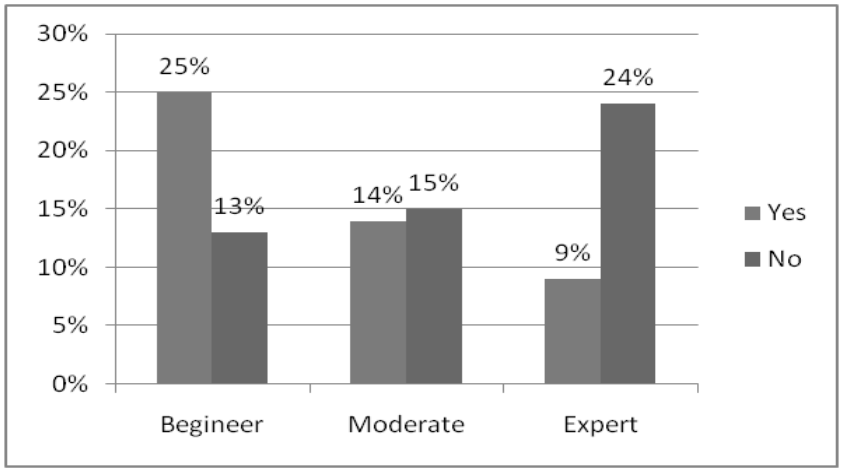
Next question asked to the surveyee, do they use online banking or any other e-commerce services? 46% say yes they used online banking or e-commerce service. 54% participants are not involved with online banking or ecommerce services shows in figure 3.

Figure 3: Use of Online Banking or Ecommerce Services



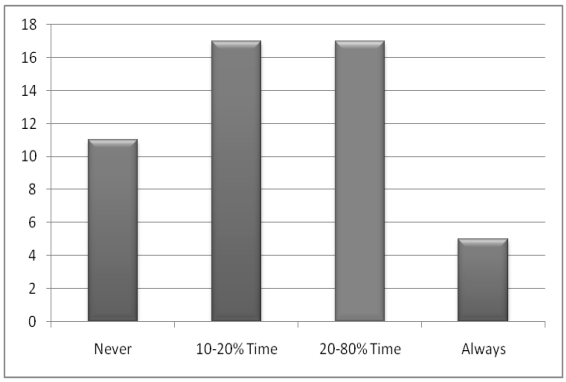
Next question was “Do you use the same email address for social network and e-commerce services?” 48% said yes they use same email address for social network and ecommerce service while 52% never use same email for the same. Figure 4 shows the proof.

Figure 4: Use Same E-mail Address for Social Networks and e-Commerce Services



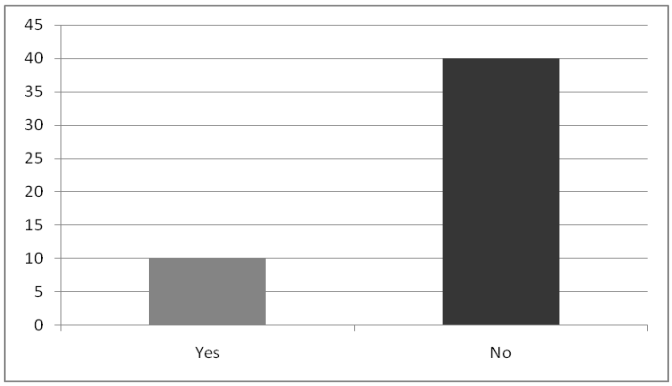
Now a day’s spamming is another major security concern. We asked to the participants “Do you click on the mail which your mailing system says spam? Participants responses are reflecting in figure 5, 10% participants always click the spam mail. 34% are clicked on 10-80% time where 22% never click on spam. Other than 22% everybody are vulnerable to serious attacks through spamming.

Figure 5: Clicking On Spam e-mails



To avail the web services, most of time users need to register with the website. So it is very much important to verify whether the website is real or fake. If user registers with a fake website, then this personal information and sensitive financial information like credit card number could be compromised. We asked to the participants whether they are able to differentiate between real and fake websites. The answer is very alarming. Only 20% of the surveyee can differentiate between fake and real website. Figure 6 shows the reflection.

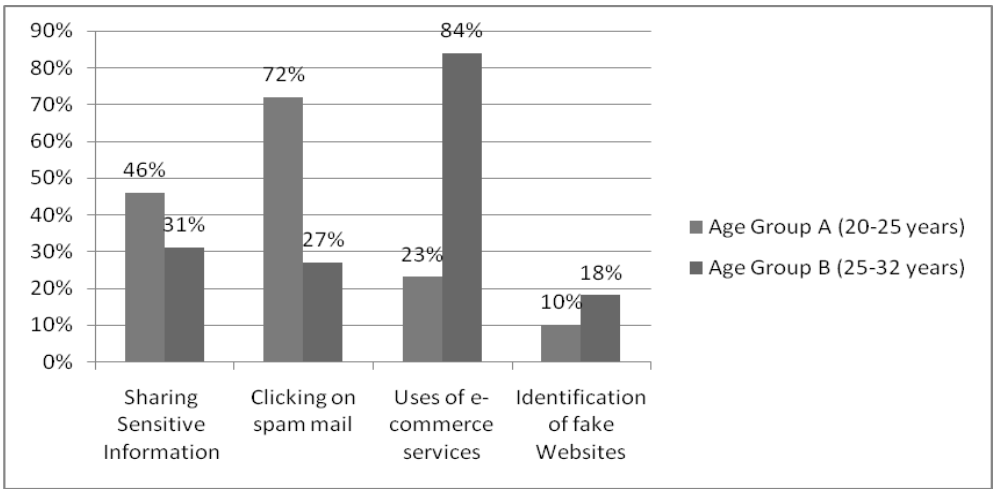
Figure 6: Able to Differentiate the Real and Fake Website



4.2 Age Perspective

in this survey, age of the participants ranges from 20-32 years. We target basically the young people who are actively engaged with the internet all the time. Form our observation participants who are relatively young (20-25 years) are not conscious about their online activities. Whereas people of relatively older age (25-32 year) is more concern about their online activities. Thus this survey indicates that younger people are more vulnerable to social security attacks.

Figure 7: Comparison of Age Group A and Age Group B on different issues



4.3 Gender Perspective

We examined the gender issue of information disclosure. In our survey, we took response from a significant number of female participants. Among them 40% are beginner, 50% are moderate and rest of them are expert users. Our survey shows that 30% of male participants click on the spam mail where 68% of the female participants click on the spam mail (figure 8). So, it clearly illustrate that female users are more vulnerable to spamming. Our survey also exhibits that female users shares more sensitive information than their male counter parts (figure 9). This clearly indicates that female users are more prone to different social security attacks.

Fig 8: Clicking of Spam Mails Sharing

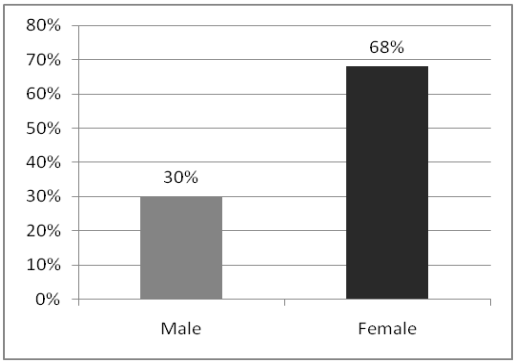
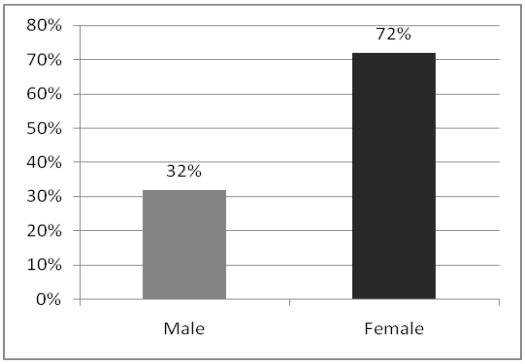


Fig 9: Sensitive Information



5 Experiments and Result

To demonstrate the impacts of information disclose in the social networking sites, we have designed a phishing attacks. We have collected information of 50 students from Facebook. We have collected their email id and favorite movie.

Then we have prepared a phishing mail (figure 10) which says they need to complete a form (figure 11) to get the ticket for their favorite movie (we chose the name of the movie from their profile as subject line of their email) in the nearby

movie theater. We have asked their card number and password to reserve their seats and win a special discount (we have masqueraded a local popular Cineplex).

Figure 10: Sample Free Movie Ticket Attack Template

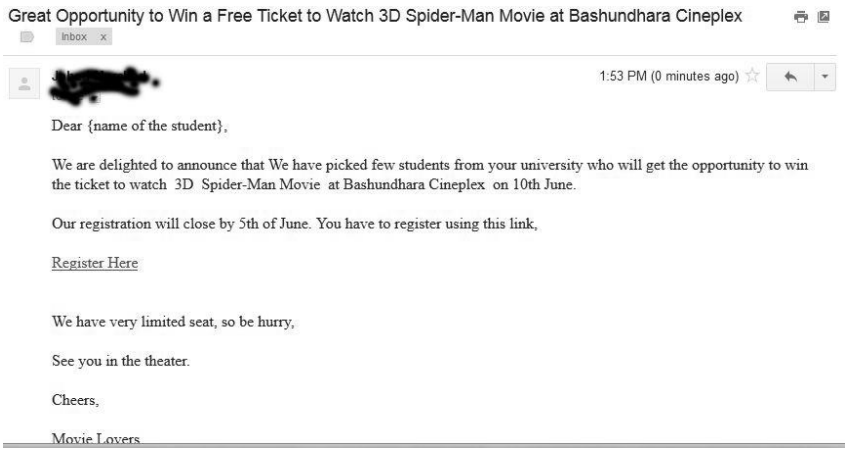
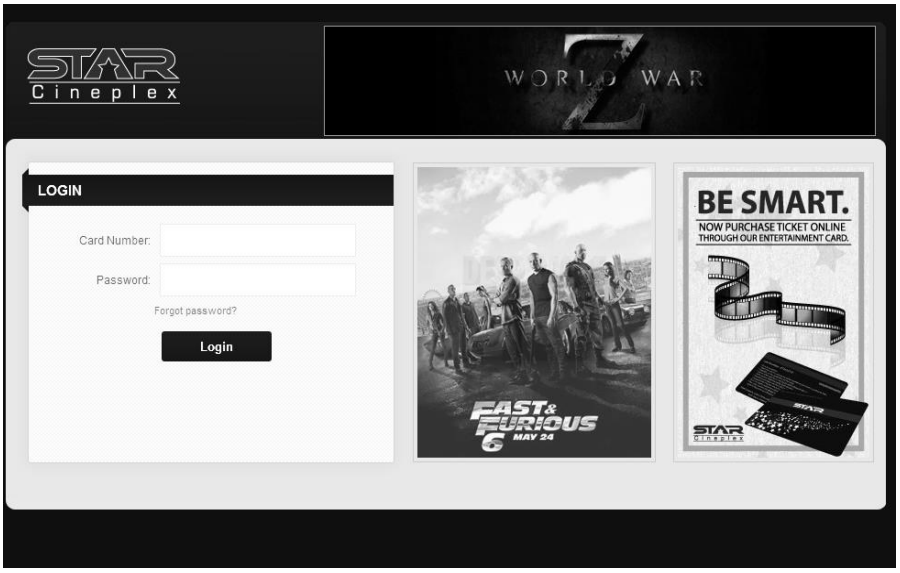


Figure 11: Phishing form to Collect User's Email ID and Password

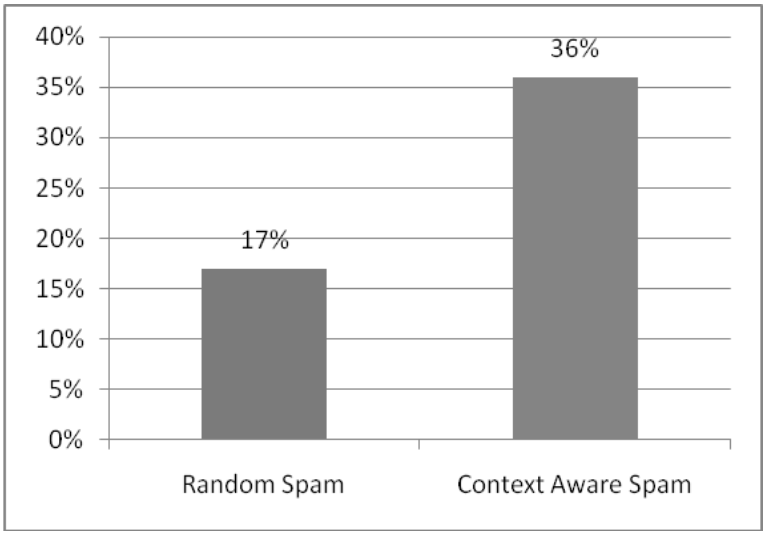


We have also sent them email by promoting a random product. The result shows that a greater number of students open and respond to the email which contains information related to their likings (in this case favorite movie).

5.1 Result

Our experiment shows that phishing and spam mails are more dangerous if attackers use the personal information in the email. Users are more used to open such emails and also provide confidential information. The following table shows the difference between a random spam email (mail without user's context) and social context aware email.

Figure 12: Comparative Chart Random Spam and Context Aware Spam Mails



Thus our experiment clearly demonstrates that social spamming and social phishing (more personally targeted with more personal information in the email) are more dangerous than random spamming and phishing emails.

6 Conclusion

In this paper, we have analyzed social networking sites, for its degree of vulnerability to different kinds of context-aware security attacks. We have presented different kinds of the potential risks for different types of attacks. We have also provided detailed analysis of security attacks and implication on different user groups.

Aspects of Facebook's policies and usage that may make its users vulnerable to sophisticated attacks via context-aware email are also examined. We have run the experiment among 50 university students. Our experiment has showed that users could be more accurately targeted with sophisticated context-aware attack email. Our findings suggest that security awareness should be created among the users, especially among female users about these kinds of social security attacks. Develop a fine grained privacy policy for social network remains as the future work.

References:

Emigh, A. (2005), “Online identity theft: Phishing technology, chokepoints and countermeasures,” *ITTC Report on Online Identity Theft Technology and Countermeasures, 3.*

Boyd, D. M. (2004), “Friendster and publicly articulated social networking,” *In Conference on Human Factors and Computing Systems (CHI 2004), April 24-29, Vienna, Austria*.

Boyd, D. (2003), “Reflections on friendster, trust and intimacy,” *In Intimate (Ubiquitous) Computing Workshop-Ubicomp (Pp. 12-15), Seattle, USA.*

Creese, S., Goldsmith, M., Nurse, J. R., and Phillips, E. (2012), “A data-reachability model for elucidating privacy and security risks related to the use of online

social networks*," In Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on (Pp. 1124-1131), Liverpool, UK.*

Donath, J., and Boyd, D. (2004), "Public displays of connection," *bt technology Journal, 22(4), Pp. 71-82.*

Ellison, N., Heino, R., and Gibbs, J. (2006), "Managing impressions online: Self-presentation processes in the online dating environment," *Journal of Computer-Mediated Communication, 11(2), Pp. 415-441.*

Ellison, N. B., Steinfield, C., and 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), Pp. 1143-1168.*

Fogel, J., and Nehmad, E. (2009), "Internet social network communities: Risk taking, trust, and privacy concerns," *Computers in Human Behavior, 25(1), Pp. 153-160.*

Fouad, M. R., Elbassioni, K., and Bertino, E. (2012), "Modeling the Risk & Utility of Information Sharing in Social Networks," *In Privacy, Security, Risk and Trust (PASSAT), 2012 International Conference on and 2012 International Confernece on Social Computing (SocialCom) (Pp. 441-450), Amsterdam, Netherland*.

Gartner Inc.: "Gartner study finds significant increase in e-mail phishing attacks," http://www.gartner.com/5 about/press releases/asset 71087 11.jsp, April 2004.

Jakobsson, M. (2005), "Modeling and Preventing Phishing Attacks," *In Financial Cryptography and Data Security (Pp. 89-89). Springer Berlin Heidelberg, Germany*.

Krasnova, H., Günther, O., Spiekermann, S., and Koroleva, K. (2009), "Privacy concerns and identity in online social networks," *Identity in the Information Society, 2(1), Pp. 39-63.*

Liu, H., and Maes, P. (2005), "Interestmap: Harvesting social network profiles for recommendations," *Beyond Personalization-IUI, Pp. 56.*