Social Networking Sites (Threats and Attacks)

Dr. M.K. Sharma*

Abstract

Computer users are spending more time on social networks like Facebook, Orkut, Ibibo etc., and sharing sensitive and valuable personal information, but hackers are there to check where you are and where the money is to be use. The dramatic rise in attacks in the last few year warning us that social networks and their millions of users have to do more to protect themselves from organized cyber crime, or risk falling prey to identity theft schemes, scams, and malware attacks. You must aware while working with these sites to safeguard your identity, personal data and financial transactions. This paper will give you some answers of questions about how to better enjoy the conveniences of the digital world of social networking and how to secure one's digital identity and information while surfing, buying, traveling and communicating on these sites. This paper will give you some answers of questions about how to better enjoy the conveniences of the digital world of social networking and how to secure one's digital identity and information while surfing, buying, traveling and communicating on these sites.

Keywords : Social Networking, Digital Identity, Information Safety, Online Threats, Attacks.

1. Introduction

Computer users are spending more time on social networks like Facebook , Orkut , Ibibo etc., and sharing sensitive and valuable personal information, but hackers are there to check where you are and where the money is to be use. The dramatic rise in attacks in the last few year warning us that social networks and their millions of users have to do more to protect themselves from organized cyber crime, or risk falling prey to identity theft schemes, scams, and malware attacks. Targeted attacks against companies are in the news at the moment, and the more information a criminal can get about any organization's structure, the easier for them to send a attachment to precisely the person whose computer they want to break from your side.

It is now more important than ever to be diligent about online security measures as relative threats are prevalent in an increasing number of channels including social networking sites such as Facebook, Orkut. In a recent poll reported by Computerworld and anti spyware development company Webroot, four out of five IT professionals believe web 2.0-based malware will pose the biggest security threat in 2010.

The one common threat is that at the end of the day everyone is concerned about protecting their personal data, their financial

*Assistant Professor & Head (MCA), Amrapali Institute of Management & Computer Applications, Haldwani, Uttarakhand, India

information, and their identity data. So , social networking sites, blogs, social media tools such as Twitter, chat tools, even search engine results are being used to infect end user systems with all sorts of data stealing malware. Users need to be aware that what they say and do on these social networking sites can be tracked. Web 2.0 based social networking sites are biggest security threat for Businesses and individuals. You must aware while working with these sites to safeguard your identity, personal data and financial transactions. This paper will give you some answers of questions about how to better enjoy the conveniences of the digital world of social networking and how to secure one's digital identity and information while surfing, buying, traveling and communicating on these sites. According to Investor's Business Daily, **evil is sweeping social networks**, moving beyond email and blogs to where you like to virtually hang out and congregate:

2. Types of Threats

Last year one virus in particular, called Koobface, is a particularly nasty virus that can do some quite astounding things. It's capable of registering an account (in your name and with your email address on Facebook), verifying the account by logging into your email, then befriending contacts or strangers. Then it posts messages to people, walls and groups full of links to spam sites and other viruses. Others take over your existing account and post messages to all of your friends containing another virus. The advise is you should change password on another computer in case the virus was logging the keys you hit on your computer.

On Twitter, a virus called StalkDaily spread the rather strange ratings of a 17-year-old called Mikey Mooney. Hundreds of thousands of messages were posted across Twitter, making Mikey a celebrity for a day. 61 percent of security chiefs in business consider Facebook the biggest threat to their security. That's not surprising considering how many of us use it.

But there is no doubt that simple changes could make Facebook like sites users safer. For instance, when Facebook rolled out its new recommended privacy settings late last year, it was a backwards step, encouraging many users to share their information with everybody on the internet.

2.1 Think before you click

Other than an up-to-date anti-virus system, think carefully about clicking on any links sent to you by friends on these sites. Is the language of the message a little out of character? Have you heard of the website they're linking to? Like On Twitter, where links often appear using web address shorteners like Bit, then it may be impossible to know where you're going to land until it's too late. That's a big and growing risk.

Security experts last week warned that a new strain of the Koobface virus is hitting Facebook, My Space and other social networking sites. It looks for links and passwords to other social networking sites. Virus creators are increasingly targeting social networking sites and other Web 2.0 technologies such as the micro-blogging site Twitter and instant messaging services from Google, AOL and others. Virus writers are also creating fake profiles of celebrities, real friends or business associates hoping people will link with them. Users can be tricked into linking to the fake profile, which can be loaded with various forms of malicious software.

Some times when you responded to an email from a "friend on Facebook" to visit a link that initiated a program that rifled through your hard drive, may install malicious software and sent the same e-mail to all of your friends through your profile.

Other attack targets included Google Talk, Yahoo and Microsoft Instant Messaging services, and Twitter users. They were sent a message to check out a video or link that required their login information.

Myspace, Facebook, LinkedIn, and other social media tools and networks are becoming the target of an increasing number of Phishing and criminal activity. Unfortunately, many of us continue to fall for these misleading attacks, handing out passwords and personal information, risking our personal identity as well as our privacy and computer data.

Identity theft is on the rise, and it's a lucrative business to disrupt your business and your online life.

3. Data Collection and Analysis about Some Theft Attacks

More than 1.2 million people filed a complaint of fraud, identity theft or a related act to law enforcement or regulatory agencies in 2008, up 16% from a year ago, according to the Consumer Sentinel Network, a branch of the Federal Trade Commission. Financial losses came to $1.8 billion, or about $3,400 per victim reporting a financial loss. Losses of $1 million or more were reported by 257 people.

Identity theft was the top complaint, named by 26% of the complainants. Credit card fraud was the most common form of identity theft, at 20%. Most fraud victims said the initial contact with the crooks came through e-mail or Web site visits.

According to research firm Javelin Strategy and Security, in 2008 about 9.9 million U.S. adults were victims of identity fraud, up 22% from the year before. It pegs the total loss at $48 billion. Most incidents were the result of lost or stolen wallets, checkbooks and credit cards, but online access accounted for 11% of the total. F-Secure reported that the total amount of malware accumulated over the past 21 years "increased by 200% in the course of just one year for the year ending in 2008.

With the big business of security attacks and identity theft come big losses. The financial impact of these cyber crimes is on the rise as well , blogs scams including the danger of exaggerated claims, how to spot a scam and report them, web hoaxes, blogs scams making money from your content and gullibility, get rich schemes, and the growing number of Phishing, fake, and impostors out there on the web pretending to be something they aren't.

Now we may say **threats of the popular social network sites** are:

- Identity theft
- Threats to personal safety such as stalking or threatening either online or in real life
- Social risks through participating in minority groups or stigmatized groups

In a recent study the researchers developed a tool to score the information disclosed on Facebook. This instrument can determine in Facebook profiles what personal information is disclosed and what is not. Next this scoring tool for personal information was used to explore means for examining identity threat.

For this they divided the personal information on Facebook in 3 categories: personal identity information (gender, birth day, birth year, email, and picture), sensitive personal information (email, employer, job position, status, mini-feed, regular wall, picture, photo albums, self-selected photos, tagged photos, message, poke, send a gift, and friends viewable) and potentially stigmatizing information (religious view, political views, birth year, sexual orientation, photos, friends viewable, interests, activities, favorite music, favorite movies, favorite TV shows, favorite books, favorite quotes, about me).

They used a sample of 400 randomly selected, accessible, personal profiles from 8 Facebook networks. Overall in all three categories those revealing their relationship status were also those to reveal more personal information. Those seeking a relationship were at greatest risk of threat, and disclosed the greatest amount of highly sensitive and potentially stigmatizing information

For all three categories as age increases less personal information is disclosed. Older people are more cautious when disclosing personal information.Facebook users who disclosed information about age, gender, relationship status disclosed more information in all three disclosure categories than people who did not disclose this information. Moreover, those who were single also revealed more stigmatizing items. Gender had no influence on these findings. Although women usually disclose more personal information, this difference from men is not present online.

Using facebook for finding a new relationship is probably accompanied by a high threat of identity theft and other social risks, so take care.

4. Attack Scenarios

Social network owners offer encoded and possibly sanitized network graphs to commercial partners and academic researchers. Therefore, we take it for granted that the attacker will have access to such data. The main question is that, can sensitive information about specific individuals be extracted from social-network graphs?

Attackers fall into different categories depending on their capabilities and goals. The strongest can be a **government-level agency** interested in **global surveillance**. Such an agency can be assumed to already have access to a large social network like orkut or facebook. His objective is large-scale collection of detailed information about as many individuals as possible. This involves aggregating the social network data.

Another attack scenario involves **abusive marketing**. A commercial enterprise, especially one specializing in behavioral ad targeting , can easily obtain an encoded social-network graph from the social networking sites for advertising purposes. As described this data may often misinterpreted as privacy. If an unethical company were able to decode the graph using publicly available data, it could engage in abusive marketing aimed at specific individuals.

Phishing and spamming also gain from social-network decoding. Using detailed information about the victim gleaned from his or her decoded social-network profile, a phisher or a spammer will be able to send a highly individualized message to others.

Yet another category of attacks involves targeted decoding of specific individuals by stalkers, investigators, nosy colleagues, employers, or neighbors. In this scenario, the attacker has detailed contextual information about a single individual, which may include some of her attributes, a few of her social relationships, membership in other networks, and so on. The objective is to use this information to recognize the victim's node in the social network and to learn sensitive information about his or her, including all of his or her social relationships in that network.

5. Conclusion

This is the Year of Original Content, a year where we fight back against those who steal our content for their own evil purposes without our permission. Don't let your guard down against those who abuse us in other ways, too. Using Facebook and other social networking sites like Orkut for finding a new relationship is probably accompanied by a high threat of identity theft and other social risks, so take care.

6. References

1. *Alby, Tom. 2007. Web 2.0. Konzepte, Anwendungen, Technologien. München: Hanser.*
2. *Baker, James R. and Susan M. Moore. 2008. Distress, coping, and blogging: Comparing new Myspace users by their intention to blog. CyberPsychology & Behavior 11 (1): 81-85.*
3. *Carroll, Kevin S. 2008. Puerto Rican language use on MySpace.com. Centro Journal 20(1): 96-111.*
4. *Charnigo, Laurie and Barnett-Ellis, Paula. 2007. Checking out Facebook.com: The impact of a digital trend on academic libraries. Information Technology and Libraries 28 (1): 23-34.*
5. *Donath, Judith and boyd, danah. 2004. Public displays of connection. BT Technology Journal 22 (4): 71-82.*
6. *Dourish, Paul. 2001. Where the action is. Boston, MA: MIT Press.*
7. *McGee, James B. and Michael Begg. 2008. What medical educators need to know about "Web 2.0". Medical Teacher 30 (2): 164-169.*
8. *Mitchell, Eleanor and Sarah Barbara Watstein. 2007. The places where students and scholars work, collaborate, share and plan: Endless possibilities for us! Reference Services Review 35 (4): 521-524.*
9. *Moreno, Megan A., Norman C. Fost and Dimitri A. Christakis. 2008. Research ethics in the MySpace era. Pediatrics 121 (1): 157-161.*