Research Journal of Forensic Sciences
Vol. **1(1),** 2-7, March **(2013)** *Res. J. Forensic Sci.*

Review Paper

Social Networking: Its Uses and Abuses

Pooja Shelke[1] and Ashish Badiye[*]
Institute of Forensic Science, Govt. of Maharashtra, R.T. Road, Civil Lines, Nagpur, MS, INDIA

Available online at: www.isca.in
Received 23rd November 2012, revised 25th December 2012, accepted 15th February 2013

Abstract

Social Networks are Web-based services that allow people to construct a public, or somewhat public, profile. Articulate a list of other users with whom they share a connection with friends, family, etc. Social networks not only allow people to meet and communicate with strangers, but they also let users organize and visible their social networks. In many ways, social media has led to positive changes in the way people communicate and share information; however, it has a dark side, as well. Social networking can sometimes result in negative outcomes, some with long-term consequences. There are millions of people on the internet who are looking to meet other people and to gather and share information and experiences on a variety of topics. Hundreds of social networking sites have been created, and have attracted millions of users. In a very short span social networking has become a phenomenon. Most of the key features of these sites are very similar, yet the cultures that form around the social networking sites vary in many different ways. Some of the sites target diverse audiences, while others attract people based on common language, race, sexual preferences, religion, or nationality. The sites also vary the ways in which the show and incorporate new information and communication tools, like mobile access, blogging, and photo and video sharing. Easily the most common use of Social Networking sites, and the main reason for them existing in the first place, is for personal reasons. It is used for its original purpose – to keep in touch with friends. Some people will go on simply to update their status or view their friends' statuses, or to look at photos from the weekend's night out. In the past it would have been nigh on impossible to keep in touch, much less keep up to date with what they are doing. But Social Networking, as coin, has two sides. However useful and creative it may be, but it also has its darker side. The current paper throws some light on a few of the common and popular methods of abuse and various risks faced by the users of social networks and some preventive measures to ensure the safety of person and personal data.

Keywords: Social media, baiting, cross site scripting, pharming, doxing, phreaking.

Introduction

The intensification of the internet age has enabled us to live a life at a faster hop. The younger section of society like children, pre-teens and teens accounts for a very large portion of the internet populace. The same group also accounts for the most rapid increase in internet use. And when this group stays online, the most common thing they do is join social networking sites. In fact, for an average American teen, social networking is basically the same as social media – it absolutely defines how and where teens get to communicate and socialize with other people. What's most intriguing about this revolution is that children and teens are leading the way[1]. But the ongoing popularity (or maybe dependence) on the internet and social networking carries not only positive but also negative effects. First, we have to consider that the web is responsible for making media, society, and our lives in general work faster. Social networking services can provide an accessible and powerful toolkit for highlighting and acting on issues and causes that affect and interest young people. Social networking services can be used for organizing activities, events, or groups to showcase issues and opinions and make a wider audience aware of them. Social networking services rely on active participation: users take part in activities and discussions on a site, and upload, modify or create content. This supports creativity and can support discussion about ownership of content and data management.

Young people who use social networking services to showcase content – music, film, photography or writing – need to know what permissions they are giving the host service, so that they can make informed decisions about how and what they place on the site. Users might also want to explore additional licensing options that may be available to them within services – for example Creative Commons licensing – to allow them to share their work with other people in a range of ways. Collaborators and team players Social networking services are designed to support users working, thinking and acting together. They also require listening and compromising skills. Some may need to ask others for help and advice in using services, or understand how platforms work by observing others, particularly in complex gaming or virtual environments. Once users have developed confidence in a new environment, they will also have gained the experience to help others. Online spaces are social spaces, and social networking services offer similar opportunities to those of offline social spaces: places for young

people to be with friends or to explore alone, building independence and developing the skills they need to recognize and manage risk, to learn to judge and evaluate situations, and to deal effectively with a world that can sometimes be dangerous or hostile. However, such skills can't be built in isolation, and are more likely to develop if supported. Going to a social networking service for the first time as a young person alone can be compared to a young person's first solo trip to a city center, and thus is important for a young person to know how to stay safe in this new environment. Managing an online presence and being able to interact effectively online is becoming an increasingly important skill in the workplace. Being able to quickly adapt to new technologies, services and environments is already regarded as a highly valuable skill by employers, and can facilitate both formal and informal learning. Most services are text based, which encourages literacy skills, including interpretation, evaluation and contextualization[2,3].

Social Networking Positive Effects

We can access information in better way. People who have a childhood and pubescent life minus the internet are faced with the difficulty of getting access to vital information and knowledge they need for education. This means that when you need to do research on something, you have to spend tons of effort and go miles in order to find books, periodicals, and other paper sources just to get started. Additionally, you may also need to conduct interviews and surveys so as to get more information about a certain issue you're tackling. But with the birth of the internet, every single bit of information or knowledge a child or teen needs to learn is compiled in a very large library called the World Wide Web. With social networking, research is a thousand times easier and getting the information you want may be done in minutes.

Social networking provides interactive involvement with other peoples. Long ago, most children and teens were limited to joining community, neighborhood, and school groups. They were not that exposed to events and happenings outside their community. But with social networking and the internet in general, correspondence to virtually anyone from anywhere is possible[4]. Interactive involvement even reaches as far putting children and teens under the spotlight for discussing and participating in online and social networking forums for issues that concern them.

It helps in improving the world awareness. It is quite usual to think that children and teens are not that keen to knowing issues that shape the world. Politics, social problems, population, health, and the economy are things that the younger populace lacks interest in. But because of social networking, they have no choice but to face the world‘s problems and share their opinions. The good thing about this is that their voices are given weight in issues where adults are traditionally the prominent protagonists. With all this positive effects social networking also lead to the hazards and adverse effects of it and are as follows.

Social Networking Negative Effects

It may encourage exploitation and abuse which may lead to the very antagonistic effects on the life of the peoples. We all know that social networking is a product of technology and technology brings new kinds of crime. While many people use it for wholesome, ethical, and healthy reasons, there are also many who utilize it to abuse and exploit others, particularly children and teens. The convenience brought by the web has led criminals to understand that carrying out their trade is much easier and less risky online. The use of fake identities is one advantage these people have in order to be more confident in exploiting and abusing children.

Sometimes social networking will be responsible to behavioral tendencies and consequences. The impact of social media and social networking sites on the behavior of children and teens is very disturbing. We're not saying that social media is bad in and of itself. The misuse of such technology is what makes it bad. For instance, there is the tendency to conform to what's popular without considering whether it's right or wrong - as often seen in cases of cyber bullying. It's much easier for young people to verbally abuse each other online than it is face to face.

Social media is responsible for revolutionizing traditional communication. However, research has shown that social networking sites can be very addictive. People who use social networking sites for their daily communication are hooked to a point that they neglect health responsibilities, especially their diet. The addictive nature of social media leads to eating disorders, obesity, heart problems, sleep disorders, and other pertinent health issues. Additionally, constant exposure to the internet because of social networking addiction prevents a child or teen from engaging in physical activities and socialization. They become so dependent on it that they start to think making contact with other people outside the social network is not necessary. As such, they become socially and physically stagnant.

In actuality, there are more consequences that we have to face as parents when it comes to social media and networking issues. We have to understand that even though that there's no stopping our children from using them, it's possible to maintain control. Trying to force a child to stop using social networking sites will probably not work too well, but a parent that is lovingly and constantly involved in their child's life will have a much better time keeping watch over their online activity. Through this active monitoring, one can at least limit the negative effects.

Dangers of Social Networking

Social Networking is the one area of the Internet that nearly every computer-literate person indulges in these days. It doesn't matter whether it's your company boss, your neighbor, your boyfriend or your girlfriend, everybody's contactable via at least one of the Social Networking portals. However, since these

platforms attract so many people – most of whom are blissfully unaware of the need for online security – they also draw in the cybercriminals who are out to make a fast buck from the unwary users[5]. The threats out there can range from just the basic spam advertisement that we all find in our inboxes, to the more sophisticated scams designed to steal your Social Network account credentials, or ultimately, to infect your computer with a Backdoor. This can result in the loss of your private data and your money, not to mention endangering the people around you also. It is important to understand that by falling victim to these criminals, you are not only endangering yourself, but also the people around you, notably your friends on these Social Networks. To keep yourself safe, you need not only to follow some basic rules yourself, but also raise the awareness of your friends too!

Account Phishing: One of the less technically dangerous security threats emanating from the world of Social Networking is the traditional attempt to Phish for a user's login credentials. As previously seen from Online Banking scams or faked IRS notifications, the attacker sets up a website that is identical to the login page of the targeted Social Network site and then spams a link to it via email or messages purportedly from the Social Network itself (figure 1).

Of course this page has no functionality except to redirect the unwary user to the original Social Networking site after the user has entered their login data. The attacker can then abuse the login credentials that they have gained in numerous ways: i. Sell the credentials on the black market, ii. Gather more information about the attacked individual from their profile, iii. Send more spam via the Social Network platform from the compromised account.

Having gained access to your account, an attacker can now exploit your network of trust. The attacker can impersonate you, sending your friends messages that appear to originate from you, and can also use your friends' trust in you to convince them to follow a link, install a malicious program, or to login to a Phishing site themselves.

Luckily these attacks are relatively easy to spot as these fake login sites do not usually have a valid SSL certificate and the domain name is normally corrupted in some way. However, the non-security-conscious users tend to ignore such indicators – as they are too busy thinking about what 'funny picture' to send to their friends. However, Social Networking sites such as Facebook do their best to make their users aware of these easily detectable attacks. Generally, sites like Facebook tend to inform their users about known threats on their respective security pages.

Losing your Login without Being Phished: Another type of threat that has graduated from simply targeting Online Banking to now attacking Social Networking users are password stealers. These programs inject sections of their code into your browser (mainly Internet Explorer and sometimes Firefox are targeted) in order to steal your account information before it is sent over the network. Since the data is stolen completely inside the browser, the SSL encryption between your computer and the website cannot protect you. However, a valid SSL certificate is presented by the Social Networking site and your browser shows the correct indicators for that. Hence, these attacks are much harder to spot than simple Phishing attacks. Because a password stealer is malware that is installed locally on your computer, a current antivirus solution is the best defense against these attempts to steal your account credentials. Once an attacker has successfully Phished your credentials, it is very likely that they will go on to send links that will install the password stealer onto your friends' machines as well, resulting in exponential propagation characteristics (figure 2)

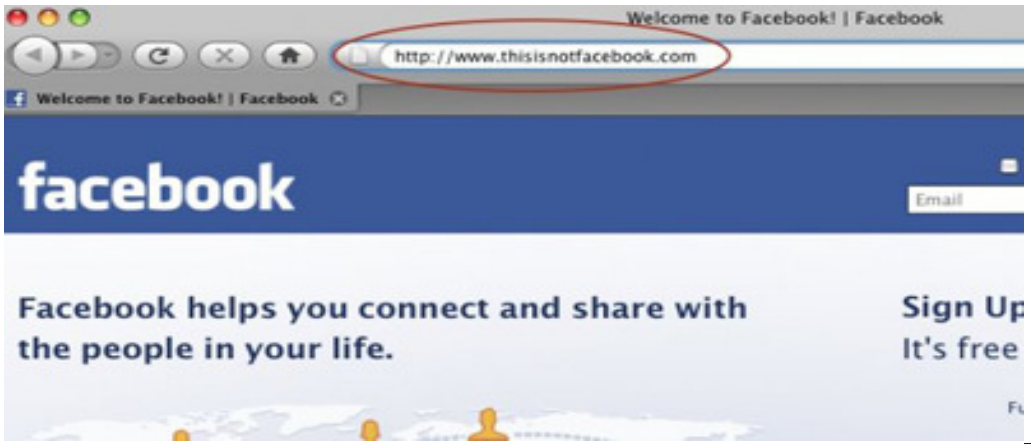

Figure-1
Facebook Phishing Site

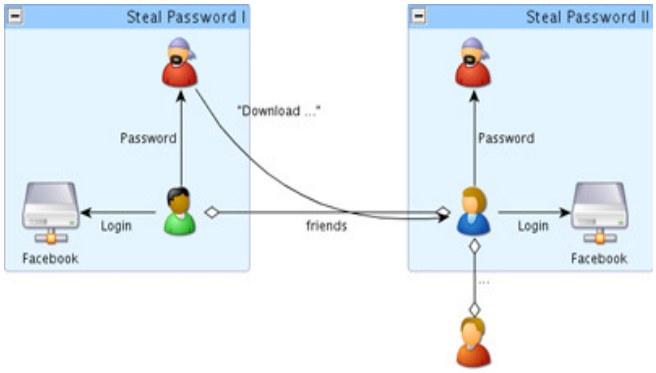

Figure-2
Social Network Password Stealer [PWS] Propagation

Most of the messages sent using the impersonation technique contain a social engineering component that tries to lure the victim (the recipient of the message) into visiting a certain website or downloading a program to their machine. Even if you cannot convince your friends to install a good antivirus solution, you can tell them that they cannot trust links sent by their friends. As these attacks are machine-generated, asking your friends if they really did send you a link is a wise precaution.

One prominent and widespread family of malware that exploits this approach is the Koobface family (an anagram of Facebook), which targets not one, but several Social Networking sites: i. Facebook, ii. MySpace, iii. Hi5 Networks, iv. Bebo, v. and many more according to variant.

Getting Hit in a Drive-By: Sometimes visiting a malicious website is enough to see malware unknowingly installed on a user's computer, as sometimes vulnerabilities in your Browser allow for the arbitrary execution of code — even when Java(Script) and Flash are turned off! Once these pages are visited by someone with a vulnerable Browser, infection is inevitable if no current antivirus solution is present. However, the attacker first needs to attract visitors to such a page. One way is the aforementioned abuse of your network of trust by sending messages purportedly from you, pointing to the attacker's page.

Another route recently adopted by attackers is spamming Twitter and posting comments on Blogger sites containing links to malicious targets. On Twitter especially, the attackers choose the most popular topics of the day and add links to their malicious sites along with their comments (on Twitter there is a concept similar to channels where certain topics are tagged with a hash-sign).

On services like Twitter, where message space is very limited, URL shortening services are very common. Most of these services do not provide a preview function of the URL they're eventually pointing to and therefore an attacker can easily hide behind a semi-trusted name like the URL shortening service's one. This further increases the breadth of the attack.

Who to entrust your data to?: Sites such as Facebook often allow third-party developers to add their own 'Applications' to the Social Networking Site and eventually to a user's profile also. These applications often have full access to your personal data and profile information. The user is asked to consent to sharing their personal data and often can even choose which specific elements of their data they wish to share. But an application that makes use of clever social engineering techniques, just like a Trojan, can get a user to divulge virtually all of their personal data.

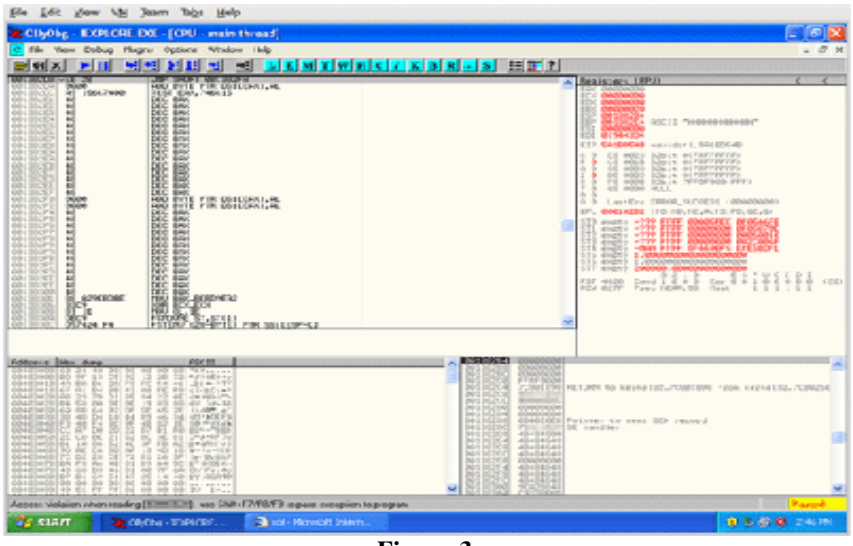

Figure-3
Internet Explorer Code Execution

Thankfully, companies like Facebook are now aware of these issues and therefore manually check any applications before they allow them to be rolled out across their network. However of course, like all companies their resources are limited, and with almost 50.000 custom applications available on Facebook these days, not everything can receive the scrutiny it deserves. Thus you could very well end up enabling a 'Daily Picture' application that displays a different cute kitty every day -- whilst behind the scenes it is accessing all of your personal data. The sad truth is that these days anyone authoring such an application could embed a backdoor that loads JavaScript from a third-party server and eventually leaks all your personal data. If the attacker is skilled enough, the application may very well just slip past the Facebook analyst's watchful eyes unnoticed!

These attacks are very difficult to detect for the average user as the third-party application can integrate itself almost entirely into the trusted Social Networking site in terms of appearance and functionality. Often, an antivirus solution cannot help here either as the third-party application is running server-side on the Facebook network. It really is down to whichever Social Networking site to eliminate these threats. Once information is posted to a social networking site, it is no longer private. The more information you post, the more vulnerable you may become. Even when using high security settings, friends or websites may inadvertently leak your information.

Personal information you share could be used to conduct attacks against you or your associates. The more information shared, the more likely someone could impersonate you and trick one of your friends into sharing personal information, downloading malware, or providing access to restricted sites. Predators, hackers, business competitors, and foreign state actors troll social networking sites looking for information or people to target for exploitation. Information gleaned from social networking sites may be used to design a specific attack that does not come by way of the social networking site.

Tactics

Baiting: Someone gives you a USB drive or other electronic media that is preloaded with malware in the hope you will use the device and enable them to hack your computer. Do not use any electronic storage device unless you know its origin is legitimate and safe. Scan all electronic media for viruses before use.

Click-jacking: Concealing hyperlinks beneath legitimate clickable content which, when clicked, causes a user to unknowingly perform actions, such as downloading malware, or sending your ID to a site. Numerous click-jacking scams have employed "Like" and "Share" buttons on social networking sites. Disable scripting and iframes in whatever Internet browser you use. Research other ways to set your browser options to maximize security.

Cross-Site Scripting (XSS): Malicious code is injected into a benign or trusted website. A Stored XSS Attack is when malicious code is permanently stored on a server; a computer is compromised when requesting the stored data. A Reflected XSS Attack is when a person is tricked into clicking on a malicious link; the injected code travels to the server then reflects the attack back to the victim's browser. The computer deems the code is from a "trusted" source. Turn off "HTTP TRACE" support on all webservers. Research additional ways to prevent becoming a victim of XSS.

Doxing: Publicly releasing a person's identifying information including full name, date of birth, address, and pictures typically retrieved from social networking site profiles. Be careful what information you share about yourself, family, and friends (online, in print, and in person).

Elicitation: The strategic use of conversation to extract information from people without giving them the feeling they are being interrogated. Be aware of elicitation tactics and the way social engineers try to obtain personal information.

Pharming: Redirecting users from legitimate websites to fraudulent ones for the purpose of extracting confidential data. (E.g.: mimicking bank websites.) Watch out for website URLs that use variations in spelling or domain names, or use ".com" instead of ".gov", for example. Type a website's address rather than clicking on a link.

Example: *Most computer infections come from websites. Just visiting a website can expose your computer to malware even if you do not download a file or program. Often legitimate sites may be unknowingly infected. Websites with information on popular celebrities or current sensational news items are frequently hijacked by criminals, or criminals may create such websites to lure victims to them.*

Phishing: Usually an email that looks like it is from a legitimate organization or person, but is not and contains a link or file with malware. Phishing attacks typically try to snag any random victim. Spear phishing attacks target a specific person or organization as their intended victim. Do not open email or email attachments or click on links sent from people you do not know. If you receive a suspicious email from someone you know, ask them about it before opening it.

Example: *In March 2011, hackers sent two spear phishing emails to a small group of employees at security firm, RSA. They only needed one employee to open an infected file and launch the malware. The malware downloaded information from RSA that then helped the hackers learn how to defeat RSA's security token. In May and June 2011, a number of defense contractors' networks were breached via the compromised RSA token.*

Phreaking: Gaining unauthorized access to telecommunication systems. Do not provide secure phone numbers that provide direct access to a Private Branch Exchange or through the Public Branch Exchange to the public phone network.

Scams: Fake deals that trick people into providing money, information, or service in exchange for the deal.

Preventive Measures: i. "Defense in Depth" – use multiple layers of security throughout the computer network. ii. Identify ways you have lost data in the past, and mitigate those threats. Educate employees about those threats and how to change their behavior, if necessary, to prevent future loss. iii. Constantly monitor data movement on your network. iv. Establish policies and procedures for intrusion detection systems on company networks. v. Establish policies about what company information can be shared on blogs or personal social web pages. Enforce the policy. vi. Educate employees about how their own online behavior could impact the company. vii. Provide yearly security training. viii. Ask employees to report suspicious incidents as soon as possible.

Additional Preventive Measures: i. Do not store any information you want to protect on any device that connects to the Internet. ii. Always use high security settings on social networking sites, and be very limited in the personal information you share. Monitor what others are posting about you on their online discussions. iii. Use anti-virus and firewall software. Keep them and your browser, and operating systems patched and updated. iv. Change your passwords periodically, and do not reuse old passwords. Do not use the same password for more than one system or service. For example, if someone obtains the password for your email, can they access your online banking information with the same password? v. Do not post anything that might embarrass you later, or that you don't want strangers to know. vi. Verify those you correspond with. It is easy for people to fake identities over the Internet. vii. Do not automatically download, or respond to content on a website or in an email. Do not click on links in email messages claiming to be from a social networking site. Instead go to the site directly to retrieve messages. viii. Only install applications or software that come from trusted, well-known sites. "Free" software may come with malware. Verify what information applications will be able to access prior to enabling them. Once installed, keep it updated. If you no longer use it, delete it. ix. Disable Global Position System (GPS) encoding. Many digital cameras encode the GPS location of a photo when it is taken. If that photo is uploaded to a site, so are the GPS coordinates, which will let people know that exact location. x. Whenever possible, encrypt communications with websites. It may be a feature social network sites allow you to enable. xi. Avoid accessing your personal accounts from public computers or through public WiFi spots. xii. Beware of unsolicited contacts from individuals in person, on the telephone, or on the Internet who are seeking corporate or personal data. xiii. Monitor your bank statements, balances, and credit reports. xiv. Do not share usernames, passwords, social security numbers, credit cards, bank information, salaries, computer network details, security clearances, home and office physical security and logistics, capabilities and limitations of work systems, or schedules and travel itineraries.

No legitimate service or network administrator will ask you for your password: Do not provide information about yourself that will allow others to answer your security questions—such as when using "I forgot my password" feature. Be thoughtful and limit personal information you share such as job titles, locations, hobbies, likes and dislikes, or names and details of family members, friends, and co-workers.

Conclusion

Along with the benefits, Connolly cautions that students who use social networking tools might pay significant hidden cognitive costs. Facebook, Google, and other web services simultaneously seize and fragment our attention. They can subvert higher-order reasoning processes, including the kind of focus, concentration, and persistence necessary for critical thinking and intellectual development. Some researchers have correlated heavy Internet use with greater impulsivity, less patience, less tenacity, and weaker critical thinking skills. The need to rapidly shift from object to object online can weaken students' ability to control their attention. Prolonged Internet use exposes students to interactive, repetitive, and addictive stimuli that produce permanent changes in brain structure and function. The more one uses the Internet and social media, the better the brain can skim and scan. But research suggests that these gains degrade the capacity for concentration, reasoning, and reflection—in fact the very sort of critical thinking and evidence-based reasoning needed to honestly appraise the full costs of using social media.

References

1. Acquisti, Alessandro, and Gross, Ralph. Predicting Social Security numbers from public data**,** *Proceedings of the National Academy of Sciences*, **106 (27)**, 10975-10980, (**2009**)
2. Adamic, Lada, Buyukkokten, Orkut, and Eytan Adar, A social network caught in the Web**.** *First Monday*, **8 (6)**, (**2003**)
3. Agarwal, S., and Mital, M., Focus on Business Practices: An Exploratory Study of Indian University Students' Use of Social Networking Web Sites: Implications for the Workplace, *Business Communication Quarterly,* (**2009**)
4. Ahmed OH, Sullivan SJ, Schneiders AG, and McCrory P., iSupport: do social networking sites have a role to play in concussion awareness?, *Disability and Rehabilitation*, **32(22)**, 1877-1883, (**2010**)
5. Ahn, Yong-Yeol, Han, S., Kwak, H., Moon, S., and Jeong, H., Analysis of topological characteristics of huge online social networking services, *WWW '07: Proceedings of the 16th international conference on World Wide Web*, 835-844, (**2007**)