The Wild Wide West of Social Networking Sites

E.D Frauenstein[1] and R. von Solms[2]

[1]Walter Sisulu University, Centre for Learning and Teaching Development, East London, South Africa
[2]Nelson Mandela Metropolitan University, Institute for ICT Advancement, Port Elizabeth, South Africa
e-mail: efrauenstein@wsu.ac.za; rossouw@nmmu.ac.za

Abstract

The use of social networking sites has become increasingly popular world-wide. Using social networks, people across the world have access to connect and share information with others from the comfort of their homes. One can establish friendships, contacts, find romance, create discussion topics, join groups, create events and advertise yourself or your business using such sites. However, with every fun and advantageous piece of technology, there is a dark side, especially in an online environment. Social networking sites have opened up many new doorways for cyber-crime and with new users rapidly joining these sites every day, it is important that people are aware and understand the dangers and risks associated when using such sites. The amount of personal information which users willingly share on these sites, poses particular security and privacy problems. The objective of this paper is to warn and alert social networking users of the dangers that lurk on popular sites such as Facebook, Twitter and MySpace. The emphasis is placed on a lack of privacy on the part of the user. Preventative measures and best practices will be suggested to avoid such threats.

Keywords

Social networking sites, social networks, social engineering, human aspects, privacy

1. Introduction

Social networking sites have become ever increasingly popular across the world and internet. It is common to find parents, children, co-workers, celebrities and even the elderly registered on popular websites such as Twitter, MySpace, Facebook, YouTube and LinkedIn. Most people spend their time on these sites updating their statuses, sharing information, commenting, posting, uploading images and viewing friends' updates. These sites have become so popular that they are also available and designed for mobile phone platforms and can be accessed either through mobile applications or the mobile site itself. On the other hand, most users are not aware of the dangers and threats that lurk when using such sites. This paper will present a background into social networking, the dangers associated with using this technology, followed by some basic protection guidelines to help prevent against threats.

2. What is Social Networking?

According to SocialNetworking.com, social networking is the grouping of individuals into specific groups, e.g. small communities or a neighbourhood. This may be further subdivided into individuals, societies and companies. Although social networking is physically possible in person e.g. in the workplace, universities etc. it is most popular online. The latter is because the internet is filled with millions of individuals who are looking to meet other people, to gather and share information and experiences on a variety of interests e.g. sport, friendships, relationships and professional alliances. In an online social networking context, websites known as social networking sites are used as a platform to satisfy some of the interests mentioned. Popular social networking websites are: Facebook, MySpace, Twitter, Friendster, LinkedIn, Flickr, YouTube etc. Social networking websites function much like online communities of internet users. Once a registered member, one can begin to socialize with other members using these sites. This socialization may include access to profile pages of other members and possibly even contacting them.

3. Dangers Associated with Using Social Networking Sites

Many people may ask: Why is my profile account hacked? How and for what purpose? There is a number of reasons why the threat would want to compromise one's account. Understanding these reasons often requires placing oneself in the position of the threat however most threats relate to poor privacy practice on the part of the user. Users are willing to share almost any type of information about themselves and even to strangers. Social engineering attacks, lax security practices, weak passwords and design problems with the site itself can undermine the privacy protection users rely on (Mills, 2010). Furthermore, users who fall for phishing scams and who have their accounts hijacked have everything within their account exposed to threats that can then use the data for identity fraud or to target the victim's friends, through the site, using social engineering techniques. Below are common threats which users are exposed to:

3.1. Sex Offenders/Paedophiles

In general, the internet has a large amount of sex predators (Department of Justice, 2005) who are taking advantage using social networking sites and other technologies to lure children and even adults to them, without having to physically reveal their true identity prior to physical contact. Children are at risk and should preferably not be using the internet without some form of parental supervision. This is difficult to control if the internet is easily accessible through other technologies such as most mobile phones and even gaming systems such as Sony Playstation 3 (PS3's) and the portable version, PSP's. Parents may also not be entirely computer literate or internet "savvy" as most young children assumingly are. Most social networking sites have a minimum age limit upon registration. However, it is easy to fool these systems. Registration on these sites is free, therefore requiring no credit card. There is no authentication other than a confirmation e-mail link sent to one's e-mail account. For a child to gain access, they can simply supply their e-mail address, an incorrect birth date and agree to the terms and conditions. Ironically, as easy as it is for a child to

falsify his or her age and information online, it is equally easy for the potential predator to also do the same. The sex offender lures the child by pretending to have similar interests, age, activities and hobbies as the child. Arguably, the typical attributes of a young child are: curiosity, loneliness, vulnerability, trustworthiness and friendliness. These attributes will be exploited to allow the predator to take advantage of the child. Ultimately, the child's main purpose for using these sites is to gain popularity amongst peers and to also create new friendships. Children see sexual and revealing pictures on Facebook and MySpace profiles, and may feel it is acceptable to do the same thus unintentionally attracting paedophiles. In New York state, it is required that sex offenders register their email addresses as well as any other online aliases. Facebook disabled 2782 and MySpace 1796 registered sex offenders of that specific state alone (NetFamilyNews, 2009; Bray, 2009). Some of the sex offenders were registered on both the social sites mentioned. This is a small portion considered with the rest of the world. Other countries and other states may not have such laws and not all sex offenders will honestly register themselves.

3.2. Lack in Good Online Privacy Practice

As previously mentioned, sharing too much information may allow a sex offender to determine where one lives. Therefore, it is important to minimize the amount of information shared on these sites. To be a member of popular social network sites, in any context, raises concern for privacy issues. The representation of oneself online, allows one to be susceptible to threats from anywhere in the world. Since one has the ability to control whom one is friends with on these sites, it is easy for users to have a false sense of security about the privacy of their information. People are not aware what consequences could follow, caused by over-divulging their character online. According to scientists at University of Texas, Austin (indianexpress.com, 2009) user profiles on social network sites, like Facebook, convey accurate images, information and personalities of the users. This breaks the assumption that most people "fake" themselves on these sites. This presents a problem that if most people portray such accurate descriptions of themselves; this will in return benefit threats.

Australian security firm Sophos, has established what most information security research had already confirmed - humans are the weakest link in information security practice (Mitnick and Simon, 2002). According to a study conducted by Sophos, (Reisinger, 2009a) to see how likely Facebook users were to offer up personal information, 41 to 46 percent of the 100 users "blindly accepted" friend requests from two fake Facebook users created by the security firm. After becoming friends with Sophos, the security firm was able to access up to 89 percent of the users' full dates of birth, all of their e-mail addresses, school attended etc. Half of all the users displayed their town or suburb as well as information on family and friends. According to Sophos, this is potentially a good starting point for scammers and social engineers.

Many fun activities such as creating photo albums, instant messaging, posting comments, supplying accurate information, notes and videos allow social sites to be appealing to both young and old. In some way, it also misleads the user into assuming that it is acceptable as the objective is to create a unique profile. Having a fully detailed and accurate profile has its advantage in allowing friends to easily

detect/locate your profile and vice versa; on the other hand, this builds a culture of weak information security practice to both users and organizations (Thomson et al. 2006). Users do not realize that their profile information can be accessed by total strangers who happen to be in the same social groups or network proximity unless they specifically change their privacy settings. In Facebook, it is possible to view a stranger's entire profile even if one is not friends at all with that particular person. This had caused such concern that in late 2009, in response to user feedback, Facebook interrupted their homepage with a window which allowed the users to review their current privacy settings and to configure their privacy settings i.e. to hide their friend lists, hide certain information, prevent outsiders to view photo albums etc. One could either strengthen their privacy settings or keep the original settings. The options were considered confusing (Needleman, 2009) and consequently many people were inclined to keep their default settings, which are set to make the data visible to the web rather than opting to strengthen their security. Since the user has a choice in this regard and is not aware of the potential dangers, this has still not completely resolved the privacy issue. Furthermore, this was possible only through the main Facebook website and not the mobile version site. This suggests that the design of the social networking site itself should also limit what users are able to share. To elaborate, these sites have fields or areas in which they allow users to add personal details (Gross and Acquisti, 2005) about themselves on their profile such as: parent names, siblings, marriage status, schools, universities and websites - all pieces of information that are commonly used in identity fraud. In LinkedIn.com for example, it also indicates the information completeness of one's profile with a progress bar displaying completion percentage. It also encourages one to add sensitive personal information such as one's entire curriculum vitae, current and past working experience and contact details. Many social sites, including LinkedIn, have allowed users to add plug-ins to other social networking sites such as Twitter. This allows status updates to be instantaneously updated across the member's other registered social network aliases. Furthermore, most websites and organizations, in some way, have openly displayed their affiliations with other social networking sites displaying a brand icon/logo. After concluding presentations, presenters also openly display their affiliation with social network sites icons along with usernames, to form part of their contact details.

It is possible to "tag" friends using any images, which will then be automatically added to the live news feed as well as photo gallery of the user for all affiliated friends to view. One has to regularly visit your account and rectify should there be a problem by un-tagging such images. In Facebook, the "mutual friends" display also deceives one into assuming that a stranger is trustworthy. Some people may accept a stranger's friend request just because that person supposedly is friends with your friends. Some use social networks purely for business purposes. Individuals upload photos and videos to market themselves and/or their business. However, this presents a problem to retain the copyright to their work as almost anyone can copy and distribute it electronically. Typically, people who would be concerned about this would be professional photographers, models, artists, musicians and celebrities etc. Uploading this material may be a great way to market oneself and to establish new business connections; however, the internet may end up "owning" the material. Another privacy issue is that if one has a listed social networking profile, it can be easily indexed globally by anyone by simply typing one's full name into a search

engine e.g. Google, Yahoo. Profile lists are made available or "leaked" to popular search engines through the social network site itself. This method allows quicker access for threats to seek out a victim. Using Twitter, for example, anyone can view one's comments (tweets) through the search engine results without having to be a registered member, at all, of the social site in question.

Most users enjoy conveniently accessing Facebook through their mobile phones for the convenience of portability, simplicity, and reduction in access time. If one is using a Facebook mobile application, it may display one's brand of mobile phone from which the status or images was updated e.g. Blackberry. MXit, a popular mobile phone instant chat messenger in South Africa, is following the trend of popular social networking sites by allowing users to also: update their status, add a profile picture, set a mood etc. In fact, most popular instant chat messengers have some of the capabilities that social networking sites make use of.

If current privacy issues in social sites are already a concern, the future may be worse. Philip Langley and Matthew Buckland (matthewbuckland.com, 2009) undertook an investigation into how social networking may work in the future. Their investigations were inspired in particular by augmented reality concept drawings of social networks accessed through mobile phones. According to Langley and Buckland, applying a social networking paradigm with augmented reality in future may create amazing resolutions, facial and object recognition, and more accurate GPS for mobile phones. They envisage that anyone could hold up their phone or other digital device against a person one has just met or randomly passed by. One would instantly have information returned about that specific person within seconds, from an automatic web, public profile and social network search. One could discover common friends, talking points and then have the ability to add him/her to one's network. Using a semantic scan, one could discover negative or positive comments on Google or elsewhere relating to this individual. This would result in instant insight into the person standing right in front of you. Langley and Buckland envisage connecting into public databases and directories and discovering users' locations and how one is affiliated with a member. They acknowledge that privacy has always been an issue for current and future concern and hence they are in the process of working out the ethical and moral framework around their concept.

To conclude, most stakeholders of these sites would perhaps argue that to prevent all of the above-mentioned privacy concerns, simply refuse to accept strangers' friend requests, delete people you dislike or configure your privacy settings. However, social networking sites themselves could also practice privacy in the design and controls of the site itself to prevent users from unwittingly sharing their private information, as users may not understand how to configure privacy settings or the risks involved with sharing their personal information.

3.3. Reputation and Employment at Risk

From the privacy concerns mentioned, individuals need to remember that when having fun on social networks, almost any other registered member of the site may see what one is sharing. As mentioned, one may tag friends in photo albums which

would result in their friends (a possible stranger) to have access to that album (which is yours) even if they are not listed as your friend. Using Facebook, rude comments on your wall or friend's wall allow easy viewing by all other connected friends. Gareth Cliff, a popular South African radio personality, outraged the public and fans when he posted rude and inconsiderate statements (tweets) on the Twitter social site of the late Dr. Msimang (Rainha, 2009). Uploading and posting pornographic, edited, or sensitive images of the user for everyone to see can be extremely embarrassing and damaging. Albums may display social activities of the weekend e.g. parties and drinking, all of which will be added to the live news feed for all friends to view and access. Therefore, one should reconsider sharing this as work colleagues may view and distribute this and could result in loss of job or a damaged reputation. Before an interview, companies may conduct an online search using your name on a social network or search engine to obtain insight into one's behaviour, activities etc. Students using social sites can be turned down by employers for jobs, internships and even interviews because of the information employers can uncover on their social networking profiles. Inappropriate images, rude statements or other information on student social networking accounts may damage students' chances of obtaining employment. Employers may take the images that students portray on social networking sites very seriously as a reflection of their personal character.

Since a threat does not have to have much prior knowledge into hacking systems, anybody has the capability to be a threat. Once the threat has access to one's profile, they will immediately change your access details i.e. username, password so that one can no longer access your profile. They can either attempt to destroy your reputation by sending out insulting and rude messages to your friends' lists or, steal your identity (identity theft) posing as you to lure your friends. Posting rude status updates either about you, your friends, people or even the employer is also possible. The helpless victims can do nothing as they cannot access their profile to inform their friends that their account has been hijacked. This will all ultimately damage one's reputation, destroy friendships and even perhaps result in legal action against you. Facebook administration can suspend one's account should they detect any abuse on the site but often it is too late. As mentioned earlier, once information is posted on the internet, it can be seen as permanent because the internet may end up "owning" that material without end. To elaborate, should people have copied the sensitive images, information or comments to a document, it can be easily distributed through email or uploaded to another website.

3.4. Anti-Social Behaviour

Since using popular social networking sites is designed to be fun, simple and arguably addictive, users may be spending too much time using them. This consumes time and may result in a lack of work being done during office time. People may develop anti-social habits as they may seem to struggle to distinguish between the "virtual world" and what is real. They may feel it is acceptable to communicate using the social site itself instead of in person or telephonically. Since these sites are also designed for mobile phones, people may, in addition, have anti-social behaviour during private time as well.

3.5. Account Hijacking

Upon registration on the Facebook site, it is required that one registers with a valid email address and password. In Facebook, this address is used, by default, as a username for logging in purposes and is also displayed on the user's profile. This is the first entry point for a threat to hijack the user's account. All that is further required is the password. If the user has displayed their birth date on their profile, the threat could test that credential as a possible password. MXit, a popular instant chat messenger in South Africa, has improved their security by allowing users to have as a username, in comparison to the past (by default), one's mobile number. The latter was to prevent threats from hijacking accounts as the mobile number alone, was not unique enough.

3.6. Rogue Applications and Marketers

Facebook has the capability for users to add/install applications within one's profile. In general, users should be cautious of trusting unknown applications as these are mostly third party developed software applications which can violate the privacy of your information by accessing one's profile information such as telephone number, street address etc. According to Mills (2010), marketers have been collecting information from social network sites. Unlike spyware, the software used to capture this information has been stealth installed onto a user's computer to collect marketing data. Since users often post information such as favorite movies, TV-shows, music etc. to update their profile, this may result in them becoming unwanted targets of marketing attempts (Tacita, 2007). Thus, posting personal information on social networking sites may be useful tools for identity thieves. Mills (2010) continues that the relationship between the applications and advertisers can also cause problems. Adding an application allows it to show advertisements inside the Facebook domain, which can leak the user's profile information to the advertiser. Cookies and other browsing tracking technology combined with data from social networks can be used by marketers to identify users for targeted advertising and other purposes. Once marketers know a specific person's user name, they can use that identifier in the URL to acquire a user's public profile page.

3.7. Scamming

Social engineering techniques, such as phishing (see: 3.9 Phishing), are a problem for social networks because the trust that users have for messages and posts from friends can be easily exploited by scammers. The scammer could use one's profile (through account hijacking or a virus) to lure and deceive friends by sending them spam messages. Since the recipients trust you, as they are your friend, they would be lured to click on the links, either within an email (see: 3.9 Phishing) appearing to originate from Facebook (Reisinger, 2009b), or within the social site itself in messages or posts, which could lead them to a website to capture financial information. Scams, in general, are mostly financially motivated and cause people to lose large amounts of money. An example is the "I need money" Facebook scam. The threat creates this scam by accessing one's Facebook account and posts a plea for help on one's Facebook profile thus luring your friends. As mentioned earlier,

threats may change your username and password, locking you out of your own account. Afterwards, they target your social friends by sending them anything from: spam, weight loss plans, lottery claims, links that install malware and steal passwords, fake messages stating a friend is stranded in another country and requiring financial help. The friend obliges and sends money to the account the hacker has set up for this particular scam.

3.8. Viruses

The biggest malware risk is Koobface (Mills, 2009a), an anagram of Facebook, which is a worm that targets social networking sites and affects Windows-based computers. Once a computer is infected, it hijacks the Facebook account and sends messages to other friends of the victim, enticing them to click on a link, much like phishing (see: 3.9 Phishing). The link redirects to a web site where they are prompted to download software in order to be able to accomplish a task e.g. to watch a video one must download Macromedia Flash Player. In this case, it is illegitimate software (malware), which infects the system, blocks access to security sites and can be used to steal sensitive information from the computer, such as credit card numbers etc. Infected machines can then be used to spread the worm to other users on Facebook, send spam and distribute fake anti-virus alerts or advertisements. Koobface, can automatically create new profiles using the infected machines and steal passwords.

3.9. Phishing

One method of acquiring information is through a social engineering technique known as phishing. As mentioned earlier, this is predictably scamming (see: 3.7). There is an increase in phishers or scammers using social networks and instant messengers to acquire sensitive or personal information from users (Bilge, 2009; Brown, 2008; Gibson, 2007; Leavitt, 2005; Unisys, 2008). This information can be used for identity theft, financial gain and crime. Typically, phishing involves a fraudster who sends an email masquerading as a legitimate entity, usually a financial institution. The email lures the user to click on a link which then directs the user to a fake/spoofed website that looks identical and legitimate in design to the original site, deceiving the user into submitting personal information and consequently capturing the details. Users of social networking sites can fall for phishing attacks (Mills, 2009b) by clicking on links in messages or e-mails purportedly coming from friends that redirect them to a fake (spoofed-website) log-in page.

4. A Basic Protection Plan to Safeguard against Social Networking Threats

From the threats outlined above, a basic protection plan can be followed to protect users of social networking sites. This plan can be categorized as: Technical Measures, Behavioural Measures and Awareness. Guidance as to how each of these aspects can be applied should be undertaken.

4.1. Technical Measures

There are a number of technology controls that one can apply to safeguard users against threats mentioned above. Threats entail finding new weaknesses in technology and in this context- social networking sites. Some technological - related methods that threats use are: instant messengers, spam, phishing, scams, email attachments containing a virus, fake websites. The following briefly mentions some common technology controls that can be applied to protect against these threats.

4.1.1. Anti-virus and Anti-malware Software

Besides its primary function of scanning for virus signatures, most anti-virus software can also analyse posts or tweets, monitor malicious URLs/links, block malware and detect most phishing websites (Software Informer, 2009). Some antivirus software can analyse posts for malicious URLs and can detect and block malware (Mills, 2009c). As mentioned earlier, some dangers of social sites include viruses lurking on these sites. The anti-virus program can also remove key-logger Trojans - a virus used to monitor keystrokes from the keyboard. Under this category, anti-spyware and anti-malware programs also form part of a defence against threats. It is crucial that the anti-virus program be regularly updated (see: 4.1.4 Software Updates) in order to detect current threats e.g. Koobface, Kneber Botnet or other malware. If infected it is essential to reset your password and notify friends who may have been affected.

4.1.2. Web Browser Software and Internet Browsing Practice

The modern Internet web browser has the built-in capacity to identify most spoofed-websites which are a concern for phishing. Common modern web browsers such as Microsoft Internet Explorer 7 and 8, Opera 9.5, Firefox 3, and Safari 3.2 etc. feature an anti-phishing blacklist which can detect most phishing websites (TopTenReviews, 2009). One should regularly check the address bar on your browser to validate if one is on a legitimate site upon entering your credentials. Depending on the browser used, an icon to be aware for is the “lock” which indicates the Secure Sockets Layer (SSL) certificate. The latter indicates that one is in a secure zone when entering sensitive information i.e. logging in and passwords. One should ensure that one is entering a legitimate website by inspecting the URL in the navigation bar e.g. the Facebook.com domain and pay particular attention to the browser alerts/warnings. Practice a good policy during and after browsing the internet, such as manually approving cookies or only keeping cookies until the browser is closed. Disable flash cookies, clear your internet browsing history, cache and delete internet files. Browser extensions are also available and can assist in this regard.

4.1.3. Network Security

Organisations can prevent their employees from spending most of their time on social networking sites during office hours (see: 3.4 Anti-Social Behaviour). If properly defined through settings, the firewall also prevents employees from accessing illegal or unwanted websites (phishing sites) and social networking sites.

The organization could block social sites completely or until a certain point of the day as a policy. The firewall has the capability to block unauthorised entry from outsiders as well as to perform content filtering (WindowSecurity.com, 2002).

4.1.4. Software Updates

Irrespective of the type of operating or application software used, i.e. commercial or Open Source, most software in a computer system should be regularly updated (Vasser, 2009). Most modern software products such as: application, utilities and system software, can be automatically updated online through websites to receive crucial software security updates. These include updates and upgrades to web browsers and the operating system software e.g. Windows XP, Windows 7. Failure to do so creates an opportunity for viruses, e.g. Koobface, to either pose as an application or warning notification, thus acquiring personal information.

4.1.5. Email Client

Some email clients have the capability to filter spam messages from legitimate messages, thus reducing the threat of a user accessing a phishing email or a scam. Most spam contains some form of phishing. Do not reply to emails that request you to submit your username or password and beware of scams. No organization would request one to submit usernames or passwords. If unsure, rather forward the email to the relevant party or authorities or contact them directly to inquire whether the request is indeed true. Beware to open attached files from unknown sources as it is most likely a virus.

4.2. Behavioural Measures

The greatest weakness through which threats can gain personal information is through a user's weak information security practice i.e. the Human Factor. Threats can be minimized if users can practice the following:

4.2.1. Avoid over-sharing personal and unnecessary information (Privacy)

Supply as little information as possible. Avoid putting up information such as occupation, e-mail address, employer, marital status, home address, sexual orientation, birth date, social security number etc. This is also unnecessary and will cut down on unwanted junk mail (spam) and also prevent threats from using this personal information to acquire your password. Pictures of pet names, location and other friends add to the ease of identifying all of one's personal info. The birth date, for instance, is a credential that many people use as a password. Limiting your information will also prevent anyone to find/track you, friends and family, especially children. If people need to contact you, they could send you a private message through the social networking site which does not require any information.

4.2.2. Evaluate your online profile representation

Evaluate your social networking profile and postings. Ask yourself-how do you feel about your employers, parents, colleagues and friends viewing what you have posted? Do not post anything (e.g. comments or images) that might be embarrassing to you, your family or workplace as it may damage your reputation. Assume that whatever one is posting, will be seen by the entire world as it is indeed on the internet. Choose carefully the friendships that you accept (see: 4.3.2) as they may make obscene or rude comments on your profile which you may not want other people to see. Think carefully before joining particular online groups, fan pages or petitions as that may also allow people to perceive your character or beliefs differently. If a friend is posting foul language, rude pictures etc, consider removing them from your friendship list as it may affect your reputation should they comment on your profile as well, or tag you in some random offensive pictures.

4.2.3. Review existing privacy settings

Regularly review your current privacy settings so that important information is not shared with friends or strangers e.g. if using Facebook, click on the pencil icon in the "friend's box". One should remember that strangers can see certain information on your profile depending on your privacy settings and friendship network. Search your name in a popular search engine to see how your name or identity is being used. Use unique logins and passwords for each web site you access especially social networking sites. Change them often and use strong passwords e.g. a combination of capital with special characters, as a brute-force attack can be used to guess passwords.

4.3. Awareness

In general, information security awareness, as well as the above-mentioned aspects, needs to be instilled in the minds of users when sharing confidential information especially when using social network sites. In fact, an information security culture needs to be adopted. Users need to be aware of all of the above-mentioned dangers which have been outlined in this paper.

4.3.1. Be cautious when adding social site applications

Be cautious when adding applications to your social networking profile. If you wish, research the developers and perform web searches to see if anyone had complained about the application. Ask yourself whether the application brings any benefit to your profile and image. It may indirectly damage one's reputation e.g. an application in a form of a game to determine how much booze one can drink to beat your friend playing the same game (see: 3.3 Reputation and Employment at Risk).

4.3.2. Do not accept friend requests from strangers

One should not blindly accept friend requests from strangers, no matter how innocent or good looking they seem from their profile information or images. Such should be the case even if they have mutual friends listed; the threat could have randomly added users and ones very own friends. If unsure, rather check the invitee's profile and determine if they are indeed who they say they are. One can determine this from conversations that other people have been posting to the threat on their profile e.g. Do I know you? Have we met before? Who are you?

4.3.3. Do not fall for scams or phishing emails

If one should ever receive a message from one of your social networking friends asking for financial help, it is most likely a scam. Be wary of unusual stories or offers that seem too good to be true. Instead, verify information with sources directly. Be cautious of any message, post or link that looks suspicious, requires an additional log-in or asks you to download or upgrade software. Do not click on links or open attachments in suspicious e-mails that appear to originate from a social networking site. One can notify all your friends on the site about the scam, by sending them a message with a link or posting on their wall/status describing information about the scam.

4.3.4. Parental Supervision

Parents should not allow children, especially under the age of 13, to be on social network sites or any other websites that exposes the user to potential paedophiles. To achieve this requires supervision from the parent however; this is not easy as the parent cannot constantly be with the child. An alternative and reliable option is to use parental control software e.g. SpyBuddy. Website visits, emails and instant messenger conversations can all be monitored without the child being aware, and in addition access to certain sites may also be blocked.

5. Conclusion

Social networking sites are fun; however, one must recognize that threats are constantly searching for new tools and techniques to access personal information. It has been established that the majority of the threats rely and expose the human element the most. Therefore users should be vigilant to ensure that strict technical, behavioural measures are understood and in place to prevent potential threats when using such sites. As social sites rapidly evolve, so do threats attack methods and techniques, therefore the basic protection plan mentioned may in future need to undergo re-evaluation to ensure its effectiveness.

6. References

Bilge, L., Strufe,T., Balzarotti, D. and Kirda, E. (2009). 'All your contacts are belong to us: Automated Identity Theft Attacks on social networks', International World Wide Web Conference Committee (IW3C2), ACM, Madrid, Spain, pp 551-560.

Bray, C. (2009), '3,500 NY Sex Offenders Taken Off Networking Sites', Available from: <http://money.cnn.com/news/newsfeeds/articles/djf500/200912011636DOWJONESDJONLINE000416_FORTUNE5.htm> [Accessed: 12 December 2009].

Brown, G., Howe, T., Ihbe, M., Prakash, A. and Borders, K. (2008). 'Social Networks and context-aware spam', Proceedings of the ACM 2008 conference on computer supported cooperative work, ACM, San Diego, CA, USA, pp 403-412.

Department of Justice (2005), 'Protecting Children from Online Exploitation and Abuse', Available from: <http://www.projectsafechildhood.gov/publications/part2.pdf> [Accessed: 19 February 2010].

Gibson, R. (2007). 'Who's really in your top 8: Network security in the age of social networking', SIGUCCS Conference on User services, ACM, Orlando, Florida, USA, pp 131-134.

Gross, R. and Acquisti, A. (2005). 'Information Revelation and Privacy in Online Social Networks', WPES, ACM, Alexandria, Virginia, USA, pp 71-80.

Indianexpress.com (2009), 'Social networking sites reveal users' true personality', Available from: http://www.indianexpress.com/news/Social-networking-sites-reveal-users---true-personality/549935 [Accessed: 12 February 2010].

Leavitt, N. (2005). 'Instant Messaging: A new target for hackers', IEEE Computer Society Press. pp 20-33.

Matthewbuckland.com (2009). 'The Future of Social Networking, with augmented reality', Available from: <http://matthewbuckland.com/?paged=2> [Accessed: 20 January 2010].

Mills, E. (2009a). 'Facebook fights new Koobface worm, another rogue app', Available from: <http://news.cnet.com/facebook-fights-new-koobface-worm-another-rogue-app/> [Accessed: 10 December 2009].

Mills, E. (2009b). 'FAQ: Recognizing phishing emails', Available from: <http://news.cnet.com/8301-27080_3-10396786-245.html> [Accessed: 12 December 2009].

Mills, E. (2009c), 'Kaspersky tool detects malware in Twitter Links', Available from: <http://news.cnet.com/8301-27080_3-10386144-245.html> [Accessed: 12 December 2009].

Mills, E. (2010). 'Using Facebook and Twitter Safely', Available from: <http://www.zdnetasia.com/insight/security/0,39044829,62060259,00.htm> [Accessed: 02 February 2010].

Mitnick, K.D. and Simon, W.L. (2002). 'The art of deception – controlling the human element of security', Indianapolis, Indiana : Wiley Publishing, Inc.

Needleman, R. (2009). 'How to fix Facebook's new Privacy Settings', Available from: <http://news.cnet.com/8301-19882_3-10413317-250.html> [Accessed: 13 February 2010].

NetFamilyNews (2009). 'NY Predators deleted from Facebook, MySpace', Available from: <http://www.netfamilynews.org/labels/social%20networking.html> [Accessed: 08 January 2010].

Reisinger, D. (2009a). 'Study: Facebook users willingly give out data', Available from: <http://news.cnet.com/8301-17939_109-10410257-2.html> [Accessed: 10 February 2010].

Reisinger, D. (2009b). 'Fake Facebook e-mail contains Trojan', Available from: <http://news.cnet.com/8301-17939_109-10384028-2.html> [Accessed: 13 February 2010].

Rainha (2009). 'Gareth Cliff creates Twitter Storm', Available from: <http://www.jucy.co.za/2009/12/gareth-cliff-creates-twitter-storm.html> [Accessed: 13 February 2010].

Software Informer (2009). Security and Privacy / Anti-virus Tools at Software Informer. Available from: http://anti-virus-tools.software.informer.com [Accessed: 17 April 2009].

Tacita, L. (2007). 'MySpace and Facebook -The Dangers of social networking', Available from: <http://webupon.com/web-talk/myspace-and-facebook-the-dangers-of-social-networking/> [Accessed: 12 December 2009].

Thomson, K.L., von Solms, R. and Louw, L. (2006). 'Cultivating an organizational Information Security Culture', Computer Fraud and Security.

TopTenReviews (2009). 'Internet Browser Software Review 2010', Available from: <http://internet-browserreview.toptenreviews.com/> [Accessed: 20 November 2009].

Unisys (2008). 'Unisys Identifies Five Security Issues Likely to Emerge Across Multiple Industries in 2008', BusinessWire, Available from: <http://www.businesswire.com/portal/site/google/?ndmViewId=news_view&newsId=20080115005324&newsLang=en> [Accessed: 14 April 2009].

Vasser (2009). 'How to keep your computer's operating system and programs up-to-date', Available from:

<http://computing.vassar.edu/safecomputing/security/ospatch.html> [Accessed: 17 April 2009].

WindowSecurity.com (2002). 'Beyond the Firewall (White Paper)', Available from: <http://www.securityforums.com/viewtopic.php?p=5787&sid=db1bca5dcddd4bff05dd056501b7e92> [Accessed: 17 April 2009].