Social networks research paper

Sociology, Communication

Abstract

Social networking has become a multi- million dollar business, and through it, diversity has been created, through networking with friends and workmates at home, school, work places, and other various social places. As a result of this increase in utilization of social networks, several challenges have emerged in relation to the same. The purpose of this paper therefore, is to look at a few ways social network users can keep their information safe and private, as well as the different ways users can identify and keep up with fake accounts that are currently being used for bulling, dating, and scams.

Introduction

A social network is a social structure formed and found on the internet that facilitates and enhances interaction and communication between organizations, and between groups of people. These individuals are usually related to one another through some kinds on interdependencies like shared values, common interests, visions, friends and kinship (Strutin, 2009). Websites for social networking provide web space for users, which they can use to make new friends, communicate, and connect with friends from foreign countries, form groups, market products and businesses, and even space to share information and knowledge with a group of people.

This web space can be customized by its users through the use of texts, videos, personal photos, music, and hyperlinks. Other users can then assess this information, which is usually on the user’s page, and browse the page’s content in addition to commenting on contents of the page (Eric, 2007). Friends, workmates, and acquaintances can find each other on such websites

through the use of contact information or names, mutual interests, and even through friends. The opportunities social networking provides are endless (Safe Social Networking and Blogging, 2010).

Such opportunities provided for by the tools of various social networks as advantageous as they are, are however, exposing users to greater risks. Such risks come about as a result of certain users exploiting such sites for unintended purposes. For example, computer criminals are becoming a danger to many users in that they distribute malware and viruses, targeting private information other users have publicly posted and shared, and also to find other targets, which they can use to social engineer or phish their schemes (Safe Social Networking and Blogging, 2010). Despite these risks and threats, social networks can also be very important and useful, take for example, the revolution that took place in Egypt this year, as a result of these social networking sites (Summers, 2011). Examples of these social networks include MySpace, Facebook, LinkedIn, and Twitter (Social Networking, n. d.).

How Information is Kept Safe in Social Networks

Although a social network's features are different from those of another social network, they all have a common feature that requires the users to provide some personal information. Another common feature is that all these networking sites offers a user some form of communication program, which can range from chat rooms to forums to instant messengers to email, all of which enable users to communicate with each other. A challenge emerges when users fail to exercise some form of caution when providing personal information. This has been found to be enhanced mainly by the sense of

anonymity the internet provides, the feeling of false security that lack of physical communication and interaction creates, and the need to impress potential associates and friends (McDowell, 2011).

While most users who access such information might not pose any kind of threat to such people, other malicious people using the same networks might be tempted to misuse this information because of the availability and accessibility of information. These people can use this information for their own interests like impersonating a good friend or convincing a user that they require and have the authority to access their financial or personal data. Because of such threats, users of social networks have to exercise various protective exercises, some of which are provided for by the networks and others that the user has to implement and exercise by themselves (McDowell, 2011).

For example, several computer networks provide for security packages that are safe, and those that a computer user can trust. A user should therefore, only run these trusted software or use the ones modern browsers such as Firefox, the current models of Internet Explorer, and Google Chrome recommend for protecting ones computer from some fraudulent sites that most social network scammers use. The utilization of the most current models of an operating system is also another measure one can use to protect themselves, because such systems have the latest patches for leaks in security (McCracken, 2010).

Most social networking sites also provide its users with numerous security and privacy settings. It is therefore, the responsibility of a user to learn about these settings and use them to their advantage. Such security settings can

help users manage their experiences online in a manner that is positive in addition to controlling those who assesses their pages, and contents of their pages. Other security measures a user can maintain and use is the utilization of anti- virus software (McDowell, 2011). They help users protect their operating systems from viruses that have already been identified. However, updating of this software is critical as attackers are constantly writing new viruses which older versions of anti virus software cannot manage. Other operating systems, like Google, also protect their users from such threats by constantly scanning different gadgets and tools used in their social networks for any threat (Krebs, 2008).

In addition to these computer based protective measures, users can also protect their information through other security measures that are based on the social network users. For example, a user should always give some thought to the kind of information they are posting on these websites. A user can even have the option to restrict access to their private information to a selected group of users, like friends, family, and school mates. A user should also keep their private information to themselves. Information like ones social security number, full names, address, credit card and bank account numbers, and phone numbers, for example should never be shared in a social networking site. Information that can be used to locate or identify someone when offline like ones school name, club, and even sports team, should also not be posted (Social Networking Sites: Safety Tips for Teens and Teens, 2006).

In addition to the above, one should also consider proofreading a blog entry to make sure that it does not give away too much information. One of the

good rules of thumb about internet use and social networking is not to post anything on the web that you would not want the world to know (Audri, n. d.). It is also important to know that once something has been posted, then it will remain posted; it therefore, is wise for a user to protect their online reputation by thinking twice before posting anything, including pictures, that might taint their reputation if accesses by say, parents or future employers. One can also control their privacy by posting limited basic information about themselves on these social networking sites (McCracken, 2010).

Keeping Up With Fake Accounts Commonly Used For Scams, Dating, and Bulling

A user should be very wise when using social network sites because it is in these sites where fake accounts run high and pose different kinds of risks to internet users. A user should therefore, be careful on what link they click away from their social networks like Facebook and Twitter. For example, if a user clicks on to one of these URLs and then they ask for a password, a user should be cautious with the next step they take because such URLs provide malicious people with access to ones account. This access can then give them an opportunity to organize scams against these users, or they can also use the information to bully the users. In addition to being careful with what one clicks, it is also important for users to carefully judge messages, and especially the messages that ask the user to click and enter a site of a trusted social network to either see a photo or watch a video. This is because such videos or photos could be a form of scam hackers and other internet criminals use to access personal information (McCracken, 2010).

Protection of ones passwords is also another measure social network users

can use to protect themselves from fake accounts. Passwords should be long, and cryptic with numbers, characters, and punctuation marks that are random. They should also be changed constantly. One should also assume that any unsolicited request for their password is a hoax always, no matter were a user encounters them. Such security measures with ones passwords are important because they keep ones account safe from bullies and scammers. Before joining a social networking site, a user should also check their privacy policies before joining. This is because some sites share their users' personal information with other companies. It is recommended to avoid such sites as they might lead to increased spam and increase the accessibility to ones account by bullies and scammers (McCracken, 2010). A social network user should always be skeptical when it comes to the internet. One can therefore, never believe what they see or read online. This is because malicious people might mislead people by providing the wrong information about their identity. Before forming any alliances or associations with strangers, it is important for them to validate and authenticate the available information about other users. In addition to this, users should also be wary of new people and strangers they meet on the internet; they might not be who they say they are. A user should always know his friends; he should also be able to manage them. This is because social networks allows for one to meet, make and accept friendship offers from a wide variety of people. A user's information should only be availed only to friends who are close. This will also help protect one from internet scams, bullying and other fake accounts (McDowell, 2011).

Conclusion

One of the best ways for a user to protect themselves from the numerous threats and risks brought about by social networking websites, is to keep personal information private, and to themselves. This is because access to personal and private information is one of the many ways malicious people access and misuse ones information to bully them and design scams against these users. This policy would be very essential as it would go in line with some of the major ethical theories in social networking. Some of these are rights based and virtue theories. Virtue theory used together with this policy will ensure that individuals accomplish their maximum potential because they will not be disrupted. Together with the rights based theory, this policy would help users uphold and maintain their human dignity and rights because no one will have access to their information.

References

Audri, J. L. (n. d.). Tips to Keep Your Teens (and Yourself) Safe on MySpace and Other Social Networking Sites. Retrieved from http://www. scambusters. org/myspace. html

Krebs, B. (2008, August 7). Researchers Warn of Social Networking Scams. Retrieved from http://voices. washingtonpost. com/securityfix/2008/08/researchers_warn_of_social_net. html

McCracken, H. (2010, March 23). Protect Yourself Against Social-Network Scams. Retrieved from http://www. foxnews. com/scitech/2010/03/23/protect-social-network-scams/

McDowell, M. (2011, January 26). National Cyber Alert System Cyber Security Tip ST06-003. Retrieved from http://www. us-cert. gov/cas/tips/ST06-003.

html

Professor Eric, G. (2007, May). Social Networking Sites and the Law. Retrieved from http://www. ericgoldman. org/Resources/socialnetworkingsitesandthelaw. pdf

Safe Social Networking and Blogging. (2010, June 30). Retrieved from http://security. rit. edu/dsd/bestpractices/socialnetworks. html

Social Networking. (n. d.). Retrieved from http://www. staysafeonline. org/in-the-home/social-networking-0

Social Networking Sites: Safety Tips for Tweens and Teens. (2006). Retrieved from http://www. ftc. gov/bcp/edu/pubs/consumer/tech/tec14. shtm

Strutin, K. (2009, February 28). Criminal Law Resources: Social Networking Online and Criminal Justice. Retrieved from http://www. llrx. com/features/criminaljustice/socialnetworking. htm

Summers, P. (2011, March 3). McCain: Zuckerberg Made Middle East Revolutions Possible. Retrieved from http://politics. blogs. foxnews. com/2011/03/03/mccain-zuckerberg-made-middle-east-revolutions-possible