Privacy Dashboard

M.Tyler-Dimond and S.Atkinson

Centre for Security, Communications and Network Research,
Plymouth University, Plymouth, UK
e-mail: info@cscan.org

Abstract

Social Networking is taking the world by storm and with over 750 million users worldwide actively using *Facebook* alone, the growth of this phenomenon is staggering. Social networks allow users to interact with each other through posting messages on each other's walls and sharing personal information. In this paper, we observe the threats which are affluent in the social networking world and apply them to the perceived organisational values placed on using social networks. Through observing the threats we analyse the ways in which users attitudes and behaviours towards social networking impacts on the privacy of the organisation as well as the individual. We evaluate the usability of the social networking websites' privacy settings in order to establish how easy it is for users to maintain their desired level of privacy, and discuss the needs for a Privacy Dashboard in order to prompt users to manipulate their privacy settings in order to reduce the level of information they share.

Keywords

Social Networking, Privacy Controls, Privacy Settings, Awareness

1 Introduction

Social networks are now a common sight in the workplace, having been embraced by many companies in order to communicate and gain information on potential employees as well as market products and services to potential consumers. However, these social networks are also being used by employees for personal use in the workplace, and represent a distinct threat to sensitive information as well as acting as a gateway to malicious software. Therefore, this paper will look at the attitudes and behaviours of employees towards social networking websites in order to establish how much information they are sharing online.

2 Background

Although the concept of social networking dates back to the 1960s people were not interested until it was supported technically by the internet (Leonard 2004 cited in Gross and Acquisti 2005). These websites take many forms. It is popular for people who wish to share information through profiles (e.g. *Facebook* and *Linked In*), collaborate on playlists and musical tastes through *Last.fm*, share and comment on photographs using *Flickr* or the most recent trend; micro-blogging on *Twitter*.

Although the way in which people collaborate on these social networking sites differs greatly, they all provide users with the ability to share personal information:

For example, contact details, relationships and interests. Through the information provided on these social networking sites, the user is able to create an online profile or 'persona' which may mimic their offline persona or they could create themselves a whole new personality. However, although these social networks allow users to share their personal information, it is not compulsory to do so. Nevertheless, it has been found that the majority of users fill out these forms (Ofcom 2008). This is because people enjoy sharing their interests and daily occurrences with other users as it provides them with an outlet to share their news, ideas, feelings and interests. However, it is also used as a way to vent anger and can in some cases damage the reputation of the user, as well as other users and potentially organisations. Therefore, it is important to observe users' attitudes and behaviours towards social networking websites in order to ensure that threats to personal as well as corporate information is not revealed.

3 Social Networking Threats

Social networking websites, such as Facebook and Linked In, need to remain cautious over threats to users' data, as with over 750 million active users, *Facebook* needs to ensure that users' personal information is secure as more and more malicious operators target users of social networking sites (Facebook 2011).

3.1 Social Engineering Threats

Social engineering is a term used to describe the psychological tricks used to mislead people into undermining their own online security through social networking sites, and, consequently, into disclosing sensitive information (Sophos 2011).

Methods of deception can influence users to follow links, open an email attachment, click a button, or fill in forms with sensitive personal information. These psychological tricks capitalise on weaknesses in users' online behaviours and lack of awareness in order to spread malware, gain access to sensitive information, and target the users' desires, fears and curiosities exercised when online (Sophos 2011).

However, attacks often take place through phishing and click-jacking scams (Wisniewski, C. 2011; Cluley, G 2011).

Many users are unaware of the level of information they are sharing on social networking sites and with whom they are sharing the information. As can be seen in the Preece vs JD Wetherspoons plc case (Lawspeed.com 2011) many believe that any information they post can only be seen by a certain number of people, mainly close friends. However, this depends on the networks joined, as well as the number of people befriended on the social networking site. Therefore, it is easy to assume that although users claim to be aware of their actions, and the consequences of their actions on these social networking sites, their actions do not fit the 'Attitudes' or 'Behaviours' of someone who is aware of the threats some posts may cause. PR Newswire (2011) surveyed that at least 52% of all social networkers post risky

information on their social networking profile. However, this information is only relevant as far as those who are aware of the risky content they post online.

Realistically, of the other 48%, a proportion of them will not be aware that they have posted any risky content and, therefore, the statistic should be much higher.

4 IT Security and User Acceptance

IT Security for many organisations is an uphill struggle. Those employees which are seeking to comply with security policies implemented need to maintain an awareness of how to avoid causing vulnerabilities, whilst those who are working against security policies need to be made aware of the dangers.

Security Awareness is defined as "An initiative that sets the stage for training by changing organizational attitudes to realize the importance of security and the adverse consequences of security failure. Furthermore, awareness reminds users of the importance of security and the procedures to be followed" (Primode 2011).

Furnell and Thompson (2009) theorize that employees' attitudes and awareness can prove to be an obstacle to effective maintenance of information security. They apply Schein's theory (1999) that there are three levels of corporate culture and apply it to IT Security policy compliance. It is Furnell and Thompson's belief that "corporate culture is a particularly intricate aspect of any organisation, and can exist whether the management and employees are aware of it or not" (Furnell and Thompson 2009:1).

Therefore, they conceive that culture can be likened to personality as it affects how employees behave in the workplace when unsupervised. It is these collective individuals and their behaviours (artefacts) within an organisation which make up the basis of how employees' values and beliefs impact upon the corporate, or in this case, security culture of the organisation.

The second tier of corporate culture relates to the 'espoused' values. For example, these values would be those which the organisation puts forth through its regulations and policies on security. However, it is important to note that should the regulations outlined in the company's IT policy and the behaviours of employees not run parallel, then the beliefs of the employees will succeed. Therefore, it is important to ensure that employees are made aware of their actions through the use of training and other awareness-raising practices. This will enable the organisation to develop a deeper level of corporate culture through "shared tacit assumptions" (Furnell and Thompson 2009:2). Therefore, the third tier of corporate culture implies that the regulations outlined in the organisation's IT policy and the subsequent behaviours of employees contribute to shared beliefs and work practices which provide unison in the achievement of a common goal.

Therefore, measuring the attitudes and behaviours of employees is crucial to the success of implementing any IT policy within an organisation, as without the compliance of the workforce, the necessary level of security will not be achievable.

5 Attitudes and Behaviours towards social networking sites

Ofcom's research suggests the importance of creating a 'well developed' profile in order to create a distinct and unique online presence. Furthermore, the more information shared within the profile, the more this attracts users to view a profile as it allows them to see a representation of who the user is 'offline', and whether or not they have common interests. Therefore, these profiles frequently contain highly detailed information about the user as although it is not compulsory to fill in this information, it is of benefit socially to the user who will enjoy sharing information about themselves and their interests, plus photographs, and playing online games (Ofcom 2008).

However, previously, social networking information such as religion, sexual orientation, and political views would not necessarily be disclosed to the general public, but instead only shared with close friends. Social networking has changed the modern perception of what is private and what is not. This has lead to 17% of adults communicating with people they do not know through these sites (Ofcom 2008).

Although all users engage with social networking websites in order to communicate, Ofcom have theorized that there are 5 different categories of user who use these websites with different motives, behaviours and attitudes.

Groups	People	Description
Alpha socialisers	a minority	People who used sites in intense short bursts to flirt, meet new people, and be entertained.
Attention seekers	some	People who craved attention and comments from others often by posting photos and customising their profiles.
Followers	many	People who joined sites to keep up with what their peers were doing.
Faithfuls	many	People who typically used social networking sites to rekindle old friendships, often from school or university.
Functional	a minority	People who tended to be single-minded in using sites for a particular purpose.

Table 1: Ofcom's 5 social networking site user categories

Categorising users into these 5 groups makes it easier to create an educated assumption of those who are at more risk to threats caused by social networking websites than others. For example, alpha socialisers and attention seekers especially, are more likely to be those who look to meet new people, and maintain a complete profile, sharing information with everyone instead of filtering their settings. In comparison, 'followers' and 'faithfuls' are more likely to lean on the side of caution, keeping abreast of any information they publically display and keeping their social networks for those with whom they have already communicated.

From the business perspective, an employer or manager of an organisation may wish to review the profiles of potential candidates when recruiting. For example, employers view social networking websites to determine if the applicant would be a suitable match to the company by looking at what information they share with others.

The Ofcom report suggested that privacy and safety issues were not of particular concern to the majority of users and that 44% of users left their privacy settings open by default, either through a lack of awareness, or through lack of manipulation of privacy controls. Ofcom also theorize that the need for 'attention seekers' to have attention is more important than protecting their information.

Giving out information, photographs and other content provides users categorized as 'attention seekers' with a high or confidence boost they need in order to feel popular or attractive. Unfortunately, people who come across as willing to give out sensitive or personal information may be seen as a liability to organisations looking to employ. It may be felt they would not maintain confidentiality of information within their company as such behaviours may be transferred from the personal lives of employees to their professional lives. In the current privacy climate new boundaries have been created by social networking websites, and the borders to these boundaries have not as yet been determined. Therefore, users need to maintain a degree of awareness when determining what information they wish to share openly, especially if it affects other people or organisations.

Consequently, because of the risks involved both to the individual, the organisation, and in some cases wider society, it is vital to establish why a large percentage of users display a lack of concern towards the visibility of their profiles.

Raising awareness of the issues is a fundamental area which needs to be addressed, particularly as users are also prone to assuming that the social networking websites themselves actually ensure that a level of privacy is maintained. However, the reality is that social networks, such as *Facebook,* leave users' privacy details 'open' by default. This not only takes advantage of the users' lack of awareness, it also benefits from users' lack of confidence in their ability to change their privacy settings.

6 Social Networking and Privacy

Facebook **settings:** *Facebook's* privacy settings are the most complex of all the social networking websites compared. Their privacy settings allow you to customise all the fields which allow you to share information, providing 5 different settings. For example, for all fields including the address field, the user can choose to share information with 'Everyone', 'Friends of friends and networks', 'friends and networks', 'friends of friends', or just 'friends'. Furthermore, within the advanced settings, the user can choose not to share with anyone, or share only with specific people (Facebook 2011).

However, for the average user, who is non-technical, knowing which settings and how to implement them can be a struggle. Therefore, *Facebook* have also implemented an easier way of setting privacy settings, using preset options of 'Everyone', 'Friends of Friends', 'Friends' and 'Recommended' settings which will

automatically update all the field's privacy settings to that standard. *Facebook* also give a table highlighting settings, enabling the user to overview their privacy settings (Facebook 2011).

However, although these added settings have been implemented, *Facebook* is still criticized for its 'opt-in' to privacy culture. For example, when signing up to *Facebook* for the first time all settings are set to share with everyone. In addition, upon implementation of new features, *Facebook* automatically enrols users into the new service, one of which called 'instant personalization' gives access to users' publicly available profile information to selected websites the user has visited (Larkin, E 2010).

***Twitter* settings:** In comparison to *Facebook*'s settings, *Twitter*'s are considerably less sophisticated. However, their type of social networking is not based on sharing personal information in the same context. Twitter is based on micro-blogging: for example, posting comments and status on current events and topics which the user feels strongly about. This allows users to build an online persona through their posts.

In comparison, *Facebook* is based upon building a profile which allows the user to create an online persona by giving information and focusing more on interaction with 'friends' and 'friends of friends'. In contrast, *Twitter* encourages building a network with people of the same interests, and not having as much control on who follows the posts. However, there is a setting which allows the user to control who is able to view their 'tweets' by approving people they wish to share with. Although, this setting is nowhere near as sophisticated as *Facebook's* as it does not allow any distinction between friends and other people who follow you. Therefore, it is more difficult to determine the identity of the follower.

***Linked In* settings:** *Linked In* privacy settings are more sophisticated than *Twitter's,* as they conform to traditional use of social networking and allow the creation of a persona through the sharing of personal information. However, the social networking websites' settings are categorized into 4 sections: Profile, Email Preferences, Groups, Companies and Applications and Account. Within these 4 sections, settings relating to the category are laid out in order to allow the user to customise settings which incorporate privacy settings, as well as sharing of information with accounts on other Social Networking Websites such as *Twitter*.

The first distinction in *Facebook's* settings is that unlike *Linked In*, *Facebook* has a dashboard devoted to the protection of data. This means that users have to check through all 4 sections to ensure that their information is secure. This inevitably would frustrate users.

However, the *Linked In* privacy controls allow the user to choose whether they wish to share their 'Activity Broadcasts'. Sharing 'Activity Broadcasts' allows people to know when the user changes their profile, makes recommendations, or follows companies. As *Linked In* is based on professional contacts, it may be advisable when searching for a job not to share activity broadcasts, as an employer may notice the user is looking elsewhere for new employment. However, the user is also able to

customise their activity feed so that only certain people can see it: for example, 'only you', 'your connections', 'your network' or 'everyone'.

Linked In also provides users with the option to 'opt-out' of advertisements selected for users dependent on their interests or profession. This sort of advertising also takes place on *Facebook*. However, *Facebook* do not provide the option to opt out of tailored advertising, as it provides them with its main source of income. Unlike *Linked In*, *Facebook* also does not directly allow opting out of data sharing with third-party applications either. This is mainly because *Facebook* encourages openness, and wants to be able to provide users with as much functionality as possible. However, in order to deliver this functionality, users may have to share information with third parties so that they can use the service

Therefore, due to the complexity of the privacy settings and lack of awareness of the threats to privacy, it was considered that a prototype application based on raising awareness of the insecurity of settings was needed to allow employees within organisations to protect both their personal information, and that of the company.

7 Prototype: Privacy Dashboard

The prototype addresses the concerns which users commonly have when using websites: knowing what settings are relevant to them and protecting their privacy. The prototype will allow users to engage with the three most recognised and popular social networking sites' (*Facebook*, *Linked In* and *Twitter*) privacy settings, which will allow them to view what information they are sharing with everyone, and provide them with a privacy rating. Furthermore, it will offer them advice on where their privacy settings are at their weakest. The prototype will be designed as an educational tool instead of manipulating settings through the prototype. This allows the user greater flexibility, as changing the settings through the prototype may influence them to implement different settings than they desire. Therefore, the tool acts as an aid which empowers the user to make their own decisions, and provides them with a greater understanding of their settings, rather than the prototype doing all the work for them.

8 Conclusion

In Conclusion, although the vast majority of the public see the lack of privacy as a threat, it has not been deterred them from using *Facebook*, or other social networking websites. Through users' attitudes and behaviours observed by Ofcom (2008) it can be determined that observing which category users' attitudes and behaviours belong to, the organisation can judge the need for training users further in order to protect their own privacy and reputation. However, in order to do this, users need to comply with the policies set by the company. This can be a particular challenge to the organisation as without awareness users will not fully understand the necessity to comply to these policies and, therefore, cause threats to the organisation. Consequently, it is vital that the organisation provides users with the means to become aware of the social networking threats, through training and updates of the latest threats through internal email systems

9 References

Cluley, G. (2011). “Lady Gaga found dead in hotel room? Beware Facebook clickjacking scam”. [Online] Available at: http://nakedsecurity.sophos.com/2011/08/05/lady-gaga-found-dead-in-hotel-room-beware-facebook-clickjacking-scam/ [Accessed 23rd August, 2011]

Facebook. (2011). ‘Timeline’ [Online] Available at: http://www.facebook.com/press/info.php?timeline [Accessed 23rd August, 2011]

Furnell, S and Thomson,K. (2009). “From culture to disobedience: Recognising the varying user acceptance of IT security”, *Computer Fraud & Security*, February 2009, pp5-10.

Gross, R. and A. Acquisti (2005). Information revelation and privacy in online social networks. Proceedings of the 2005 ACM workshop on Privacy in the electronic society. Alexandria, VA, USA, ACM.

Larkin, E. (2010). ‘Can You Really Trust Facebook?’ [Online] Available at: http://www.pcworld.com/article/199162/can_you_really_trust_facebook.html [Accessed 24th August, 2011]

Lawspeed. (2011). “Employee posting offensive remarks on Facebook” [Online] Available at: http://www.lawspeed.com/news/Employee_posting_offensive_remarks_on_Facebook.aspx [Accessed 17th August, 2011]

Leonard, A (2004) ‘You are what you know[Online] Available at: http://dir.salon.com/tech/feature/2004/06/15/social_software_one/ [Accessed 31st August, 2011]

Ofcom. (2008). ‘Social Networking: A quantitative and qualitative research report into attitudes, behaviours and use’ [Online] Available at: http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/report1.pdf [Accessed 30th August, 2011]

Primode. (2011). ‘Glossary’ [Online] Available at: http://www.primode.com/glossary.html [Accessed 26rd August, 2011]

PR Newswire. (2011). “Consumer Reports Survey: 52 Percent of Social Network Users Post Risky Information”. [Online] Available at: http://www.prnewswire.com/news-releases/consumer-reports-survey-52-percent-of-social-network-users-post-risky-information-92748344.html. [Accessed 23rd August, 2011]

Sophos. (2011). ‘Security threat report 2011’ [Online] Available at: http://www.sophos.com/medialibrary/Gated%20Assets/white%20papers/sophossecuritythreatreport2011wpna.pdf [Accessed 25th August, 2011]

Wisniewski, C. (2011). “Twitter is not charging in October, there is no petition, you're being phished”. [Online] Available at: http://nakedsecurity.sophos.com/2011/08/18/twitter-is-not-charging-in-october-there-is-no-petition-youre-being-phished/. [Accessed 23rd August, 2011]