South African Journal
of Information Management
[DoE accredited]

Peer Reviewed Article Vol.11(2) June 2009

Potential influence of Web 2.0 usage and security practices of online users on information management

R.J. Rudman*
Department of Accounting
University of Stellenbosch
Stellenbosch, South Africa
RJRudman@sun.ac.za

L.P. Steenkamp
Department of Accounting
University of Stellenbosch
Stellenbosch, South Africa
LSteenkamp@sun.ac.za

The proliferation of Web 2.0 applications was the impetus for this survey-based research into practices that online users currently employ when using Web 2.0 sites. As part of the study, the popularity of Web 2.0 technologies and sites among online users at a university was investigated to determine the extent of the potential threat to corporate security, arising from Web 2.0 use and access. The results of this study indicate that the use of Web 2.0 sites is very popular among students, as a proxy for the potential future business users, and that users are not necessarily aware of the risks associated with these sites. The respondents indicated that they regularly visit Web 2.0 sites, and that they post personal information on these sites. This is of concern in protecting arguably the most valuable asset of a business.

Key words: Internet risks, online usage patterns, security practices, Web 2.0, user behaviour

Received: 26 May 2009; accepted 1 June 2009

Contents

1 Introduction and problem statement

1.1 Introduction

A recent trend in information technology is business-to-business collaboration, where business functionality is supported through virtual applications (Coetzee and Eloff 2005) that include Web 2.0 applications. This makes it necessary for business users to have greater access to the Internet as part of their normal business day. This trend, which is expected to continue (Metz 2007; Valdes 2008), is driven by the new generation of Internet users entering the workforce and bringing with them the familiarity of social computing tools (Ghandi 2008). As users become more comfortable with technological advances in their personal lives, they also demand this in their professional lives (Bradley 2007). They have different views on data access, multi-tasking, connectivity and control. With the growth and widespread use of Web 2.0 applications, much of the technological focus has been on ensuring that users gain access to data and resources, with less thought being given to whether users should have access (Johnson 2008). Many organisations have blocked access to Web 2.0 sites as employers become more worried about the impact on security and productivity, as well as about the possibility that employees share too much information on the Internet, which could result in attacks against companies and employees. A new generation of thieves is trolling the Internet, from social networking sites to sites devoted to real estate, looking for personal infomation they can use in scams and attacks (Boudreau 2007). One of the more recent attacks was a virus dubbed 'Koobface' that used information on social networking messaging systems to infect PCs and to gather sensitive information (Albanesius 2008), thereby invalidating privacy.

Privacy has emerged as a central concern about the Internet as more users come online and as methods of Internet access become more widespread (Fox, Rainie, Horrigan, Lenhart, Spooner and Carter 2000). Privacy is defined as an individual's ability to control the terms by which personal information is acquired and used. As far as the Internet is concerned, privacy affects aspects such as the obtaining, distribution or non-authorised use of personal information. According to Flavian and Guinaliu (2006), privacy and security are related. This raises the question: which practices do online Web 2.0 users currently employ when managing their online identity and to what extent do users protect their privacy?

1.2 Problem statement

The widespread publicity resulting from the increasing number of cases of identity theft (Butler 2005) has caused more emphasis to be placed on advising users on the use of Web 2.0 applications. The question now arises as to whether users have changed their practices in using Web 2.0 applications. The primary objective of this research was to assess which practices online users currently employ when using Web 2.0 sites, creating profiles and managing their online identity. An ancillary objective was to establish how popular these new Web 2.0 technologies and sites were, among online users, to determine the scale of the potential threat to corporate security.

It is important to understand how Web 2.0 users manage their identity, as Web 2.0 is a new, poorly understood technology and with the growing mobility of users, the potential threat increases (D'Agostino 2006). The research was conducted in an attempt to assess the level of awareness among university students who are the future business IT users, since students entering the job market understand how to use Web 2.0 sites, but the enforcers of the policy might not fully know how the technology works. The results of this study will help business determine strategies to aid in the adoption and diffusion of Web 2.0 and Web 2.0 access.

1.3 Research method

1.3.1 Questionnaire design and administration

A literature review was undertaken to identify existing research on users' behaviour. A survey was conducted among students in the Faculty of Economic and Management Sciences at a South African university to assess the practices they employed when using Web 2.0 applications. The questionnaire was developed based on the current practices employed by users identified in research studies conducted internationally and consisted of three parts, each part containing questions to:

1. Identify users' current Web 2.0 usage patterns
2. Determine how the respondents manage their Web 2.0 identity
3. Evaluate the users' awareness of the risks relating to Web 2.0 and how they manage these risks.

The questionnaire was reviewed by lecturers in the field of auditing as well as information systems, a statistician and ten volunteers from the target student population. They considered the questionnaire in terms of logic and intelligibility. Minor amendments were made on the basis of their feedback.

The questionnaire was Web-based and students were encouraged to complete the questionnaire in their own time. Two follow-up e-mails were sent to encourage students to complete the questionnaire. Owing to the fact that this was an exploratory study and in an effort to encourage respondents to complete the questionnaire, the questionnaire was kept as short as possible and a small incentive prize was offered. The results were cleaned and

analysed. All answers were scrutinised to eliminate instances where respondents clearly did not attempt to answer the questions. The answers to the open-ended questions were analysed and summarised in similar categories.

1.3.2 Target population

Currently, in South Africa, university students are the most connected Internet users because all of them have access to computer facilities on campus. They are followed by medium to large businesses in terms of connectivity. Historically, students have been early adopters of technology in South Africa; in many instances they are the ones responsible for introducing new technologies to businesses when they reach the employment market. This is underpinned by the Clearswift (2008) study that found that younger, early adopter employees are using Web 2.0 technologies to a greater extent than their older employee counterparts. Since the students become the future business users, the questionnaire was distributed to students enrolled in a number of courses: two first-year Information Systems courses; the second- and third-year Information Systems and Financial Accounting courses; as well as the honours classes for Bachelor of Commerce (BComm) (Management Accounting) and Bachelor of Accounting (BAcc) degree. This ensured that a large number of students enrolled in the faculty were reached.

In selecting students from various years of study and degree programmes, the researchers were able to identify whether users apply better practices as they become more technology literate and aware of the dangers of Web 2.0 applications. It would be expected that these students would be more aware of issues relating to the misuse of Web 2.0 applications and the possible consequences of such misuses, and thus more in line with the typical Internet users employed by business. These students should also be aware of security features provided by the Internet.

In total, 2 944 invitations to participate in the study were sent to students. Altogether 660 students completed the questionnaire. The response rate of 22,4% is considered sufficient to arrive at the necessary conclusions.

top

2 Literature review

2.1 Web 2.0

Although numerous definitions exist for the term 'Web 2.0', it is not well defined (Radcliff 2007). According to Wikipedia (2008), an online encyclopaedia, the publicly accepted definition for Web 2.0 is 'a perceived second generation of web-based communities and host servers that facilitate collaboration and sharing between users; referring to a change in the way in which the platform is used'.

The most significant difference between traditional web (i.e. Web 1.0) and Web 2.0 is the greater collaboration between users, programmers, service providers and enterprises, among others, thus enabling them to update, contribute and re-use the content in various forms (Getting 2007). Web 2.0 constitutes a paradigm shift in the manner in which existing technology is used. In essence, it is the evolution of the browser from a static request-response interface to a dynamic, asynchronous interface. The key features of Web 2.0 sites can be summarised as having the following three components:

- **Community and social:** This entails software that permits users to study, change and improve content or source-code and to simultaneously redistribute and re-use it in modified form. This component considers the dynamics around social networks, communities and personal content publishing tools that facilitate sharing and collaboration.
- **Technology and architecture:** These are Web-based applications with a rich interface that run in a Web browser and do not require specific software installation, a specific device or platform, but still have the features of traditional applications.
- **Business and process:** This component involves resources on a network made available as independent services that can be accessed without knowledge of their underlying platform implementation. Software is being delivered as a service rather than an installed product, thereby freeing users from a specific platform or operating system (Smith 2008).

Web 2.0 applications are based on four broad types of technologies as presented in Table 1:

Table 1 Types of Web 2.0 technologies

Technology	Examples of technology
1. **Publication**: Blogs and wikis which can be edited and contribute content by various users in real-time	Weblogs (blogs), wikis, user-generated media

2. **Syndication**: This allows for the sharing, consolidation and sourcing of information from various sources	Really simple syndication (RSS) or newsfeeds, social tagging or bookmarking, folksonomies
3. **Collaboration**: Users can create communities to collaborate or use tools to collaborate on projects	Social networking, peer-to-peer networking, Web application program interfaces (APIs)
4. **Recombination**: Flash-based players, podcasts etc. are easy to create and can be used for various purposes	Podcasts, mash-ups

The debate around the questions: 'What is Web 2.0?' and 'How should Web 2.0 be classified?' continues. Web 2.0 as a field is growing, with related concepts also being explored and researched.

2.2 Historical review of prior research

As the popularity of Web 2.0 services such as Facebook, YouTube and Wikipedia grew, the popular media published various articles on, for example, security risks relating to Web 2.0 services, while others focused mainly on business risks (D'Agostino 2006; Fanning 2007; Mitchell 2007*)*. Popular media publications in almost every industry have published some kind of article outlining how Web 2.0 has impacted that specific industry.

Most research relating to Web 2.0 has been conducted by private organisations such as Gartner, Clearswift, PEW/Internet & American Life Project and KPMG, among others, with limited academic peer-reviewed research being performed (Shin 2008). Initially, research focused on understanding the technology, its benefits, uses in a business environment and potential challenges (Clearswift 2007a; 2007b; Matuszak 2007). Other research studies focused on the areas of privacy (Cavoukian and Tapscott 2006), collaboration (Lee and Lan 2007), usage and users' behaviour patterns (Horrigan 2007; Lenhart and Madden 2007a; 2007b; Shin 2008).

Various attempts have been made to develop an organisational framework to help businesses to understand and address Web 2.0 risks and to generate business value for enterprises using Web 2.0 applications. The most widely used frameworks were developed by Dawson (2007; 2008).

Before frameworks for risk or value evaluation can be implemented, users' behaviour needs to be understood. Lardner (1999) argues that the lack of privacy on the Internet could pose an obstacle to the growth of the Internet. Flavian and Guinaliu (2006) analysed the effect of privacy and perceived security on the level of trust shown by consumers on the Internet. They found that an individual's loyalty to a Website is linked to the level of trust. The trust associate with the Internet is particularly influenced by the security perceived by consumers regarding the handling of their private information. Consequently, the level of trust can be evaluated from the types of information posted on Web 2.0 sites.

2.3 Prior research studies

Much work has been conducted on users' behaviour, what information users disclose and how users manage their privacy. The Pew Internet & American Life Project conducted a series of studies on Internet users' behaviour and related topics such as privacy, trust online, identity management and protection. They focused on various user groups ranging from teens to established employees. The earlier studies by Fox *et al*. in 2000 focused on the use of the Internet. These authors concluded that there is a presumption of privacy when users go online and that many users do not know how to manage their identities, how their identities can be tracked, or how to protect themselves. As a consequence, they unwittingly share personal information about themselves. Early in 2007, when the focus changed to Web 2.0, Lenhart and Madden (2007a) conducted a national survey of young people between the ages of 12 and 17 across the United States. The study focused on which sites were used, why (the reasons for using these sites) and how the sites were used and accessed, as well as how teenagers protected themselves against potential threats. During April 2007 another study was conducted that focused specifically on how teens managed their online identities and personal information in the Web 2.0 era. They focused on how teens chose which information to share, on assessing how they evaluated the vulnerabilities, and on which relationships teens maintained online. They found most teens protect themselves by limiting the information they disclose and to whom, yet relying very little on automated protection (Lenhart and Madden 2007b).

Guess (2007) reported on a study conducted by the Educause Center for Applied Research, which investigated how students were using information technology at college and how it could be harnessed to improve the learning experience. They found that users spent more time on the Internet and that they relied more heavily on mobile access. They also noted a change in the reasons why students were using the Internet. They commented that engineering and business students were using more technology, specifically spreadsheets and graphics editing

tools, among other things. This confirmed comments by Horrigan (2007) that users of all ages were becoming more connected, and that Web 2.0 applications were becoming a platform for communication and sharing via, among other things, handheld devices and cell phones.

Other research focused on business users in general, as well as industry-specific business users. Clearswift (2007a) investigated the impact of Web 2.0 on security and, while conducting the study, usage patterns and management of identity of employees in the United States and the United Kingdom were also investigated. The study focused on the type of service most frequently used, the time spent, as well as most prominent risks and related safeguards to mitigate any risks. Another study conducted by Clearswift in 2008, investigated the attitude of human resources (HR) professionals to Web 2.0 and investigated how they had adapted Web 2.0 to their organisations. The study investigated HR practitioners' knowledge of Web 2.0, the uses of the technology and currently acceptable and disallowed practices. The general findings were as follows:

- Organisations perceive risks in allowing employees uncontrolled access to Web 2.0 sites at work, and some of the problems include time and resource wastage, loss of confidentiality and posting inappropriate content.
- Unintended disclosure of personal information could harm a user's future.
- Although many sites have security features, many users are unaware of the features or do not enable these features.

A study by the IT security and control firm, Sophos PLC, investigating the risks of identity and information theft, revealed that 41% of Facebook users were prepared to disclose personal information, such as biographical and contact information, to complete strangers, thus increasing their susceptibility to identity theft and other forms of intrusion against individuals and companies (Kelly and O'Brien 2007).

These studies highlight the importance of identity management and risks in an international mature context. A similar study has not been conducted in a less developed Internet user market as in South Africa.

top

3 Results

The respondents were questioned about the nature of their Internet use before specific consideration was given to Web 2.0-related matters.

3.1 Respondents' profile and Internet activity

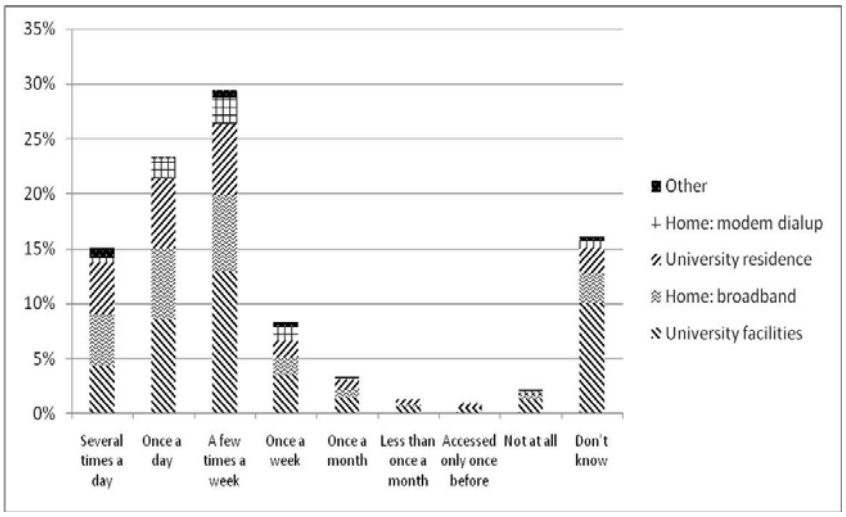
The 660 respondents comprised 54% male and 45% female students (1% did not indicate gender), of whom 71% were white, 21% coloured and 3% black (5% preferred not to indicate ethnicity). The demographic profile was not as important as the respondents' connectivity. Table 2 shows the respondents' source of connectivity. The majority of the respondents indicated that they accessed the Internet from their place of residence, either at home or university residence, while 43,4% used the university's computer facilities. These all have high-speed access points.

Table 2 Most frequently used Internet access point

Point of access	**Percentage**
University: computer facilities	43,4%
Home: broadband	23,2%
University: residence	22,8%
Home: modem dialup	6,5%
Other	4,1%

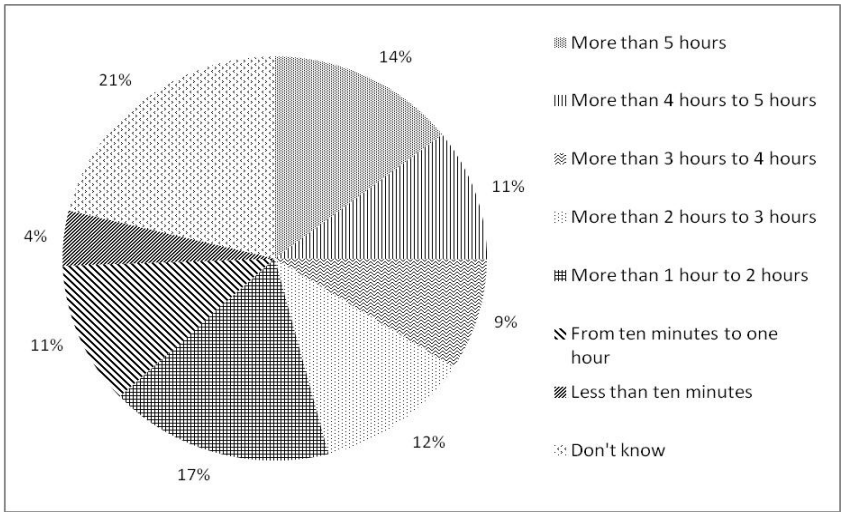
The source of access had a direct impact on the frequency at which the respondents accessed the Internet and the time spent on the Internet. This is graphically represented in Figure 1.

Figure 1 Frequency of accessing Web 2.0 sites



Respondents indicated that 38% accessed Web 2.0 sites at least once a day, with a further 38% accessing it at least once a week (Figure 1). In total, 76% of the respondents, therefore, accessed Web 2.0 sites at least once a week, clearly indicating that this was a favoured activity. This is borne out by the time spent on Web 2.0 sites in an average week (Figure 2). While one fifth of the respondents were unable to estimate the time spent on Web 2.0 sites, 14% of the respondents who were able to make an estimation spent more than five hours per week on Web 2.0 sites. This could have implications for large organisations, as the students (once employed) would have direct access to the Internet from their workstations once they started working.

Figure 2 Time spent using Web 2.0 sites in an average week



These high-speed access points facilitated the seamless use of Web 2.0 applications and were reflected in the nature of the services the respondents used. The most frequently visited sites based on type of site are set out in Table 3.

Table 3 Most frequently visited types of sites

Type of sites	**Percentage**
Personal communication	
Webmail (e.g. Gmail, Webmail)	32,8%
Social networking sites (e.g. LinkedIn, Facebook)	27,8%
Web-based Instant Messaging (e.g. MSN Web Messenger)	7,9%
Information source, excluding current events or news	
Online encyclopaedia and information sources (e.g. Wikipedia)	13,3%
Entertainment	
Online video sites (e.g. YouTube)	4,8%
Photo sharing sites (e.g. Flickr)	4,1%
News, current events, sharing of views	
Blogs	2,4%

Forums	1,8%
Really simple syndication (RSS) feeds (e.g. Newsvine)	1,4%
Podcasts	1,2%
Applications, virtual lives	
Online applications (e.g. Thinkfree, Smartsheet)	2,0%
Second Life	0,6%

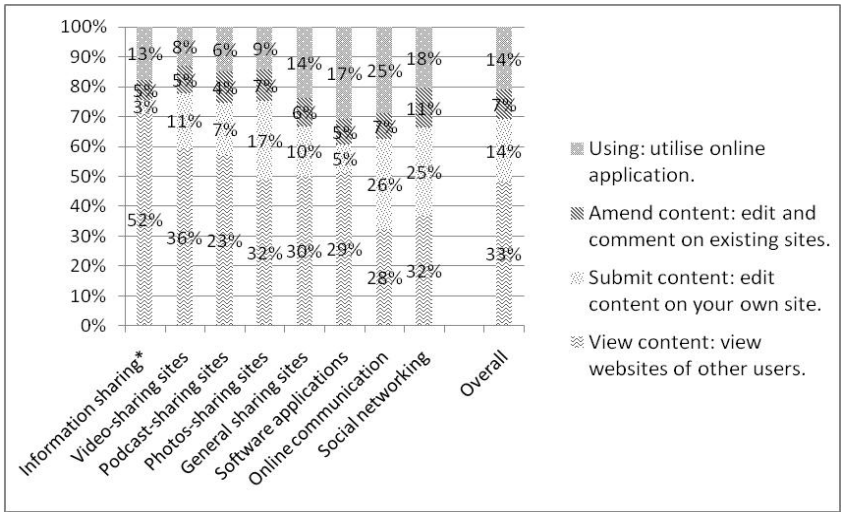
Social networking sites rank second to e-mail accounts in terms of popularity of usages. It is interesting to note that the sites with a direct communication component are used more often than content driven services.

3.2 Awareness and utilisation of Web 2.0 services

Although a wide range of services were used, many of the users were not aware of the nature of the service they used, with only 18% of the respondents aware of what Web 2.0 meant before they completed the questionnaire. A similar percentage was able to distinguish between static and Web 2.0 Websites. Those respondents that were able to identify Web 2.0 sites listed the differentiating characteristics of these sites as interactive, constantly changing, personal information sharing and user-orientated.

One of the primary characteristics of Web 2.0 sites is the interactivity of the sites. More than half of the respondents (53,3%) indicated that the activities they performed most often on Web 2.0 sites were viewing the Websites of other users, as confirmed by the results in Table 3. However, 15,0% and 8,4% of the respondents indicated that they submitted and amended information respectively, while 23,3% used online applications. Nearly half of the respondents, therefore, fully engaged with Web 2.0 sites in the manner in which, in their opinion, Web 2.0 sites have been designed to be utilised. These results are summarised in Figure 3, which provides a more detailed breakdown of the manner in which the respondents interacted with different types of Web 2.0 sites. These findings concur with the findings in international research by Guess (2007) and Horrigan (2007).

Figure 3 Different methods of interacting with the types of Web 2.0 services



** Information sharing refers to Websites where information is predominantly shared by way of text.*

3.3 Influence of Web 2.0

Using these services could be resource-intensive and influence the organisation negatively. A number of questions were asked to gauge the respondents' awareness of the effect of Web 2.0 on them and others. This is important since Internet use, including Web 2.0 use, does have an influence in some way or another on, for example, bandwidth or time that could be spent on another activity. Web 2.0 is typically rich in multimedia, for example, pictures or graphics, music and/or movies. These content types use greater quantities of resources than simple text and would, therefore, use more bandwidth. Of the respondents, 30,5% were of the opinion that Web 2.0 usage does not influence university resources such as bandwidth. But interestingly, 57,4% were of the opinion that the time spent on Web 2.0 sites influences other users. This might be because 43,4% of the respondents used the university's computer facilities to access the Internet, thereby making these computers unavailable for academic purposes. A similar impact could be surmised to occur in a business environment. The month after the questionnaire was administered, the university blocked Facebook and YouTube because of the large use of resources and the resultant slowdown in network speed.

Similarly, 46% of the respondents stated that they believed that Web 2.0 use influences students' studies. Responses were not gathered as to whether this effect is positive or negative, but the result, taken in conjunction with Table 2, may indicate that the effect will be predominantly negative. From Table 2, it appears that Web 2.0 was for the most part used for social networking, communicating and entertainment, none of which were primarily academic in nature. Web 2.0, therefore, potentially takes time away from academic endeavours. The respondents were divided on the effect on their social life, with 48,2% believing that Web 2.0 influences their social life and the ways in which they interact socially.

3.4 Risks and consequences

Unproductive time and resources constitute but only one risk relating to Web 2.0 applications. Overall (65,3%), the respondents were not aware of the risks posed by Web 2.0 sites. The questionnaire contained a list of seven potential risks that respondents were required to rate, where 1 was the most significant risk and 7 was the least significant risk for a user. Table 4 contains the average ratings for the seven risks. The most significant risk, in the opinion of the users, was electronic intrusion such as viruses and worms. Phishing attacks, a real risk which could be based on socially engineered information, were rated second. Unproductive time and unavailability of services (i.e. denial of service problems) were rated low, confirming earlier findings.

Table 4 Average ranking of risks by respondents

Risk	**Average ranking**
Electronic intrusion (worms, zombie bots) embedded in downloads	1,96
Phishing attacks	2,63
Breach of security of the controls on the Website	2,64
Information leakage and brand damage	2,92
Unproductive time	3,38
Content errors on websites	3,40
Denial of service	3,59

A ranking of 1 represents the most significant risk and a ranking of 7 is the least significant risk.

3.5 Inappropriate disclosure of information

Many of the risks presented in section 3.4 arise from sharing too much information. A number of statements were presented to the respondents where they were required to indicate whether they agreed or disagreed with the statements presented. Approximately 80% of the respondents agreed that sharing too much information on Web 2.0 sites such as social networking sites could lead to identity theft and possible phishing attacks. In sharing information online, two types of personal information could be posted online: either (1) by means of creating a profile or (2) through disclosure of personal information.

3.5.1 Online profiles

Of the respondents, 80,6% indicated that they created online profiles on Web 2.0 sites such as social networking and sharing sites. The respondents were asked which personal information they posted on their online profiles (Table 5).

Table 5 Information posted by respondents on their online profiles

Information	**Percentage**
First name	94,5%
Last name	87,5%
Photos of yourself	83,0%
Name of your university	77,2%
Photos of your friends	70,8%
Name of place of residence	70,2%
Full date of birth	68,2%
Hobbies	57,5%
Name of your school	55,4%
Likes and dislikes	52,6%
Student e-mail address	39,2%
Personal e-mail address	36,6%
Cell phone or other contact numbers	21,4%
Instant message screen name	20,7%

Current address	19,3%
Videos	13,8%
Employer details *(if applicable)*	6,6%
Streamed audio to your profile	6,0%
Link to your blog	3,7%
Your work e-mail address *(if applicable)*	3,5%
(Respondents were able to select more than one option, leading to a total in excess of 100%.)	

Respondents indicated that they usually make a variety of personal information available when they use Web 2.0 and that it would make social engineered attacks easier. The respondents acknowledged that a motivated Internet user would be able to identify them from their Internet profiles, with only 38,3% believing it would be difficult or very difficult to identify them.

3.5.2 Disclosing information

In light of the responses above, the respondents were asked which types of information they disclosed on Web 2.0 sites other than when creating their profile. The results are summarised in Table 6. Respondents would be willing to share personal information such as their religious affiliation, relationship status and photos on these sites. Most (53%) would also disclose their e-mail addresses, in spite of the real possibility of it being used for spamming purposes. One quarter of the respondents would even provide their cell phone numbers and 13% would knowingly provide information that might allow someone to find Internet users easily, such as address, home phone number and parents' names. A further 12% would even provide their passwords online and 10% would share personal identification information such as identity numbers, medical information or student numbers. It should be noted that this refers to information which they would disclose on their own or somebody else's Website, and not information that is used to create online profiles.

Table 6 Nature of information respondents would be willing to share on Web 2.0 sites

Type of information	**Yes**	**No**	**Maybe**
Biographical information			
Gender	85%	9%	6%
Age	75%	13%	11%
Town/city where you live	66%	21%	13%
Name and location of university	64%	23%	13%
Parents' professions	16%	70%	14%
Information that might allow someone to find Internet users easily, such as address, home telephone number, parents' names	13%	72%	15%
Contact information			
E-mail address	53%	33%	14%
Area code	30%	58%	12%
Cell phone number	25%	62%	13%
IM screen name	22%	61%	17%
Personal information			
Areas of interest	62%	23%	15%
Religious affiliation	62%	25%	13%
Personal preferences (movies, food, etc.)	62%	24%	14%
Boyfriend or girlfriend status	61%	25%	13%
Pictures or photos	61%	24%	15%
Your profession	56%	31%	14%
Pet information	36%	49%	15%
Physical appearance	34%	44%	22%
Sharing your experiences about your life	33%	48%	19%
Gossip	25%	57%	17%
Personal identification information such as identity numbers, medical information or student number	10%	82%	8%
Passwords or combinations	12%	84%	4%
(For ease of reading, the percentages are presented without any decimals. Owing to rounding, some rows may not add up to 100% exactly.)			

Respondents' willingness to disclose these types of personal information on Websites may be due to the perceived anonymity of the Internet.

3.6 Safeguards to mitigate risk

To limit the risks, safeguards could be implemented by the user or the organisation whose facilities are used, either by (a) limiting use, (b) self-protection, or (c) policy implementation. The findings in the previous sections are supported by the results of an additional question which asked respondents whether they would limit their activities on the Internet if they knew that the information being disclosed or the activities are being monitored by, for example the university or employer. The majority (44,2%) indicated that they would at least limit their activities, while 11,6% indicated that they would stop using the Internet, and 4,3% felt that, with the large volume of Internet activity, it would be impossible for the university or their employers to effectively monitor activities and that, consequently, they would not act. Only 39,9% of the respondents felt that their activities did not expose them to such an extent that they would need to change their Internet behaviour.

While the respondents may have been unaware of the risks (refer to section 3.4), 60,6% of the respondents did take some steps to protect themselves online. They used two main methods to protect themselves:

- Almost two thirds (63,4%) made use of the security settings on Web 2.0 sites (25% were not sure whether they did).
- Altogether 56,3% made their online information (including profiles) available to their friends only. One fifth of the respondents made their profiles visible to anyone and 10,3% did not know to whom their profiles were visible.

Other methods that respondents used to restrict access to their profiles were giving as little personal information as possible (50,4%), password protection (59,5%) and disclosing information to known friends (37,1%). This confirms findings by Fox *et al*. (2000) and Lenhart and Madden (2007b).

Controls implemented by an organisation could also not be as effective as expected. Many organisations have Internet policies that govern the use of company resources when accessing the Internet. The majority of the respondents (82,8%) indicated that they would comply with such a policy and 14,2% would probably ignore the policy in their use of the Internet. It is noteworthy that the students in the sample were required to agree to comply with the university's Internet policy before they were able to access the Internet. In spite of this, 3% of the respondents stated that they had never seen such a policy. This would, therefore, indicate that an Internet policy may not be the most effective way of regulating Internet use, as 17,2% of the respondents would not comply with the policy or would not be aware of it.

Access could be blocked; however, in spite of the acknowledged risks referred to in section 3.4, 68% of the respondents felt that the university should not block access to Web 2.0 sites, even though nearly half (47,2%) stated that the time spent on Web 2.0 sites may impact on the security of the university. Contradicting themselves, more than a third (37%) of the respondents indicated that employees should be entitled to access Web 2.0 Internet content from their work computer for personal reasons and should, therefore, not be blocked (21% elected not to give an opinion on this matter), clearly indicating a potential for abuse.

top

4 Discussion and conclusion

Internet security and privacy is a concern for most businesses. With the growing use of Web 2.0 applications that feature increased interactivity with the Internet, this concern and the potential risk related to Web 2.0 will, in all probability, not abate in the near future.

Against this background, a study was conducted through a survey administered to university students to determine which practices online users employed when using Web 2.0 sites. In addition, the study also considered the popularity of these sites. A response rate in excess of 22% was achieved. The use of students as proxy for business users was justified, as these students would soon join the business world and the online practices and habits would, therefore, impact businesses directly.

The respondents indicated that two thirds of them accessed Web 2.0 sites at least once a week and that social networking sites were accessed frequently. Nearly half of the respondents indicated that they fully engaged with Web 2.0 sites through amending and submitting content. The respondents were aware of the risks posed by sharing too much information on Web 2.0 sites, but more than a third believed that employees should be entitled to access Web 2.0 sites from their work computers for personal reasons. The majority of respondents created online profiles, posting personal information. A cause for concern was that the respondents indicated that they were not aware of the risks posed by Web 2.0 sites. Most respondents indicated that they did take some measures to protect their online identity, but more than 10% would post information that could be used to perform socially engineered attacks successfully.

The results of this study, therefore, indicate that the use of Web 2.0 sites was enjoying great popularity and that users were not necessarily always aware of the risks when using these sites. This is of concern in protecting arguably the most valuable asset of modern-day business: information. Considerations should be given to blocking access to popular Web 2.0 sites which are not needed for business purposes, since other potential measures would, in all probability, be ignored. At a minimum, users should be warned frequently of the dangers posed by disclosing too much information on these types of sites. It should be made clear that even though users' access of Web 2.0 for personal reasons may not affect the business in any obvious way, it does pose a risk to the business through potential spam, virus and other malware attacks, as well as through the real possibility of socially engineered risks.

It may well seem as if educating users on the risks posed by the Internet is being flogged to death in the popular press. However, this study has indicated that this process can never be taken too lightly, especially if protecting the information and data of a business is seen to be at all important.

top

5 References

Albanesius, C. 2008. Facebook users hit by Koobface virus. *PC magazine* (12 May). [Online]. Available WWW: http://www.pcmag.com/article2/0,2817,2336021,00.asp?kc=DAILYNEWS_120508_STORY3 (Accessed 7 April 2009).

Boudreau, J. 2007. Report: Facebook users lax on privacy: fake 'friend' easily scoops up loads personal data. *San Jose Mercury News* 15 August. [Online]. Available WWW: www.mercurynews.com (Accessed 7 Sept 2008).

Bradley, A. 2007. Key issues in the enterprise application of Web 2.0, practices, technologies, products and services 2007. *Gartner*. Research report. 14 June. [Online]. Available WWW: http://www.gartner.com/DisplayDocument?ref=g_search&id=507237&subref=simplesearch (Accessed 20 June 2008).

Butler, R. 2005. An investigation of 'phishing' develop guidelines to protect the Internet consumers' identity against attacks by phishers. *South African Journal of Information Management* 7(3). [Online]. Available WWW: http://www.sajim.co.za/default.asp?to=peer1vol7nr3 (Accessed 7 Sept 2008).

Cavoukian, A. and Tapscott, D. 2006. Privacy and the enterprise 2.0. *New Paradigm Learning Corporation*. Whitepaper. 17 October. [Online]. Available WWW: http://newparadigm.com/media/Privacy_and_ the_Enterprise_2.0.pdf (Accessed 20 June 2008).

Clearswift. 2007a. Content security 2.0: the impact of Web 2.0 on corporate security. *Clearswift Limited.* Whitepaper. 11 May. [Online]. Available WWW: http://resources.clearswift.com/Externalcontent/Features/Clearswift/9586/200704SurveyReport_US_1063233.pdf (Accessed 20 June 2008).

Clearswift. 2007b. Demystifying Web 2.0. *Clearswift Limited.* Whitepaper. July. [Online]. Available WWW: http://resources.clearswift.com/ExternalContent/C12CUST/Clearswift/9514/ 200707 DemystifyingWeb21].0_US_1062190.pdf (Accessed 20 June 2008).

Clearswift 2008. Content security 2.0. The role of HR and IT in effectively managing the business benefits and risks of Web 2.0. *Clearswift Limited.* Whitepaper. 3 July 2007. [Online]. Available WWW: http://resources.clearswift.com/main/pages/Clearswift/RSRCCTR/ContentDisplay.aspx?sid=3230&yid=2711 (Accessed 20 June 2008).

Coetzee, M. and Eloff, J. 2005. An access control framework for Web services. *Information management & computer security* 13(1):29-38.

D'Agostino, D. 2006. Security in the world of Web 2.0. *CIO Insight* (Winter):12-15.

Dawson, R. 2007. Web 2.0 framework. [Online]. Available WWW: http://www.rossdawsonblog.com/Web2_Frame work.pdf (Accessed 20 June 2008).

Dawson, R. 2008. An enterprise 2.0 governance framework - looking for input! [Online]. Available WWW: http://rossdawsonblog.com/weblog/archives/2008/02/an_enterprise_2.html (Accessed 20 June 2008).

Fanning, E. 2007. Security for Web 2.0. *Computerworld* 3 September:44.

Flavian, C. and Guinaliu, M. 2006. Consumer trust, perceived security and privacy policy: three basic elements of loyalty to Website. *Industrial management & data systems* 106(5):601-620.

Fox, S., Rainie, L., Horrigan, J., Lenhart, A., Spooner, T. and Carter, C. 2000. Trust and privacy online: why Americans want to rewrite the rules. *The PEW Internet & American Life Project*. Princeton Survey Research Association. Research report. 20 August. [Online]. Available WWW: http://www.pewinternet.org/~/media//Files/Reports/2000/PIP_Trust_Privacy_Report.pdf. (Accessed 20 June 2008).

Getting, B. 2007. Basic definitions: Web 1.0, Web. 2.0, Web 3.0. [Online]. Available WWW: http://www.practicalecommerce.com/articles/464/Basic-Definitions:-Web-1.0,-Web.-2.0,-Web-3.0/ (Accessed 23 June 2008).

Ghandi, A. 2008. Security threats from social computing. *Securitymag*. March:20-22.

Guess, A. 2007. Students' 'evolving' use of technology. *Inside higher ed* 17 September. [Online]. Available WWW: http://www.insidehighered.com/layou/set/print/news/2007/09/17/it (Accessed 18 September 07).

Horrigan, J. 2007. A typology of information and communication users. *PEW/Internet & American life Project.* Princeton Survey Research Association. Research report. 7 May. [Online]. Available WWW: http://www.pewInternet.org/pdfs/PIP_ICT_Typology.pdf (Accessed 20 June 2008).

Johnson, K. 2008. Control collaboration â€“ don't inhibit. *Networkworld* 14 January:26.

Kelly, C. and O'Brien, R. 2007. In study, Facebook users with strangers. *Wall Street Journal* Eastern Edition 250 (37):83.

Lardner, J. 1999. I know what you did last summer and fall. *US News & world report* 126(15):55.

Lee, M. and Lan, Y. 2007. From Web 2.0 to conversational knowledge management: towards collaborative intelligence. *Journal of Entrepreneurship Research* 2(2):47-62.

Lenhart, A. and Madden, M. 2007a. Social networking Websites and teens: an overview. Research report. *PEW/ Internet & American life Project.* Princeton Survey Research Association. 3 January. [Online]. Available WWW: http://www.pewinternet.org/~/media//Files/Reports/2007/PIP_SNS_Data_Memo_Jan_2007.pdf.pdf. (Accessed 20 June 2008).

Lenhart, A. and Madden, M. 2007b. Teens, privacy, and online social networks. Research report. *PEW/ Internet & American life Project.* Princeton Survey Research Association. 18 April. [Online]. Available WWW: http://www.pewInternet.org/pdfs/PIPTeens_Privacy_SNS_Report_Final.pdf (Accessed 20 June 2008).

Matuszak, G. 2007. Enterprise 2.0: the benefits and challenges of adoption. *KPMG LLP International.* Whitepaper. 1 May. [Online]. Available WWW: http://us.kpmg.com/microsite/attachments/2008/ Enterprise 20_Adoption.pdf (Accessed 20 June 2008).

Metz, C. 2007. Web 3.0. *PC Magazine* 10 April. [Online]. Available WWW: http://www.pcmag.com/ article2/0,2817, 2102852,00.asp (Accessed 20 June 2008).

Mitchell, R. 2007. Web 2.0 users open a box of security risks. *Computerworld.* 26 March:32.

Radcliff, D. 2007. Are you watching? *SC Magazine.* September:40-43.

Shin, D. 2008. Understanding purchasing behaviour in a virtual economy: consumer behaviour involving currency in Web 2.0 communities. *Interacting with computers* 20:433-446.

Smith, D. 2008. Web 2.0 and beyond: evolving the discussion. *Gartner.* Research report. 24 January. [Online]. Available WWW: http://www.gartner.com/DisplayDocument?ref=gsearch&id=588707&subref= simple search (Accessed 20 June 2008).

Valdes, R. 2008. Key issues in rich Internet application platforms and user experience 2008. *Gartner.* Research report. 25 January. [Online]. Available WWW: http://www.gartner.com/DisplayDocument? ref=gsearch&id=589413&subref=simplesearch (Accessed 20 June 2008).

Wikipedia. 2008. Web 2.0. *Wikipedia*. [Online]. Available WWW: http://en.wikipedia.org/wiki/Web_2 (Accessed 23 June 2008).

ISSN 1560-683X
Published by InterWord Communications for Department of Information and Knowledge Management, University of Johannesburg