DE GRUYTER OPEN

Scientific Annals of the "Alexandru Ioan Cuza" University of Iaşi Economic Sciences
62 (SI), 2015, 53-63
DOI 10.1515/aicue-2015-0036

SOCIAL NETWORKS SECURITY IN UNIVERSITIES: CHALLENGES AND SOLUTIONS

Daniela POPESCUL[*], Mircea GEORGESCU[**]

Abstract

Nowadays, information flows are powerfully augmented by Social Media. This situation brings along the adjustment of the traditional information security threats to this new environment, as well as the emergence of new characteristic dangers. The purpose of this study is to learn about Generation Y students' attitude to risks and security measures when using Social Networks (SN). The correct identification of their behavior is, in our opinion, essential for the academic community. Firstly, we need to understand what their real knowledge in the field is. Then, a serious and consistent adaptation of our courses in Information Security and other subjects and a redefinition of universities' security policies and procedures is necessary. On this basis, in an empirical study, we try to determine how much our students know about security threats and subsequent protection measures in SN.

Keywords: Social Networks, Social Networks use in universities, Social Networks security, Web 2.0 security threats

JEL classification: L86, M15

1. INTRODUCTION

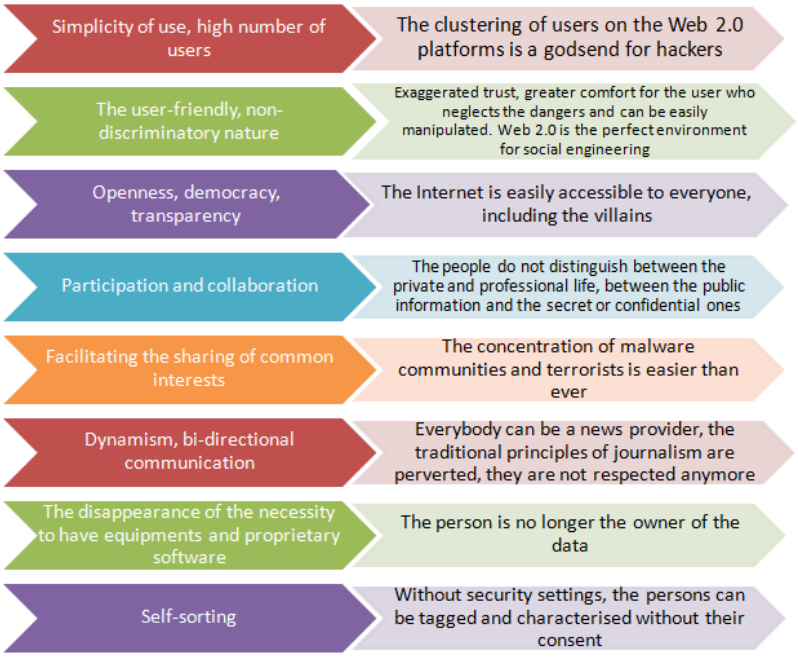
Web 2.0 represents an ensemble of technological platforms which allows the interaction of the users by spreading and consuming information and/or different online materials. The concept is based on a few key elements among which we mention creating and sharing user generated content, participation, communication and collaboration. According to (Airinei *et al.*, 2014, Horváth *et al.*, 2014, Radu, 2013, Ţugui and Şiclovan, 2013), the Web 2.0 technologies made possible the appearance of Social Media, such as Social Networks (SN), wikis, blogs, podcasting, RSS flows and so on. Social Media (SM) offers users a high degree of comfort, they are easy to use, and people can very easily join them. SM' openness deepens the more and more common perception of the Internet as utility, given by the low cost of connectivity, high speed for data and information transfers and ubiquity. The attraction proven by the SN on individuals is rooted in the similarity to

[*] Alexandru Ioan Cuza University, Iaşi, Romania; e-mail: *rdaniela@uaic.ro*.
[**] Alexandru Ioan Cuza University, Iaşi, Romania; e-mail: *mirceag@uaic.ro*.

real life when it comes to storing and consuming information – under the form of familiar discussion threads and easy-to-access links, more than well-structured databases.

But, the undoubtedly positive characteristics which we previously mentioned also have an unfavorable aspect from the point of view of information security, as we would like to present in Figure 1. SM are easy to understand and learn, designed so that they could very quickly gather fragmented information and knowledge, and used for a wide range of experiences (most of the times entertaining). In these friendly environments, people nowadays can very easily unveil sensitive aspects from their lives but also from the companies they work for. Thus, information confidentiality is affected, as shown in (Grama and Păvăloaia, 2014, Măzăreanu, 2010, Munteanu *et al.*, 2008, Oprea, 2007).

At the same time, SM make the user neglect the dangers in virtual world and trust excessively the validity of the information available online. This situation of feeling relaxed and trustworthy described above, in a combination with the permanent availability of the mobile devices connected to Web 2.0, leads to a stage in which the individuals become their own enemies. They are no longer able to clearly distinguish between the private, the social life and that of the organization, between the public information and knowledge and the private ones.



Source: authors' own contribution

Figure no. 1 – Challenges from the perspective of information security in Social Media

The right of ownership over their own data also disappears, since security is managed by third parties who are not very motivated or informed about the importance of information for its users.

Even more, the over-usage of Web 2.0 has changed it into a global village with millions of inhabitants where crooks can disguise under false identities and get lost, sharing more and more advanced fraud techniques without being seen. The classical forms of attack

such as Denial-of-Service (attempts to make Internet resources unavailable to their intended users), SQL attacks, spoofing etc. are brought to life once the social environments have evolved and the trust the users have in the above mentioned networks leaves place for manipulation by phishing, spam and other treacherous acts.

2. THEORETICAL FRAMEWORK - THE PERCEPTION OF STUDENTS AS REGARDS THE DANGERS AND RISKS ON THE SOCIAL NETWORKS

Nowadays, students form the category which is most exposed to SM. They are well-educated, internet savvy, and eager to learn (Vasilescu, 2011, Bolton *et al.*, 2013, Pînzaru and Mitan, 2013), but also more shallow, skeptical, blunt, critical, cynical, narcissistic, difficult to wow and impatient relative to their predecessors. They act as multitaskers, filter and consume relevant and interesting information with great speed, have high expectation and are headed to fast achievements (Vasilescu, 2011, Airinei *et al.*, 2014, Horváth *et al.*, 2014, Radu, 2013, Ţugui and Şiclovan, 2013). Social Media help digital natives to define and redefine themselves, to satisfy their requests for autonomy, recognition and achievement, as well as the need for affiliation and belonging.

The studies undertaken by (Ujhelyi and Szabó, 2014), (Tkalac Verčič and Verčič, 2013), (Whiting and Williams, 2013), (Pînzaru and Mitan, 2013), (Friedl and Tkalac Verčič, 2011), (Andrei *et al.*, 2010) show that students use SM for:

- Interaction with old or new friends;
- Keeping up-to-date;
- Searching for information about school, studies, shopping, events, entertainment, free time;
- Fighting boredom by listening to music, playing games, watching movies;
- Reading posts or comments;
- Self-promotion;
- Self-education.

Another category of use, more malicious, include surveillance or spying on friends and search for information about different people. These activities come at hand even more when people willingly unveil all sorts of personal information about them. (Benson *et al.*, 2015) shows that this phenomenon, boosted by the more and more common use of smartphones and localization services affect our civil rights ant intimacy. Finding a user profile on different data bases which has been willingly made available, is easier especially on SN, as they are different from e-commerce networks or other online environments. The service providers, third parties and especially users with a very relaxed attitude are equally involved in disclosing information. Apart from other negative effects on long term of using SN, (Santos and Čuta, 2015, Ernek Alan and Eyuboğlu, 2012, Bolton *et al.*, 2013) mention, as regards the students, the loss of intimacy and public safety, reduced civil involvement, increased cyber-crime and less involvement in online activities, addiction (the students seem to obsessively check the new posts and profile updates, stopping the activities they are usually involved in).

On the other hand, beyond the common supposition that the users neglect SM dangers and threats, trust excessively these environments and the credibility of the information accessed online, (Benson *et al.*, 2015 and Bolton *et al.*, 2013) have discovered in their studies that most users apply enough settings in order to ensure the information security,

being very careful about what they post and their own actions, and avoiding exposure to hackers, viruses, spammers and other attacks.

Considering these observations extracted from the literature in the field, the research questions formulated by us were:

Q1. How do the students perceive the risks when using SN sites?

Q2. What security settings do they use in their favorite SN site, Facebook?

In order to find answers Q1 and Q2, we conducted an online survey, consisting of 10 questions. We recruited 628 participants from Faculty of Economy and Business Administration, "Alexandru Ioan Cuza" University in Iași, who received a link to our online survey. It took approximately 10-15 minutes to complete the questionnaire, which was open from 9th to 13th November 2015.

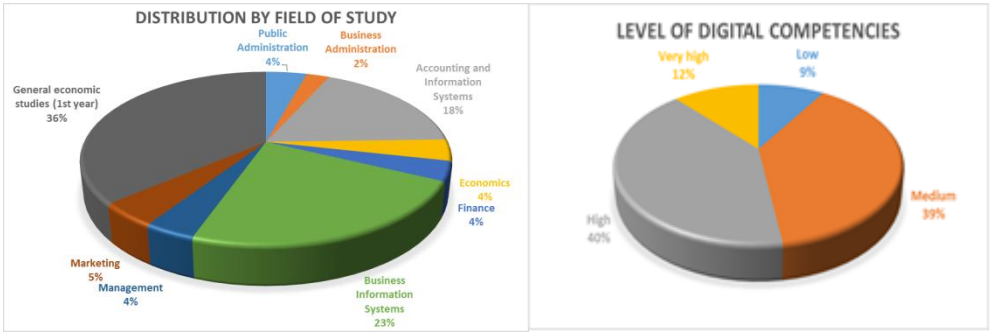
3. METHODOLOGY

The study aimed to analyze the degree in which the students from the Faculty of Economy and Business Administration are aware of the general dangers to which they expose themselves when using SN and to discover the security measures they use. A number of 628 students (10% of all the students in the faculty, 167 males, and 461 females) answered a questionnaire distributed by Google Forms; all the received answers were valid. Our questionnaire has two main sections. In the first section we asked participants about their age, gender, level of digital competence and possession of a smartphone. In the second section, participants were asked to rate items concerning privacy and responsibility issues, using 4-point Likert scales or True/False items.

Also, a number of 200 students specializing in Accounting and Information Systems, in the third year, bachelor degree, were asked to mention, which are, in their opinion, the three main benefits and risks of using the SN by professional accountants. The reason for choosing this group was their participation, the previous semester, in a course on the Security of Accounting Information Systems (28 hours of lecture, 28 hours of practical work). The security of SN was studied in detail during the above mentioned course. The students' knowledge was assessed during the whole semester – apart from improving the theoretical knowledge in the field, they also had to make an individual project to present the dangers and security measures discovered in the accounting information systems from different organizations. The average of the final exam grades for this group was 7.56/10, while the average of the grades given for the projects was 8.70/10. Hence we consider this group has a higher understanding of the security issues and we wanted to know their opinion about risk/dangers in SN, in connection with their future profession.

4. RESULTS AND FINDINGS

The charts below present the distribution of the 629 students by their field of study and their level of digital competence (self-evaluation). More than a half of the students are digitally literate and extremely proficient with technology, or at least that is their perception regarding themselves. 92% of them possess a smartphone and use it for visiting SN sites.

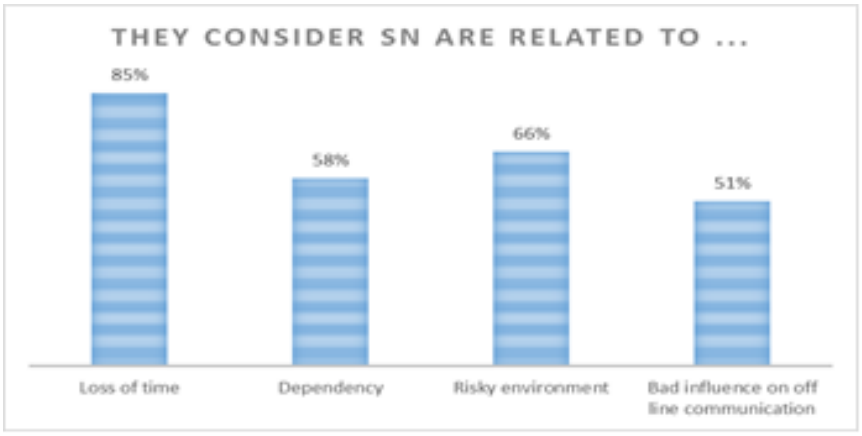


Source: questionnaire interpretation

Figure no. 2 – Respondents' structure by field of study

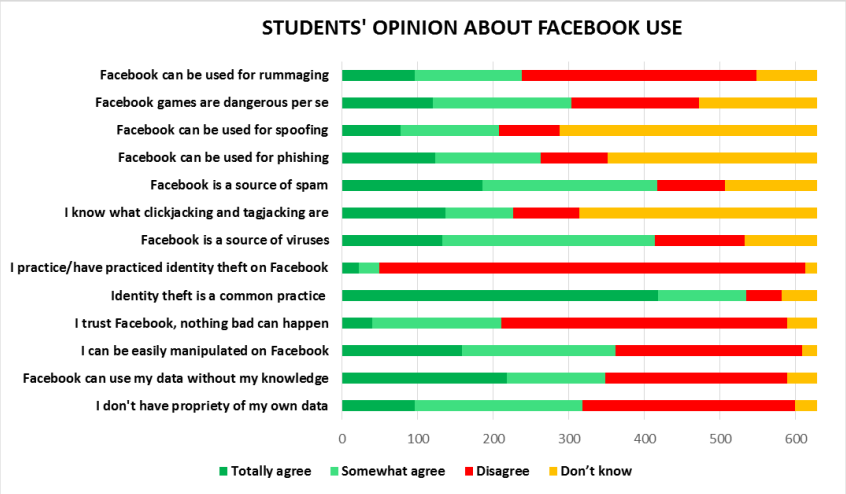
After these general observations, a set of 13 more specific questions showed that:

- Most of the students agree or strongly agree that Facebook is a source of viruses and spam, and that it can be used for rummaging;
- Most of the students aren't aware of more "technical" dangers, as spoofing, click-jacking, tag-jacking, phishing – they admit that they don't have knowledge about these types of attacks. On the other side, those who know the attacks agree that Facebook is a favorable medium for their appearances;
- Even if almost 95% of respondents consider the identity theft a common practice on Facebook, less than 10% admit they have practiced this form of attack;
- More than half of the students understand that Facebook can use their data without their knowledge, that they aren't the real owners of their data and that they can be easily manipulated on Facebook;
- Games that can be accesses through Facebook are considered dangerous.



Source: questionnaire interpretation

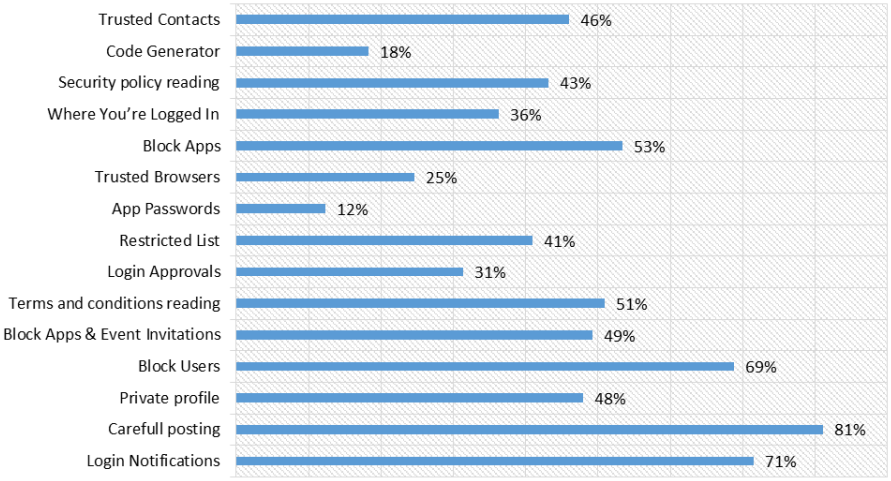
Figure no. 3 – General risks in Social Networks



Source: questionnaire interpretation

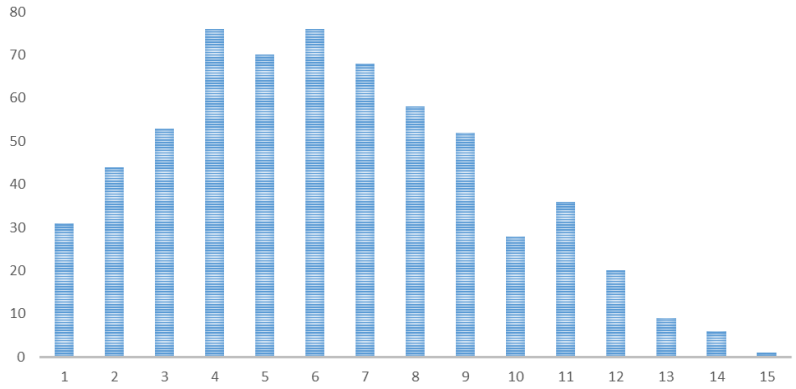
Figure no. 4 – Students' opinion on Facebook use

On the other side of the story, even if the common assumption is that in SN users neglect the potential security dangers and threats and are excessively confident in the trust and truthfulness of the online available information, we founded that an overwhelming majority of SN users define the privacy settings on who can access their profile information, and pay a lot of attention on their posts and actions, not exposing themselves to hackers, viruses, spam and other attacks, as can be seen in Figures 5 and 6.



Source: questionnaire interpretation

Figure no. 5 – Students' use of Facebook security settings

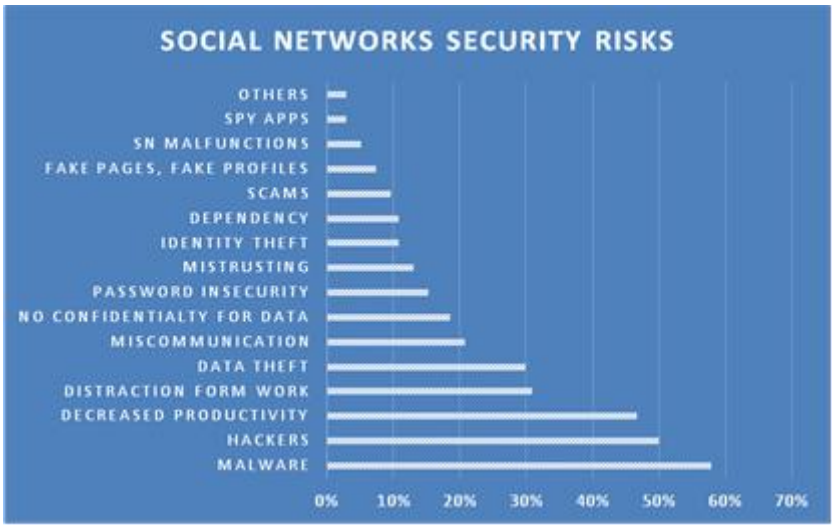


Source: authors' own contribution

Figure no. 6 – Number of security settings used by students

Focusing on the study applied on the 200 students specializing in Accounting and Information Systems, in the third year, bachelor degree, the hierarchy of risks/dangers identified is presented in Figure 7.

58% of the respondents consider that the SN are important gateways for malware. They mentioned viruses, worms, spyware, Trojans under the disguise of advertisements. Even though it is certain that the whole picture of IT threats shown by the led and combined action of the viruses, worms and Trojans is rather wide and presenting an infinite variety of details, there were not mentioned other "modern" or more technical dangers in this category, such as scareware, ransomware or rootkits. The second place is held by a technical danger as well, hacker attacks. They were introduced as a term, but the real types were not mentioned. In our opinion, by hacking students mean everything that refers to the creation and distribution of malware, data stealing by breaking passwords, but not to DDoS (electronic attack involving multiple computers, which send repeated requests to a server to make it inaccessible for a period of time), phishing, backdoor, botnets. This option they have should be regarded as one at hand, easy to extract from theory and bring to discussion. The next two dangers frequently mentioned by the future accountants are not technical. 47% of the students mentioned the decrease of work productivity as an effect of employees wasting time on SN sites, chatting with friends, which leads to a delay in finishing and handing over the accountancy documents. 31% say that the SN disrupt the employees from working tasks – receiving messages or other notes or checking the SN in order to see new posts, they might make mistakes when they upload or process data. In percentages between 20% and 30%, there is mentioned data theft (photos, documents, personal or company information), including IT spying, destroying data, affecting confidentiality, breaking or finding the password from user access accounts.



Source: questionnaire interpretation

Figure no. 7 – Risks and dangers hierarchy in Social Networks

Less than 20% of the respondents wrote about the following:

– Communicate wrong or unsuitable data about the company (even accountancy data), by mistake or being angry, which could consequently compromise the company;

– Lack of credibility of the information received from partners / displayed in SN;

– Employee identity theft which might lead to compromising the image of the company;

– Addiction of the employees on SN;

– Information theft / associating information about the employees and the products of a company and using them maliciously by the competitors.

10% or less of the students mentioned the following:

– Cheating/harassment/abuse/denigration of the employees or the company which become possible because the employees upload too much information about themselves;

– The fact that the official page of the company might be mistaken for other fake pages, the users might create fake profiles, so that the employees don't know who they communicate with in reality;

– If the employees use SN to solve tasks from work, in case the network fails due to an electricity or connection failure, this might lead to delays in the accomplishment of the tasks;

– Gathering data about the users without them being aware of it (Social Ads);

– Loss of official papers or even the access of unauthorized people to them;

– The social networks might install applications on the computer without the user's knowledge which leads to overloading the memory or the system;

– The posted data are in Cloud, and they are not owned by the users;

– The data from the browsing history is often non-encrypted and they can be a valuable source of confidential information;

– Continuous exposal to the information flow offered by the SN leads to a degree of inertia in the employees, since they no longer search for the information on their own, they expect they should receive them.

Out of the 200 students who took part in the study, only 10 noticed the inadequate use of SN in accomplishing the tasks of a professional accountant.

The main benefit identified by the students, is, in our opinion, still a risk. 36% considered the SN as an appropriate environment for the sending files, ideas, plans, reports easily and in real time, to a large number of employees. There were often mentioned accountancy files, information required for the accountancy reports. We can notice from their answers that they already have this habit of sending files to their peers. In the same percentage, they consider that SN, especially the internal networks of the companies (e.g. Microsoft) help to a better collaboration of the employees, facilitate team work at distance, allowing video or text conferences with several participants at the same time. A third of the students, again, consider that the social networks make it possible to spread information about the company easily and free of charge, serving as publicity and enhancing the image of the company. The educational aspect of these networks was greatly appreciated. Different segments or social groups are directly interested in the accountancy news, spreading a lot of useful information. The future accountants keep up with the latest news on laws being annulled, changed or voted from pages such as *AvocatNet*, *contabilul.ro*, *codfiscalnet*, *Acounting all the time*, and they follow the official pages of state institutions. They exchange opinions about accountancy issues, ask for help in solving the accountancy problems in their (private) group and receive quickly the expected answer. Thus, they have the feeling of belonging to a community or even that they work in a team and consider Facebook a valuable environment to spread and acquire knowledge. Apart from the groups on Facebook, they state that the tutorials on YouTube can also be useful.

30% of the students consider that SN are useful when communicating to clients and suppliers. Other benefits they mention are the low cost, the fact that Facebook is a good source of information, including news about products, clients and suppliers. 10% of the answers mention the fact that keeping in touch with the family or friends, the employees share pleasant memories and become more relaxed. Then, there are mentioned widely the benefits of LinkedIn, from both the individual perspective (”It helps to find a job and to meet new, valuable people from your field”), as well as the perspective of the company (social networks might help the company to advertise new positions and find information about the psychological profile, marital status or previous experience of their future employees).

5. CONCLUSIONS

Few universities have adopted coherent strategies and policies for a secure Social Media integration in pedagogical teaching and learning activities. In our opinion, there is a real need for institutional involvement and individual actions at the academic level, regarding the SM in general and SN sites use in particular. Web 2.0 technologies and SN are here to stay, so blocking their use or simply letting them be are not viable solutions. Based on the already acquired student knowledge in the field and on their awareness regarding the SM risks and security problems, faculty management should establish a coherent security policy and a set of procedures that should be diffused so that all the students should become aware of it. The already-careful behavior of students should be trusted – in universities, the general trend is one of technological advance and today’s employees are the same people

who previously embraced the e–mail communication, browsing and searching – and they serve as good examples and inspiring factors for their students. In the most cases, they know the rules and have the adequate behavior. The students' involvement in SM must be encouraged, existing teaching methods must be adapted to these new media and the students' real life and SM knowledge must be exploited. Feedback should be sought and given in a constant, coherent and consistent manner. The permanent availability of SM and its capacity to remember can be used to keep in touch with graduates, whose help can be required for providing support to their younger colleagues, in the form of information, advice, internships or job offers. The informal nature of SM can be the source for an increased communication between professors and students, with positive results on both categories' satisfaction level and on university' reputation.

We have to admit that the methodology applied in this two studies has some limitations. First, by some measures, the sample size might be considered relatively small (even if it is larger than the ones used in similar Romanian studies). Secondly, the first study assesses a specific group, primarily students attending university, who may differ from other Internet users in important ways, such as their easy access to Internet connections. The group questioned in the second study is even narrower and has previous knowledge on SM security. Thirdly, only one type of social networking site was mainly assessed here. It may be that other sites are used in different ways, particularly since Facebook originated as a student site and has attracted many student-age people.

References

Airinei, D., Grama, A., Fotache, D., Georgescu, M., Munteanu, A., Dospinescu, O., . . . Păvăloaia, V. D., 2014. *Tehnologii informaţionale aplicate în organizaţii*. Iaşi: Editura Universităţii „Alexandru Ioan Cuza"

Andrei, A. G., Iosub, D., and Iacob, A., 2010. Motivations for Using Social Networking Sites: The Case of Romania. *Revista economică, 1*(5(52)), 17-22. https://mpra.ub.uni-muenchen.de/61150/1/MPRA_paper_61150.pdf

Benson, V., Saridakis, G., and Tennakoon, H., 2015. Information disclosure of social media users: Does control over personal information, user awareness and security notices matter? *Information Technology & People, 28*(3), 426-441. DOI: http://dx.doi.org/10.1108/ITP-10-2014-0232

Bolton, R. N., Parasuraman, A., Hoefnagels, A., Migchels, N., Kabadayi, S., Gruber, T., . . . Solnet, D., 2013. Understanding Generation Y and their use of social media: a review and research agenda. *Journal of Service Management, 24*(3), 245-267. DOI: http://dx.doi.org/10.1108/09564231311326987

Ernek Alan, A., and Eyuboğlu, E., 2012. *Generation Y Consumers in Turkey: Are They Really Social Media Nerds or Pretend To Be?* Paper presented at the 11th International Marketing Trends Congress, Venice, Italy.

Friedl, J., and Tkalac Verčič, A., 2011. Media preferences of digital natives' internal communication: A pilot study. *Public Relations Review, 37*(1), 84-86. DOI: http://dx.doi.org/10.1016/j.pubrev.2010.12.004

Grama, A., and Păvăloaia, V. D., 2014. Outsourcing IT - The Alternative for a Successful Romanian SME. *Procedia Economics and Finance, 15*, 1404-1412. DOI: http://dx.doi.org/10.1016/S2212-5671(14)00605-4

Horváth, G., Bakó, R. K., and Biró-Kaszás, E. (Eds.), 2014. *Ten Years of Facebook. Proceedings of the Third International Conference on Argumentation and Rhetoric*. Oradea, Romania: Partium Press.

Măzăreanu, V. P., 2010. *Economia digitală si managementul riscurilor*. Iaşii: Editura Tehnopress.

Munteanu, A., Fotache, D., and Dospinescu, O., 2008. *Information Systems Security Risk Assessment. Harmonization with International Accounting Standards*. Paper presented at the International Conferences on Computational Intelligence for Modelling, Control and Automation (CIMCA 2008), Intelligent Agents, Web Technologies and Internet Commerce (IAWTIC 2008), Innovation in Software Engineering (ISE 2008), Vienna, Austria.

Oprea, D., 2007. *Protecția și securitatea informațiilor* (2 ed.). Iași: Editura Polirom.

Pînzaru, F., and Mitan, A., 2013. Generation Y Students: Using Facebook for Communicating with University Staff and Professors. *Management Dynamics in the Knowledge Economy, 1*(2), 221-239.

Radu, D. L., 2013. The Influence of Social Media on Green IT. In B. Pătruț (Ed.), *International Conference SMART 2013 - Social Media in Academia: Research and Teaching* (pp. 213-219). Bologna, Italy: Medimond - Monduzzi Editore International

Santos, D., and Čuta, M., 2015. The usage of social networks by university students (A survey of Facebook use patterns among young people). *Anthropologia integra, 6*(1), 35-43.

Tkalac Verčič, A., and Verčič, D., 2013. Digital natives and social media. *Public Relations Review, 39*(5), 600-602. DOI: http://dx.doi.org/10.1016/j.pubrev.2013.08.008

Țugui, A., and Șiclovan, A., 2013. Social Media Interaction via Cloud Computing in Romania. In B. Pătruț (Ed.), *International Conference SMART 2013 - Social Media in Academia: Research and Teaching* (pp. 239-245). Bologna, Italy: Medimond - Monduzzi Editore International.

Ujhelyi, A., and Szabó, E., 2014. Sharing on Facebook. From "Loners" to "Popularity seekers". In G. Horváth, R. K. Bakó and E. Biró-Kaszás (Eds.), Ten Years of Facebook - Proceedings of the Third International Conference on Argumentation and Rhetoric (pp. 15-32). Oradea, Romania: Partium Press. DOI: http://dx.doi.org/10.13140/2.1.1765.2808

Vasilescu, R., 2011. The Romanian Generation Y: Preparing Today's Students for Tomorrow's Job Market. *Annals of Spiru Haret University, 2*(1), 47-53.

Whiting, A., and Williams, D., 2013. Why people use social media: a uses and gratifications approach. *Qualitative Market Research: An International Journal, 16*(4), 362-369. DOI: http://dx.doi.org/10.1108/QMR-06-2013-0041