Croatian Journal of Education
Vol.17; No.2/2015: pages: 569-595
Professional paper
Paper submitted: 23rd October 2012
Paper accepted: 16th November 2013
doi: 10.15516/cje.v17i2.555

The Impact of Media on Students' Perception of the Security Risks Associated With Internet Social Networking – A Case Study

Nenad Putnik and Milica Bošković
Faculty of Security Studies, University of Belgrade

Abstract

From the viewpoint of cybercrime, young people represent a particularly vulnerable category of Internet users: children, adolescents and students. Young people are, undoubtedly, the most common and the most gullible users of social networks. Due to lack of education related to dangers they are exposed to on social networks, inexperienced users recklessly post information and multimedia contents on their profiles which can be misused by differently motivated Internet users. Apart from being exposed to the risk from the violation of personal privacy and misuse of personal data, young people are exposed to the risk from political or ideological manipulation. Various studies on social networks and secondary school students have been conducted in the Republic of Serbia. However, no study in this field which would look at university students has yet been conducted. The purpose of this study was to discover the extent to which students use social networking sites, but also the sources and ways students perceive online security risks associated with social networking. Study results show that the media has a dominant role in educating young people on the risks associated with social networking and that the impact of the media is greater than the impact of other educational factors such as family, school or university.

Key words*:* *media; security impact; social networks.*

Introduction

Cybercrime is a relatively new kind of criminal activity that covers all the ways in which computers and other types of portable electronic devices such as cell phones and PDAs capable of connecting to the Internet are used to break laws and cause harm.

In a more technical sense it refers to the use of computers or other electronic devices via information systems such as organizational networks or the Internet to facilitate illegal behaviours. Cybercrime has come about and evolved with the Internet and the proliferation of the advances in the information technologies.

Definitions of Cybercrime differ depending on the perception of both the observer/ protector and the victim and the phenomenon has many different facets and occurs in a wide variety of scenarios and environments. The Council of Europe's Cybercrime Treaty uses the term 'Cybercrime' to refer to the offences ranging from criminal activity connected with data misusage to content and copyright infringement. Zeviar Geese (1997-98) suggests that the definition has a broader scope and includes activities such as fraud, unauthorized access, child pornography, and cyber stalking, and the UN Manual on the Prevention and Control of Computer Related Crime includes fraud, forgery, and unauthorized access in its cybercrime definition. Probably the most appropriate definition is that Cybercrime is any crime that is facilitated or committed using a computer, network, or hardware device. The computer or device may be the agent of the crime, the facilitator of the crime, or the target of the crime; indeed, the crime can take place on the computer alone, or in other non-virtual locations.

Gordon and Ford (2006) suggest two main types of Cybercrime.

Type I, more technical in nature, with the following characteristics:

1. It is generally a singular, or discrete, event from the perspective of the victim.
2. It often is facilitated by the introduction of crimeware programs such as keystroke loggers, viruses, rootkits or Trojan horses into the user's computer system.
3. The introductions can, but may not necessarily be, facilitated by vulnerabilities.

This type of Cybercrime requires that data be protected from the traditional threats such as viruses and worms, but also that users be cognizant of the concept of 'vulnerabilities'.

More human in nature is type II Cybercrime which is positioned at the other end of the spectrum: it includes, but is not limited to activities such as cyber stalking and harassment, child predation, extortion, blackmail, stock market manipulation, complex corporate espionage, and planning or carrying out terrorist activities online. The characteristics of Type II Cybercrime are that:

1. It is generally facilitated by programs that do not fit under the classification crimeware. For example, conversations may take place using IM (Instant Messaging) and clients or files may be transferred using the FTP protocol (File Transfer Protocol).
2. There are generally repeated contacts or events from the perspective of the user.

Even though there is no generally accepted definition of Cybercrime, it is clear that this phenomenon is assuming new forms and is continuously expanding. Cybercriminals constantly devise new tools, equipment and methods for achieving their goals. One of them includes collecting data on a potential victim from their profile on a social network. Data collected are used, in the second step, for committing a criminal activity in the real or virtual world.

From the viewpoint of cybercrime, young people represent a particularly vulnerable category of Internet users: children, adolescents and students. The access to different Internet contents and currently very popular social networks such as Facebook and Twitter is provided to young people not only through personal computers or computer networks, but also through smartphones. Quick wireless access to the Internet with these devices enables receiving and sending e-mails as well as communication within social networks. The access to social networks, exchange of information, receiving and sending messages in this way, assumed multiple dimensions including space and time, which significantly reduced the possibility of parental control.

Young people are, undoubtedly, the most common and the most gullible users of social networks. Due to lack of education related to dangers they are exposed to on social networks, inexperienced users recklessly post information and multimedia contents on their profiles which can be misused by differently motivated Internet users. Apart from being exposed to the risk from a violation of personal privacy and misuse of personal data, young people are exposed to the risk from political or ideological manipulation.

Young People and Internet-Based Social Networking Sites Security Risks

The information published on public social networking sites may be misused by other Internet users among whom are cybercriminals, mentally ill people, politically and ideologically motivated groups and the like. The youngest users, unaware of the dangers, often post their home address details, telephone numbers, information about the time when their parents are at work (when they are home alone), the period in which they will be on holidays and other sensitive information. Twitter, which is very popular among this population, enables them to post even their personal timetables of daily activities – when the children are at school, where they are going to go after school, where they currently are and what they are doing, etc. This information may be misused for planning and carrying out criminal activities: robbery, abduction, physical and psychological abuse, etc. Violation of personal privacy may consequently lead to violation of physical integrity of a person.

The information children post on their user profiles is most commonly misused by their peers. It is the phenomenon of cyber-bullying which implies teasing, tormenting, or in more severe cases, abuse in the virtual world. Cyber-bullying is a phenomenon which shows a steady increase. The results of the study which was conducted in five secondary schools in Belgrade indicate that 10% of the students aged between 11 and 15 were engaged in this type of activity directed against other students. Besides, the study indicated that 20% of the students fell victim to these virtual campaigns (Popović-Ćitić et al., 2011, p. 412). This form of torture can cause serious psychological effects, which was widely debated in the professional literature after discovering the first case of virtual rape (Johnson, 2001).

On the other hand, however, cases were registered where bullies take over even the virtual identity of the target of attack, i.e. the victim with the aim of enhancing the effect of campaigns of denigration or, perhaps, achieving criminal intentions.

Every individual is vulnerable to different types of overt and covert attacks by malevolent perpetrators, whether with the purpose of playing practical jokes or clear criminal intent. A sense of violation and loss of personal peace and privacy may have long-term psychological effects. Internet-based social networking sites supply the attacker with a large amount of information about the victim, which gives them the opportunity to engage in psychological warfare. Cyber libel or digital campaigns of denigration have a potential to reach incredibly large numbers of people quickly, and at the same time cause immense frustration and inflict collateral damage on victims. Restoring trust and re-establishing reputation in the midst of virtual campaigns of denigration represent a great difficulty for the victim. The targets of attack are put in a position to defend themselves and they are uncertain about the attacker's identity, motives, location, goals, as well as whether the attack is being performed by an individual or a group of people. The targets usually do not know who to turn to for help in such situations since there is confusion over the responsibilities for these offences in the majority of countries.

The second category of risk involves propaganda and integrating capacities of social networks. The fact is that social networks represent space where ideas and ideologies are promoted, campaigns initiated, like-minded people motivated and grouped. These digital meeting places enabled individuals and different, most often marginalized groups of people, to exchange ideas. On social networks group identity is rapidly formed and strengthened – lone voices echo easily and rapidly. There is a fine line between apparently harmless lobbying and fierce criticism of the circumstances of a society and digital anarchy.

Previous Research

The media has a long-term and sometimes systematic impact on cultural and sociological shaping and behaviour of communities, and it even influences political, economic and security-related circumstances of a country. The need to analyze and explain sociological, economic as well as security-related role and impact of mass media on the society, groups, and individuals arises from all the above mentioned (Bošković et al., 2012). Many authors concentrated their intellectual efforts and research on the analysis of media impact on the violent behaviour of its consumers, individuals and social groups alike. The backbone of the majority of studies is based in the findings about the processes of imitation, social learning and identification.

Although often inconsistent regarding the methodological approach and followed by criticism or praise from other researchers (Cook et al., 1983; Freedman, 1984), many studies, laboratory and field research indicate that scientific and professional bodies are considerably and continually interested in researching the phenomenon of the media and its impact on the consumers. Certain studies in this field indicate that the exposure to media violence has short-term effects, to say the least, in terms of encouragement to aggressive behaviour.

According to one type of a cognitive approach adopted by Berkowitz (1984), aggressive motives and ideas conveyed in violent films may activate aggressive thoughts in viewers. When one such thought is activated, other thoughts strongly associated with it will also be activated (Felson, 1996). Bandura (1973) however, presumes that violent scenes broadcast by the media may provoke aggressive thoughts and behaviour in those individuals who are predisposed to such emotions and concrete reactions due to the psychological structure of their personalities. Banks (2005) conducted a study on the impact of media crime on insecurity in local context.

The Internet, as a specific medium, and social networks as one of the most up-to-date modes of communication, from the very beginning were considered as one of many technological and virtual phenomena. This type of a social model which resides in, above all, global network technology is a subject of numerous and various studies. Social networks have been studied from the aspect of telecommunications, technical and computer science disciplines, but they have also been the subject of various Psychological, Sociopolitical, Pedagogical and Security Studies.

Social networks represent a model of virtual connecting and interacting between people or groups of different gender, age, ideological, religious or political beliefs; they also serve as portals for the promotion of commercial products and services, for dissemination of ideas about social and political movements or presentation of personal skills, experiences or emotional states. Considering the above mentioned information, social networks represent a current and attractive research issue which is being studied from different aspects – social, political, organizational, security aspects.

Early studies indicated that the most active users of social forums were of libertarian orientation, and they passionately believed in the capability of social circles and individuals, rather than states, to solve the problems of today (Katz, 1997, pp. 68-82). Activist groups such as associations for animal rights, or gay or lesbian organizations, determined to win equal rights to their members, used forums as one of their earliest weapons to express opinions in a cheap and far-reaching way. Strategy and tactic as such were not significant. Their goal was mass dissemination of ideas. There are cases where social networks were used by activist groups which advocate a ban on abortion, euthanasia and cloning. They were, in a way, the forerunners of future militarization of social and ideological activism.

The impact of the Internet and social networks on creating or changing political, social or economic circumstances in countries was a subject of numerous studies (Schmitt-Beck & Mackenrodt, 2010; Margetts et al., 2011; Bošković & Putnik, 2011). In recent years, social networks such as Facebook and Twitter have become an inevitable tool for gathering political activists and even initiating revolutionary movements in some countries. Their role and importance were apparent especially in, provisionally speaking, non-democratic countries or in case of serious social and legal disruption where the media such as radio and television stations, printed and online magazines were controlled by governing structures (Bošković & Putnik, 2011). With the advance of global computer network and graphical user interface, social and political activists are presented with more options for engaging in debates, proving their own 'truths', raising funds or recruiting new members. Religiously or ideologically motivated groups such as religious sects or terrorist organizations now have funds at their disposal to wage electronic wars.

The exchange of personal details through social networking sites and the use of these systems for disseminating ideological, religious and political beliefs and calls for activism represent a challenge for national security structures in relation to national security protection and achieving personal safety of network users, especially underage users. The security issues, privacy protection and the rights of citizens on social networks were studied by Asher et al. (2009), and Van Eecke and Truyens (2010).

In a digital environment, the risks of manipulating and recruiting young people by such organizations became much more apparent due to a reduced possibility of controlling child behaviour by parents or teachers. Forkosh-Baruch and Hershkovitz (2012), and Popović-Ćitić et al. (2011) conducted studies in the field of the impact of social networking on the educational processes and the climate of educational institutions. Bicen & Cavus (2011) investigated the students' habits regarding the usage of the social network Facebook. Facebook is one of the biggest social networks according to the number of users and therefore it is a subject of numerous studies (Buckman, 2005; Ross et al., 2009).

Motivational Factors and the Frequency of Use of Social Networking Sites by Secondary School Population

The studies related to online social networks have recently become ever more developed. Recent studies confirmed the existence of three dimensions of using these networks, namely: informative, friendly and connecting (Raacke & Bonds-Raacke, 2010), and four primary reasons behind joining Facebook groups were discovered: socializing, fun, search for their own status and information (Park et al., 2009).

National studies on the social usage of Facebook by secondary school students identified three factors: F-virtual, F-socializing and F-friends (Kordić & Babić, 2011). F-friends factor refers to Facebook usage which adds to and enriches socializing with actual friends and acquaintances. F-socializing factor refers to the usage of Facebook which satisfies the need for socializing, fun, lifting the mood and alleviating life's hardships. The difference between these two factors is that the first one is related to the instrumental use, and the second one is related to the compensatory use of Facebook. F-virtual factor refers to certain effects of Facebook usage such as more intensive socialization and greater fun with online friends, greater sense of acceptance in the virtual world and neglecting daily responsibilities and meetings. Higher values of this factor reflect the compensatory usage of Facebook, and lower values reflect the instrumental use of Facebook.

Previously mentioned national study on the social usage of Facebook (Kordić & Babić, 2011) explained that Facebook was primarily used as an extension and support of the users' real social lives. Only a minor group of secondary school students preferred socializing on Facebook to common forms of socializing. The increase in Facebook popularity in Belgrade coincided with the increase in its popularity in the USA. The number of Facebook users increased from 22% in 2008 to 78% in 2009 (Lenhart et al., 2010). The majority of secondary school students in Belgrade (73.33%) used Facebook at least once a day (Kordić & Babić, 2011) and mainly spent up to two hours on Facebook according to the data obtained in 2009. The data from 2008 on American teenagers showed that 48% used Facebook once a day (Lenhart, 2009).

Evaluation of Risks of Using Online Social Networking by Secondary School Population

In the previous chapters we indicated the fact that young people as social network users are exposed to the risks of violating personal privacy, misuse of private information and political or ideological manipulation. All the mentioned risks, if they materialize, result in the violation of the psychological integrity of a person.

From the aspect of the security risks evaluation, the important factors are the size of an online social network and the number of the unknown 'friends' the user accepted. According to the data for the year 2010, an average Facebook user had 130 Facebook friends (Hepburn, 2010). The sample of Belgrade secondary school students contained 84% of users with more than 100 Facebook friends. Security risks are represented by the number of unknown Facebook friends since 38% of Belgrade secondary school students had more than 50 unknown friends (Kordić & Babić, 2011).

Foreign studies confirmed a significant correlation between prosperity, the frequency of visiting the sites and information received by others on those sites (Valkenburg et al., 2006), as well as a greater benefit for users with low self-confidence and low life satisfaction (Ellison et al., 2007). Based on the domestic research on Facebook usage and socializing among Belgrade secondary school students, four typical groups of young people were identified under the following names (Kordić & Babić, 2011): 1. a group of young people who seldom use Facebook and rarely socialize (the Shy) makes up 38% of secondary school students, 2. a group of young people focused on socializing through sporting activities with their neighbourhood friends (Athletes) makes up 16% of secondary school students, 3. a group of young people who socialize on Facebook and at school (Virtual) makes up 12% of secondary school students, and 4. a group of young people who contact their neighbourhood friends in real life and on Facebook (Friendly) makes up 34% of secondary school students.

Evaluation of risk from using online social networks among secondary school population was conducted at the end of 2011 (Kordić & Putnik, 2011). This study conceived from the socio-psychological aspect concluded the following:

A smaller number of young people among Belgrade secondary school students is especially attached to Facebook (12%) and uses it mainly in a compensatory manner since it satisfies many basic social needs in a virtual way (Kordić & Babić, 2011). They have the impression that Facebook lifts their mood, brings new friends, creates a sense of fellowship and assistance in hard times. It is a group of secondary school students who use Facebook for boosting self-confidence and popularity among their peers (Christofides et al., 2009). Such a group of young people is a risky group which is easily manipulated especially because their personal integrity is weaker than the integrity of the average population of young people. In relation to the types of security risks, this group is more vulnerable to all types of security risks, although a greater risk lies in violating personal privacy and misusing private information since it can cause personal disintegration of a user.

A significant number of young people among secondary school students in Belgrade socialize with real friends and Facebook friends alike. This group also falls into a risky category, but in a different way from the previous group. They use Facebook in a more instrumental manner and therefore the possibility of political (ideological) manipulation is increased since the members of this group are vulnerable to group pressure due to their need to preserve group identity.

The third group in terms of the risk factor is the group of 'shy' students. The probability of materializing the risks is significantly lower due to the less frequent use of online social networks. However, it remains uncertain as to what socio-psychological characteristics of the 'shy' group are, given that a high level of socialization is normally expected at the secondary school level. If it is a socio-psychologically vulnerable group, even a limited use of online social networks may present a risk in the case of cyber threats.

The lowest risk group is the group of 'athletes' due to their active lifestyle, clear social identity and limited instrumental use of online social networks.

The general conclusion of the above mentioned study explicitly states that a lack of education on the safe usage of these resources is apparent among secondary school students in the Republic of Serbia, and that promoting security culture and safe online behaviour would increase the security level of the members of virtual communities, among which young people are the most vulnerable category.

Assessment of Media Impact on Students' Awareness of Risks Associated with Using Online Social Networks

The conclusion of the above-mentioned study refers to the population of secondary school students. Our intention was to test this hypothesis on the student population in a separate study. The aim was to discover the perception of threats and security risks related to the use of social networks among the student population, as well as the information about how they had learnt the basic facts about these risks.

Method

Descriptive research methodology was used with a non-experimental fixed design in this research paper, along with quantitative survey research. Descriptive research methodology was used with a non-experimental fixed design because dealing with things as they are has the advantage of not disturbing that what is of interest (Robson, 2002). A non-experimental fixed design can be defined as a systematic inquiry in which the researcher does not have direct control of the independent variables because the manifestations of the independent variables have already occurred (Kerlinger, 1986). Fixed designs generally employ a detached researcher to protect against the actual researcher having an effect on the results of the research (Robson, 2002).

This study was quantitative because questions were answered about the relationships among the measured variables with the purpose of explaining, predicting, and controlling phenomena (Leedy & Ormrod, 2005). Self-report or survey research was used in this study that required a questionnaire, which is a written group of questions that are answered by a selected group of research participants (Gay, Mills, & Airasian, 2006). Survey research involves acquiring information about one or more groups of people by asking them questions on a questionnaire and tabulating their answers using statistical indexes to draw inferences about a particular population (Leedy & Ormrod, 2005).

Participants

The study examined the attitudes of 100 final year students at the Faculty of Security Studies of the University of Belgrade and 50 secondary school students-graduates, who preliminary applied to enrol the said faculty. The research was conducted in the period from April to May 2012.

The sample was purposive because the researcher wanted to examine participants' attitudes for a purpose. Purposive sampling is the process of choosing a sample that is believed to be representative of a given population and the researcher identifies criteria for selecting the sample (Gay et al., 2006). Both participant groups were surveyed because this was not a large-scale study. We applied our experience and the expertise of university teachers to select the sample and examine the participants' attitudes for a purpose. One may think that the sample is not representative because the students of only one faculty were surveyed, but that is not the case. The Faculty of Security Studies of the University of Belgrade, Serbia, with its curriculum in the field of Security Studies, is a unique state-owned educational institution in the Republic of Serbia. It is one of few higher education institutions whose curriculum provides for the education of students in the field of cybercrime. Bearing in mind the contents of the Security Studies curriculum and the fact that the Faculty educates future graduates with security management degrees, we assumed that final year students must have more acute awareness of the threats posed by cybercrime than their colleagues from other faculties. Precisely for these reasons we wanted to conduct a research study to assess the extent of media impact, specific education and social environment on the perception of security risks of this sample of students. The permission from the University of Belgrade – Faculty of Security Studies had been obtained before the questionnaire was distributed to the examinees.

Instrument

The survey instrument used in the study was developed by the authors. The participation was voluntary and anonymous. The questionnaire contained 4 closed-ended questions. The examinees selected one of the options offered. Two of the questions were answered by all examinees. Those two basic questions were dichotomous, i.e. the options offered were YES and NO. Answering the remaining two questions was conditioned by the answers given to the dichotomous questions. The options offered for two optional questions are given in the section which analyzes research results.

The questionnaire contained the following questions:

1. 'DO YOU HAVE YOUR OWN *PROFILE* ON ANY SOCIAL NETWORKING SITE?'; this question was both a basic question and a dichotomous question.
2. 'PRIMARY PURPOSE OF USING SOCIAL NETWORKING SITES'; this question was answered by the examinees who answered the first question with YES.
3. 'DO YOU THINK THAT THE INTERNET AND SOCIAL NETWORKING SITES CAN SIGNIFICANTLY COMPROMISE PHYSICAL, MORAL OR PSYCHOLOGICAL INTEGRITY OF A PERSON?'; this question was both a basic question and a dichotomous question.
4. 'HOW AND FROM WHAT SOURCES WERE YOU MAINLY INFORMED ABOUT DIFFERENT RISKS AND DANGERS OF USING THE INTERNET, E-MAIL ACCOUNTS OR SOCIAL NETWORKING SITES?'; this question was answered by the examinees who answered the third question with YES.

Data Analysis

Statistical method was applied to analyze the examinees' answers, and the results were expressed as numerical values and as percentages. In this paper, characteristic results are also presented in charts.

Results and Discussion

The survey questions were asked for the purpose of establishing whether students and secondary school graduates use the Internet, social networks and other global network applications, and how they participate in the benefits and risks of these modern media. 79 students and 35 secondary school graduates created 'Profiles' on some social network. The majority of those who have a 'Profile', 61 students and 30 secondary school graduates, use it for virtual contacts and association, rather than for promoting their own knowledge and skills or making new contacts in the real world. The question 'Do you think that a social network can significantly compromise physical, moral or psychological integrity of a person?' provided an almost equal number of answers for the options 'Yes' (56 students) and 'No' (44 students). The same question was answered by 39 secondary school graduates with 'Yes' and by 11 of them with 'No'. For those who answered the previous question positively, the questionnaire asked an additional question 'How were you informed about the harm that the Internet, e-mails and social networks can cause?' For this question the provided options were: 'family talks' (A), 'at secondary school' (B), 'at the Faculty' – for students only (C), 'from personal experience and learning' (D), 'through the media – news, documentaries and entertainment programs' (E). The most frequent answers were: (D) – 24 students and 9 secondary school graduates and (E) – 32 students and 30 secondary school graduates.

Students and secondary school graduates were also asked about the modern types of media, such as the Internet and social networks. The examinees were asked if they had a so-called 'profile' at some social network and 79% of students and 70% of secondary school graduates answered 'Yes'. The majority of them use their 'profile' for virtual socializing. Whether or not they have 'profiles', 56% of all students and 78% of secondary school graduates answered that they believed that social networks could compromise a person's physical, moral or psychological integrity. Those results are shown in Figure 1.

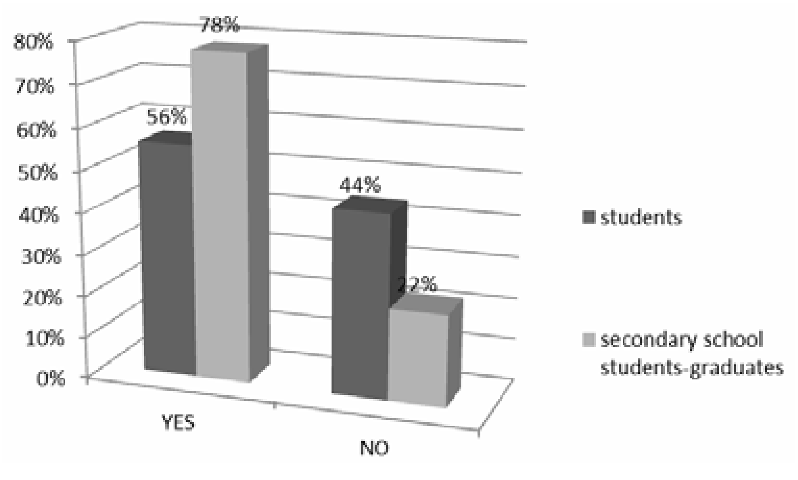

Figure 1. Answers given to the question: 'Do you think that the Internet and social networking sites can significantly compromise physical, moral or psychological integrity of a person?'

Most students (57% of them) learned about the potential risks of using the Internet and social networks from the media and 42.8% learned about such risks from personal experience. The same question was answered by secondary school graduates and 76.9% of them learned about the possible dangers from the media and 23% of them learned about the dangers from personal experience. Those results are shown in Figure 2.

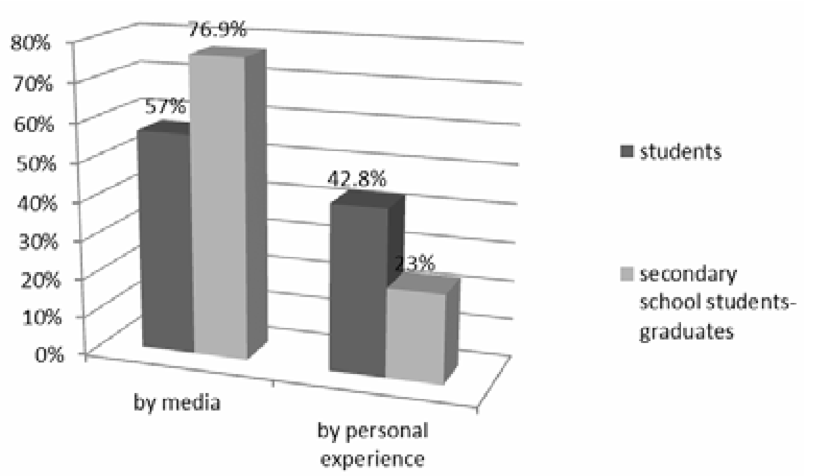

Figure 2. Answers given to the question: 'How and from what sources were you mainly informed about different risks and dangers of using the Internet, e-mail accounts or social networking sites?'

The answers given to these last questions mentioned show that students and secondary school graduates have satisfactory knowledge and skills necessary for using the global network and its products, but also that they are aware of the dangers and risks which could arise from this modern media.

Conclusion

Social networks, as a form of wireless global communication, represent a necessity, but also an unambiguous requirement of the contemporary society. Every achievement, including social networks, aims at making everyday life easier, more creative and interesting. However, innovations carry risks and security challenges. Nowadays Facebook and Twitter have tens of millions of users of different ages and interests, but also of different motives for using social networking sites. The nature of some motives is criminal. As a result of the above mentioned and having in mind the data on the misuse of profit on social networks, security prevention in relation to the risk has been made more difficult. Continual education in the field of the safe use of the Internet and communication portals is justified, necessary and has an important role in developing general security culture.

The research results showed that more than half of the students of the Security Studies, as well as the secondary school graduates, achieved a satisfactory level of security culture regarding the use of social networks, and that they acquired the knowledge about the risks and protection measures mainly through the media. Secondary school graduates-examinees acquired the knowledge about informatics and computer systems through secondary school education. Students-examinees received a four-year university education in the field of security which covers contemporary risks such as cybercrime. In their answers both groups of examinees demonstrated a personal initiative and desire for self-education in no small percentage.

Nevertheless, apart from all of the points mentioned above, the research results show that contemporary media effectively impacts acquiring different types of knowledge and creating young people's perceptions. In this case the media, more than education or social environment, has made the greatest impact on developing the awareness of the examinees of the existence of cybercrime and security risks associated with using social networks. Such results indicate that educational programs, especially those related to Security Studies, need a practical improvement of their educational processes; it also needs to make the transfer of the knowledge and messages at least equally challenging and interesting, like the media does in its own way. In relation to educational tasks, a greater attention has to be paid to the contemporary security challenges such as the risks associated with using social networks, cybercrime and similar activities on the global network. The media has an important place in the contemporary world and an unambiguous role in creating political, cultural and security awareness in the people, but education must be a directed process and an adequate primary source of knowledge and skills for social life in the communities.

References

Asher, C., & Aumasson, J. R. C-W. (2009). Security and Privacy Preservation in Human-Involved Networks. *IFIP Advances in Information and Communication Technology* 309, 139-148. http://dx.doi.org/10.1007/978-3-642-05437-2_13

Attia, A. M., Aziz, N., Friedman, B., & Elhusseiny, M. F. (2011). Commentary: The impact of social networking tools on political change in Egypt's 'Revolution 2.0'. *Electronic Commerce Research and Applications* 10(4), 369-374. http://dx.doi.org/10.1016/j.elerap.2011.05.003

Bandura, A. (1983). Psychological mechanisms of aggresion. In R. G. Green & E. I. Donerstein (Eds.), *Aggression: Theoretical and Empirical* Reviews (1-40), New York: Academic 1.

Banks, M. (2005). Spaces of (in)security: Media and fear of crime in local context. *Crime, Media, Culture* 1(2), 169-187. http://dx.doi.org/10.1177/1741659005054020

Berkowitz, L. (1984). Some effects of thought on anti – and pro-social influences of media effects. *Psychol. Bull.* 95, 410-427. http://dx.doi.org/10.1037/0033-2909.95.3.410

Bonds-Raacke, J., & Raacke, J. (2010). MySpace and Facebook: Identifying dimensions of uses and gratifications for friend networking sites. *Individual differences research 8*(1), 27–33.

Bošković, M., Alibabić, S., & Budimir Ninković, G. (2012). Obrazovni i bezbednosni rizici plasiranja šokantnih informacija u mas-medijima. Institut za pedagogiju i andragogiju, *Andragoške studije* 2, 125-140

Bošković, M., & Putnik, N. (2011). The role of social networks for modern sociopolitical and security events. *19th Telecommunications Forum (TELFOR), IEEE Conference Publications*: 110-113 /online/. Retrieved on 13th April 2012 from http:// http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6143505. http://dx.doi.org/10.1109/TELFOR.2011.6143505

Buckman, R. (2005). *Too much information? Colleges fear student postings on popular Facebook site could pose security risks*. Retrieved on 11th May 2010 from http://www.wsjclassroomedition.com/monday/mx_05dec12.pdf.

Christofides, E., Muise, A., & Desmarais, S. (2009). Information disclosure and control on Facebook: are they two sides of the same coin or two different processes? *Cyberpsychology & behavior*, 12(3), 341–345. http://dx.doi.org/10.1089/cpb.2008.0226

Cook, T. D., Kendzierski, D. A., & Thomas, S. V. (1983). The implicit assumptions of television: an analysis of the 1982 NIMH Report on Television and Behaviour. *Public Opin. Q*. 47, 161-201. http://dx.doi.org/10.1086/268779

Dabner, N. (2012). 'Breaking Ground' in the use of social media: A case study of a university earthquake response to inform educational design with Facebook. *The Internet and Higher Education*, 15(1), 69-78. http://dx.doi.org/10.1016/j.iheduc.2011.06.001

DeAndrea, D. C., Ellison, N. B., LaRose, R., Steinfield, C., & Fior, A. (2012). Serious social media: On the use of social media for improving students' adjustment to college. *The Internet and Higher Education*, 15(1), 15-23. http://dx.doi.org/10.1016/j.iheduc.2011.05.009

Ellison, N. B., Steinfield, C., & Lampe, C. (2007). The benefits of Facebook 'friends': *Social capital and college students' use of online social network sites. Journal of computer-mediated communication*, 12, 1143–1168. http://dx.doi.org/10.1111/j.1083-6101.2007.00367.x

Felson, R. B. (1996). Mass Media Effects on Violent Behavior. *Annual review of Sociology*, 22, 103-128. http://dx.doi.org/10.1146/annurev.soc.22.1.103

Forkosh-Baruch, A., & Hershkovitz, A. (2012). A case study of Israeli higher- education institutes sharing scholarly information with the community via social networks. *The Internet and Higher Education*, 15(1), 58-68. http://dx.doi.org/10.1016/j.iheduc.2011.08.003

Freedman, J. L. (1984). Effects on television violence on aggressiveness. *Psychol. Bull*, 96, 227-246. http://dx.doi.org/10.1037/0033-2909.96.2.227

Gay, L. R., Mills, G. E., & Airasian, P. (2006). *Educational research: Competencies for analysis and applications* (8th ed.). Pearson Education, Inc. Upper Saddle River, New Jersey: Pearson Prentice Hall.

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology,* 2, 13–20. http://dx.doi.org/10.1007/s11416-006-0015-z

Hepburn, A. (2010). *Facebook: Facts & figures for 2010*. Retrieved on 2nd December 2010 from http://www.digitalbuzzblog.com/facebook-statistics-facts-figures-for-2010/.

Johnson, D. (2001) *Computer ethics* (3rd Edition). Pearson Education, Inc. Upper Saddle River, New Jersey: Pearson Prentice Hall.

Katz, J. (1997). The digital citizen. *Wired*, 5(12), 68 – 82.

Kerlinger, F. N. (1986). Foundations of behavioral research. Fort Worth, TX: Harcourt, Brace, & Jovanovich.

Kordić, B., & Babić, L. (2011). Facebook i druženje kod srednjoškolaca. *Teme*, 35(4), 1627-1640

Kordić, B., & Putnik, N. (2012). *Društvene mreže na Internetu i bezbednost učenika*. In B. Popović-Ćitić, S. Đurić, Ž. Kešetović (Eds.*), Bezbednosni rizici u obrazovno-vaspitnim ustanovama* (pp. 203-223), Beograd: Fakultet bezbednosti.

Leedy, P. D., & Ormrod, J. E. (2005). *Practical research: Planning and design* (8th ed.). Upper Saddle River, New Jersey: Pearson Prentice Hall.

Lenhart, A. (2009). *Pew Internet project data memo* /online/. Retrieved on 7th June 2010 from http://www.pewinternet.org/~/media//Files/Reports/2009/PIP_Adult_social_networking_data_memo_FINAL.pdf.pdf.

Lenhart, A., Purcell, K., Smith, A., & Zickuhr, K. (2010). *Social media and young adults* /online/. Retrieved on 11th December 2010 from http://www.pewinternet.org/~/media//Files/Reports/2010/PIP_Social_Media_and_Young_Adults_Report_Final_with_toplines.pdf.

Margetts, H., John, P., Escher, T., & Reissfelder, S. (2011). Social information and political participation on the internet: an experiment. *European Political Science Review*, 3, 321-344. http://dx.doi.org/10.1017/S1755773911000129

Park, N., Kee K. F., & Valenzuela, S. (2009). Being immersed in social networking environment: Facebook groups, uses and gratifications, and social outcomes. *Cyberpsychology* & *Behavior*, 12(6), 729–733. http://dx.doi.org/10.1089/cpb.2009.0003

Popović-Ćitić, B., Djurić, S., & Cvetković, V. (2011). The Prevalence of cyberbullying among adolescents: A case study of middle schools in Serbia. *School Psychology International*, 32 (4), 412-424. http://dx.doi.org/10.1177/0143034311401700

Robson, C. (2002). *Real World Research* (2nd ed.). Malden, MA: Blackwell Publishing.

Ross, C., Orr, E. S., Sisic, M., Arseneault, J. M., Simmering, M. G., & Orr, R. R. (2009). Personality and motivations associated with Facebook use. *Computers in Human Behaviour*, 25 (2), 578-586. http://dx.doi.org/10.1016/j.chb.2008.12.024

Zeviar-Geese, G. (1997-98). The State of the Law on Cyberjurisdiction and Cybercrime on the Internet. California Pacific School of Law.

Nenad Putnik
Faculty of Security Studies, University of Belgrade
Gospodara Vučića 50, 11 000 Belgrade, Serbia
nputnik@fb.bg.ac.rs

Milica Bošković
Faculty of Security Studies, University of Belgrade
Gospodara Vučića 50, 11 000 Belgrade, Serbia
boskovicmil@gmail.com

Utjecaj medija na percepciju sigurnosnih rizika povezanih s društvenim umrežavanjem putem interneta – studija slučaja

Sažetak

S gledišta kibernetičkoga kriminaliteta mladi ljudi (djeca, adolescenti i studenti) predstavljaju osobito ranjivu skupinu korisnika interneta. Mladi su ljudi, bez sumnje, najčešći i najlakovjerniji korisnici društvenih mreža. Zbog nedostatka edukacije o opasnostima kojima su izloženi na društvenim mrežama, neiskusni korisnici na svojim profilima nesmotreno objavljuju informacije i multimedijske sadržaje koje mogu upotrijebiti korisnici interneta koji imaju drugačije motive. Osim što su izloženi riziku kršenja osobne privatnosti i zlouporabe osobnih podataka, mladi se ljudi izlažu mogućoj političkoj i ideološkoj manipulaciji. U Republici Srbiji provedene su razne studije o društvenim mrežama i srednjoškolcima, no ni jedna od tih studija nije za ciljnu skupinu imala studente. Svrha ovoga istraživanja bila je ustanoviti do koje se mjere studenti koriste društvenim mrežama na internetu i utvrditi izvore putem kojih se informiraju o sigurnosnim rizicima vezanim uz društveno umrežavanje. Rezultati istraživanja pokazuju da mediji imaju dominantnu ulogu u upoznavanju mladih ljudi s rizicima vezanim uz društveno umrežavanje. Utjecaj medija veći je od utjecaja ostalih odgojno-obrazovnih čimbenika kao što su obitelj, škola ili fakultet.

Ključne riječi: *društvene mreže; mediji; sigurnosni utjecaj.*

Uvod

Kibernetički kriminalitet relativno je nova vrsta kriminalnih aktivnosti koja obuhvaća sve načine na koje se koriste računala i ostali prijenosni elektronički uređaji kao što su mobilni telefoni i dlanovnici s pomoću kojih se korisnici mogu spojiti na internet i prekršiti zakon ili nekome učiniti nešto nažao. U tehničkom se smislu navedenim terminom opisuje uporaba računala i drugih elektroničkih uređaja putem informacijskih sustava, kao što su organizacijske mreže ili Internet, s ciljem obavljanja nezakonitih aktivnosti. Kibernetički je kriminalitet nastao i razvio se razvojem interneta i procvatom napretka informacijskih tehnologija.

Definicije kibernetičkoga kriminaliteta razlikuju se ovisno o viđenju promatrača/zaštitnika i žrtve, a ta pojava ima puno raznih aspekata i pojavljuje se u vrlo različitim scenarijima i okruženjima. U *Konvenciji Vijeća Europe o kibernetičkome kriminalitetu* terminom „Kibernetički kriminalitet" opisuju se kažnjiva djela u rasponu od kriminalne aktivnosti zlouporabe podataka do kršenja sadržaja i autorskih prava. Zeviar-Geese (1997-98) smatra da je definicija širega opsega i da uključuje aktivnosti kao što su prevara, neovlašten pristup, dječja pornografija i kibernetičko uhođenje, a *Smjernice Ujedinjenih naroda za prevenciju i kontrolu računalnog kriminaliteta* navode prevaru, krivotvorenje i neovlašten pristup u svojoj definiciji kibernetičkoga kriminaliteta. Vjerojatno najprimjerenija definicija kibernetičkoga kriminaliteta jest ta da je to bilo koji zločin koji je počinjen ili potpomognut računalom, internetskim mrežama ili drugim oblicima računalne opreme. Računalo ili uređaj može biti oruđe zločina. Zločin se može počiniti virtualno, s pomoću računala i na nevirtualnim lokacijama.

Gordon i Ford (2006) navode dva temeljna tipa kibernetičkoga kriminala. Tip 1 tehničke je prirode, a ima sljedeće karakteristike:

1. To je uglavnom rijedak ili diskretan događaj s gledišta žrtve.
2. Često ga se može počiniti tako da se u računalni sustav žrtve ubace zloćudni programi, primjerice programi koji pamte tipke koje korisnik pritisne (engl. *keystroke loggers*), virusi ili zlonamjerni programi koji mijenjaju sustavske podatke i objekte kako bi na taj način izbjegli detekciju (engl. *rootkit*) ili trojanski konji.
3. Takve se radnje mogu, ali i ne moraju olakšati s pomoću ranjivosti sustava.

Takva vrsta kibernetičkoga kriminaliteta zahtijeva zaštitu podataka od tradicionalnih prijetnji kao što su virusi ili crvi, no korisnik također treba biti svjestan pojma „ranjivosti".

Kibernetički kriminalitet tipa 2, koji se nalazi na drugom kraju spektra, više je ljudske prirode. On obuhvaća, ali nije ograničen na aktivnosti kao što su kibernetičko uhođenje i maltretiranje, pedofilno zlostavljanje, iznuđivanje, ucjena, burzovna manipulacija, kompleksna korporativna špijunaža, planiranje i provođenje terorističkih aktivnosti putem interneta. Karakteristike kibernetičkoga kriminaliteta tipa 2 su sljedeće:

1. Uglavnom je potpomognut programima koji se ne uklapaju u definiciju zloćudnih programa. Primjerice, pri razgovorima koji se odvijaju slanjem istodobnih poruka (engl. instant messaging) klijenti i datoteke mogu se prenositi s pomoću FTP protokola.
2. Korisnik uglavnom primjećuje ponovljene kontakte ili događaje.

Iako općenito prihvaćena definicija kibernetičkoga kriminaliteta ne postoji, jasno je da ta pojava poprima nove oblike i da se stalno širi. Kibernetički prijestupnici stalno osmišljaju nove alate, opremu i metode za postizanje svojih ciljeva. Jedna od njih obuhvaća prikupljanje podataka o potencijalnim žrtvama putem njihovih profila na društvenim mrežama. Prikupljeni podatci u drugom se koraku koriste s ciljem kriminalne aktivnosti ostvarene u stvarnom ili virtualnom svijetu.

S gledišta kibernetičkoga kriminaliteta mladi ljudi (djeca, adolescenti i studenti) predstavljaju osobito ranjivu skupinu korisnika interneta. Pristup raznim internetskim sadržajima i trenutno vrlo popularnim društvenim mrežama kao što su Facebook i Twitter mladim je ljudima moguć ne samo putem njihovih osobnih računala ili računalnih mreža već i putem pametnih mobilnih telefona. Brz bežični pristup internetu s pomoću navedenih uređaja korisnicima omogućava primanje i slanje elektroničke pošte i komunikaciju unutar društvenih mreža. Pristup društvenim mrežama, razmjena informacija, zatim primanje i slanje poruka, na taj su način poprimili višestruke dimenzije, uključujući prostor i vrijeme, čime se značajno umanjila mogućnost roditeljske kontrole.

Mladi su ljudi, bez sumnje, najčešći i najlakovjerniji korisnici društvenih mreža. Zbog nedostatka edukacije o opasnostima kojima su izloženi na društvenim mrežama, neiskusni korisnici na svojim profilima nesmotreno objavljuju informacije i multimedijske sadržaje koje mogu upotrijebiti korisnici interneta s drugačijim motivima. Osim što su izloženi riziku kršenja osobne privatnosti i zlouporabe osobnih podataka, mladi se ljudi izlažu mogućoj političkoj i ideološkoj manipulaciji.

Mladi ljudi i sigurnosni rizici internetskih stranica društvenih mreža

Informacije koje korisnici objavljuju na javnim stranicama društvenih mreža ostali korisnici interneta mogu zloupotrijebiti. Ti korisnici mogu biti kibernetički prijestupnici, mentalno bolesni ljudi, politički ili ideološki motivirane skupine i dr. Najmlađi korisnici, nesvjesni opasnosti, često na mreži objavljuju svoje kućne adrese, brojeve telefona, informacije o vremenu kad su njihovi roditelji na poslu (kad su sami kod kuće), vrijeme kad će biti na godišnjem odmoru, kao i ostale osjetljive informacije. Twitter je vrlo popularan među navedenom korisničkom populacijom, a čak im omogućava objavljivanje rasporeda svojih dnevnih aktivnosti – kad su djeca u školi, kamo idu poslije škole, gdje se trenutno nalaze i što rade i sl. Te se informacije mogu zloupotrijebiti pri planiranju i provedbi kriminalnih aktivnosti kao što su pljačka, otmica, tjelesno i psihološko zlostavljanje itd. Povreda osobne privatnosti može dovesti do povrede osobnog integriteta.

Informacije koje djeca objavljuju na svojim korisničkim profilima najčešće zloupotrebljavaju njihovi vršnjaci. Radi se o pojavi kibernetičkoga nasilja koje obuhvaća zadirkivanje, dodijavanje, a u težim slučajevima i maltretiranje u virtualnom svijetu. Kibernetičko je nasilje u stalnom porastu. Rezultati istraživanja provedenog u pet srednjih škola u Beogradu pokazuju da je 10% učenika u dobi između 11 i 15 godina bilo uključeno u takav tip aktivnosti usmjeren protiv drugih učenika. Istraživanje je također pokazalo da je 20% učenika bilo žrtvom takvih virtualnih poduhvata (Popović-Ćitić i dr., 2011, str. 412). Navedena vrsta nasilja može izazvati ozbiljne psihološke posljedice. O tome se naveliko raspravljalo u profesionalnoj literaturi nakon što je otkriven prvi slučaj virtualnog silovanja (Johnson, 2001).

Također su zabilježeni slučajevi u kojima nasilnici preuzimaju čak i virtualni identitet mete svojega napada, odnosno žrtve, s ciljem pojačanog učinka aktivnosti sustavnog uništavanja reputacije žrtve ili provođenja kriminalnih namjera.

Svaka je osoba osjetljiva na različite vrste otvorenih i prikrivenih napada koji za cilj imaju praktičnu šalu ili jasnu kriminalnu namjeru. Osjećaj povrede i gubitka osobnog prostora i privatnosti može imati dugoročan učinak na psihu osobe. Internetske stranice društvenih mreža opskrbljuju napadača mnogobrojnim informacijama o žrtvi koje napadaču omogućuju psihološku borbu. Kibernetička kleveta i digitalne aktivnosti sustavnog uništavanja reputacije žrtve mogu brzo doprijeti do nevjerojatno velikih brojeva ljudi i u isto vrijeme u žrtve izazvati golemu frustraciju i počiniti kolateralnu štetu. Žrtvi je iznimno teško povratiti izgubljeno povjerenje i dobru reputaciju usred virtualnog sustavnog uništavanja njezine reputacije. Mete napada stavljene su u poziciju da se brane, a ne znaju identitet napadača, njegove motive, lokaciju, ciljeve, niti je li napad počinjen od jedne osobe ili skupine. Mete najčešće ne znaju kome se obratiti za pomoć u takvim situacijama jer u većini država nije jasno koje se državno tijelo treba baviti takvim kažnjivim djelima.

Druga skupina rizika obuhvaća propagandu i integriranje kapaciteta društvenih mreža. Činjenica je da društvene mreže predstavljaju mjesto na kojemu se promoviraju zamisli i ideologije, iniciraju kampanje, motiviraju i okupljaju istomišljenici. Ta digitalna mjesta susreta omogućuju pojedincima i različitim, često marginaliziranim, skupinama razmjenjivanje ideja. Na društvenim se mrežama identitet skupine brzo formira i učvršćuje – usamljeni glasovi lako i brzo odjekuju. Vrlo je tanka granica između naizgled bezopasnog lobiranja i žučnog kritiziranja društvenih okolnosti i digitalne anarhije.

Prethodna istraživanja

Mediji imaju dugoročan i ponekad sustavan učinak na kulturološko i društveno formiranje i ponašanje zajednica, a mogu utjecati čak i na političke, ekonomske i sigurnosne okolnosti u nekoj državi. Potreba za analizom i objašnjenjem društvene, ekonomske i sigurnosne uloge i utjecaja masovnih medija na društvo, skupine i pojedince proizlazi iz svega što smo prethodno spomenuli (Boskovic i dr., 2012). Mnogi su autori usmjerili svoje intelektualne napore i istraživanja na analizu učinka medija na nasilno ponašanje korisnika, kako pojedinaca tako i društvenih skupina. Okosnica većine istraživana temelji se na spoznajama o procesima imitacije, društvenoga učenja i poistovjećivanja. Iako su često nedosljedna u metodološkim pristupima i praćena kritikama i hvalama drugih znanstvenika (Freedman, 1984; Cook i dr., 1983), mnoga laboratorijska i terenska istraživanja pokazuju veliko zanimanje znanstvenih i profesionalnih tijela za proučavanje medija i učinaka koje mediji imaju na korisnike. Neka istraživanja u tom području pokazuju da izloženost nasilju u medijima ima, u najmanju ruku, kratkoročne posljedice u smislu poticanja na agresivno ponašanje. Prema jednom tipu kognitivnoga pristupa kojim se koristi Berkowitz (1984), agresivni motivi i ideje iz nasilnih filmova mogu u gledatelja aktivirati agresivne misli. Kad se aktivira jedna takva misao, aktivirat će se i ostale slične misli (Felson, 1996). No, Bandura (1973) pretpostavlja da nasilne scene koje emitiraju mediji mogu izazvati agresivne misli i ponašanje u pojedinaca koji su predodređeni na takve emocije te mogu biti popraćene konkretnim reakcijama zbog psihološke strukture njihovih osobnosti. Banks (2005) je proveo studiju o utjecaju kriminala u medijima na nesigurnost u lokalnom kontekstu.

Internet, kao specifičan medij, i društvene mreže, kao jedan od suvremenih načina komunikacija, od samoga su početka smatrani jednim od mnogih tehnoloških fenomena. Taj tip društvenoga modela, koji iznad svega počiva na tehnologiji globalnih mreža, predmet je mnogih i raznovrsnih studija. Društvene se mreže proučavaju s gledišta telekomunikacija, tehničkih i računalnih disciplina, no također su predmetom raznih psiholoških, društveno-političkih, pedagoških studija i sigurnosnih studija.

Društvene mreže predstavljaju model virtualnog povezivanja i interakcije među ljudima ili skupinama ljudi različitih spolova, dobi, ideoloških, vjerskih i političkih uvjerenja te imaju ulogu portala za promociju komercijalnih proizvoda i usluga, razglašavanje zamisli o društvenim i političkim pokretima i prezentaciji osobnih vještina, iskustava i emocionalnih stanja. Kad se sve to uzme u obzir, društvene mreže predstavljaju moderan i atraktivan istraživački problem koji se proučava s raznih gledišta – društvenoga, političkoga, organizacijskoga i sigurnosnoga.

Rane studije su pokazale da su najaktivniji korisnici društvenih foruma bili zagovaratelji prava slobodne volje te su strastveno vjerovali u sposobnosti društvenih krugova i pojedinaca, prije nego država, za rješavanje problema današnjega društva (Katz, 1997, str. 68-82). Aktivističke skupine kao što su udruge za zaštitu prava životinja ili organizacije homoseksualaca, odlučne u stjecanju jednakih prava za svoje članove, koristile su se forumima kao jednim od svojih najranijih oružja i tako izražavali svoje stavove na jeftin i dalekosežan način. Strategija i taktika tu nisu bile važne. Njihov je cilj bio širenje ideja. Postoje slučajevi u kojima su društvene mreže koristile skupine aktivista koji su zagovarali zabranu pobačaja, eutanaziju i kloniranje. Oni su na neki način bili prethodnici buduće militarizacije društvenog i ideološkog aktivizma.

Utjecaj interneta i društvenih mreža na formiranje ili promjenu političkih, društvenih, ili ekonomskih okolnosti u državama bio je predmetom mnogih studija (Schmitt-Beck i Mackenrodt, 2010; Margetts i dr., 2011; Boskovic i Putnik, 2011). Posljednjih su godina društvene mreže poput Facebooka i Twittera postale neizbježno oruđe za okupljanje političkih aktivista, pa čak i za započinjanje revolucionarnih pokreta u nekim državama. Njihova uloga i važnost bile su osobito očite u, uvjetno rečeno, nedemokratskim državama ili u slučajevima ozbiljne društvene i pravne blokade u kojima su mediji poput radija i televizijskih stanica, tiskanih i internetskih novina kontrolirale vladajuće strukture (Boskovic i Putnik, 2011). S napretkom globalne računalne mreže i grafičkog korisničkog sučelja društveni i politički aktivisti stekli su više mogućnosti za uključivanje u rasprave u kojima su dokazivali svoje

„istine“, skupljali sredstva i regrutirali nove članove. Vjerski ili ideološki motivirane skupine kao što su vjerske sekte ili terorističke organizacije sad raspolažu sredstvima kojima mogu voditi elektroničke ratove.

Razmjena osobnih podataka na stranicama društvenih mreža i korištenje sustava za širenje ideoloških, vjerskih i političkih uvjerenja i poziva na aktivizam predstavlja izazov za strukture nacionalne sigurnosti u smislu zaštite nacionalne sigurnosti i postizanja osobne sigurnosti korisnika mreže, osobito onih maloljetnih. Sigurnosne probleme, zaštitu privatnosti i prava građana na društvenim mrežama istraživali su Asher i dr. (2009), Van Eecka i Truyens (2010).

U digitalnoj su okolini rizici od manipulacije i regrutiranja mladih ljudi od takvih organizacija postali vrlo očiti zbog smanjene mogućnosti roditelja ili nastavnika da kontroliraju ponašanje djece. Forkosh-Baruch i Hershkovitz (2012), zatim Popović-Ćitić i dr. (2011) proveli su istraživanja o utjecaju korištenja društvenih mreža na odgojno-obrazovne procese i ozračje odgojno-obrazovnih institucija. Bicen i Cavus (2011) istražili su navike učenika u smislu uporabe Facebook društvene mreže. Facebook je jedna od najvećih društvenih mreža s obzirom na broj korisnika pa je stoga predmetom mnogih istraživanja (Ross i dr., 2009; Buckman, 2005).

Motivacijski čimbenici i učestalost uporabe stranica društvenih mreža u srednjoškolskih učenika

Istraživanja internetskih društvenih mreža u posljednje su vrijeme postala sve razvijenija. Istraživanja su potvrdila postojanje tri dimenzije uporabe tih mreža: informativne, prijateljske i povezujuće (Raacke i Bonds-Raacke, 2010). Otkrivena su četiri temeljna razloga za pristupanje Facebook skupinama: socijalizacija, zabava, potraga za vlastitim statusom i potraga za informacijama (Park i dr., 2009).

Nacionalna istraživanja o društvenoj uporabi Facebooka među srednjoškolcima utvrdila su postojanje triju faktora: F-virtualno, F-socijalizacija i F-prijatelji (Kordić & Babić, 2011). Faktor F-prijatelji odnosi se na korištenje Facebookom koje dodaje i obogaćuje socijalizaciju sa stvarnim prijateljima i poznanicima. Faktor F-socijalizacija odnosi se na korištenje Facebookom koje zadovoljava potrebu za socijalizacijom, zabavom, podizanjem raspoloženja i olakšavanjem životnih nedaća. Razlika između tih dvaju faktora jest u tome što se prvi odnosi na instrumentalnu uporabu, a drugi na kompenzacijsko korištenje Facebookom. Faktor F-virtualno odnosi se na određene čimbenike korištenja Facebooka kao što su intenzivnija socijalizacija i bolja zabava s internetskim prijateljima, veći osjećaj prihvaćenosti u virtualnom svijetu i zanemarivanje svakodnevnih odgovornosti i sastanaka. Više vrijednosti toga faktora reflektiraju kompenzacijsko korištenje Facebookom, a niže vrijednosti reflektiraju instrumentalno korištenje Facebookom.

Spomenuta nacionalna studija o društvenoj uporabi Facebooka (Kordić & Babić, 2011) pojašnjava da se Facebook primarno koristi kao ekstenzija i podrška stvarnih društvenih života korisnika. Samo manja skupina srednjoškolaca preferira druženje putem Facebooka od uobičajenih načina druženja. Porast u popularnosti Facebooka u Beogradu podudara se s porastom njegove popularnosti u SAD-u. Broj korisnika Facebooka porastao je s 22% u 2008. godini na 78% u 2009. godini (Lenhart i dr., 2010). Prema podatcima iz 2009. većina beogradskih srednjoškolaca (73,33%) koristila se Facebookom barem jednom dnevno (Kordić & Babić, 2011) te je na Facebooku provodila do dva sata dnevno. Podatci o američkim tinejdžerima iz 2009. pokazali su da ih se 48% koristilo Facebookom jednom dnevno (Lenhart, 2009).

Evaluacija rizika od korištenja internetskim društvenim mrežama u srednjoškolaca

Prethodno smo naveli činjenicu da su mladi koji se koriste društvenim mrežama izloženi rizicima od kršenja osobne privatnosti, zlouporabe privatnih informacija i političke ili ideološke manipulacije. Svi spomenuti rizici, ako se ostvare, mogu dovesti do povrede psihološkoga integriteta osobe.

Sa stajališta procjene sigurnosnih rizika važna je veličina internetske društvene mreže i broj nepoznatih „prijatelja“ koje je korisnik prihvatio. Prema podatcima iz 2010. prosječan korisnik Facebooka imao je 130 prijatelja na Facebooku (Hepburn, 2010). Uzorak beogradskih srednjoškolaca sadržavao je 84% korisnika s više od 100 prijatelja na Facebooku. Sigurnosni rizici predstavljeni su s pomoću broja nepoznatih prijatelja na Facebooku, s obzirom na to da je 38% beogradskih srednjoškolaca imalo više od 50 nepoznatih prijatelja (Kordić i Babić, 2011).

Strane su studije potvrdile značajnu korelaciju između dobrog imovinskog stanja, učestalosti posjećivanja tih stranica i informacija koje dobivaju drugi korisnici tih stranica (Valkenburg i dr., 2006), kao i veće koristi koju imaju korisnici niskog samopouzdanja i zadovoljstva životom (Ellison i dr., 2007). Na temelju domaćeg istraživanja o korištenju Facebooka i socijaliziranja beogradskih srednjoškolaca, utvrđene su sljedeće četiri tipične skupine mladih (Kordić & Babić, 2011): 1. skupina mladih (38%) koji rijetko koriste Facebook i rijetko se kreću u društvu (Stidljivi), 2. skupina mladih (16%) usredotočenih na druženje na sportskim aktivnostima sa svojim susjedima (Atleti), 3. skupina mladih (12%) koji se druže na Facebooku i u školi (Virtualni) i 4. skupina mladih (34%) koji kontaktiraju sa svojim susjedima u stvarnom životu i na Facebooku (Prijateljski).

Evaluacija rizika korištenja internetskih društvenih mreža u srednjoškolaca provedena je potkraj 2011. godine (Kordić & Putnik, 2011). Ova studija zamišljena je s društveno-psihološkoga gledišta, a zaključci su joj sljedeći:

Manji broj mladih u uzorku beogradskih srednjoškolaca osobito je privržen Facebooku (12%) te se njime koristi pretežno u kompenzacijske svrhe jer Facebook zadovoljava puno temeljnih društvenih potreba na virtualan način (Kordić & Babić, 2011). Korisnicima se čini da Facebook podiže njihovo raspoloženje, pomaže im kako bi stekli nove prijatelje, stvara u njih osjećaj pripadanja i podrške kad im se život čini teškim. To je skupina srednjoškolaca koji se koriste Facebookom za poticanje samopouzdanja i popularnosti među vršnjacima (Christofides i dr., 2009). Takva je skupina mladih rizična jer je njome lako manipulirati osobito zbog toga što je njihov osobni integritet slabiji od integriteta prosječne populacije mladih. U odnosu na vrste sigurnosnih rizika, ta je skupina ranjivija i podložnija svim tipovima sigurnosnih rizika, iako je veći rizik u kršenju osobne privatnosti i zlouporabe privatnih informacija, jer to može uzrokovati osobnu propast korisnika.

Značajan broj beogradskih srednjoškolaca druži se sa stvarnim i Facebook prijateljima. Ta je skupina također rizična, ali na drugačiji način od onoga koji smo prethodno opisali. Oni se koriste Facebookom na instrumentalniji način te se tako povećava mogućnost političke (ideološke) manipulacije jer su članovi te skupine ranjivi na pritisak skupine s obzirom na njihovu potrebu da zadrže identitet skupine.

Treću skupinu s obzirom na čimbenik rizika čini skupina „stidljivih“ učenika. Vjerojatnost materijalizacije rizika značajno je niža zbog manje učestalog korištenja internetskim društvenim mrežama. Međutim, ostaje nejasno što su to društveno-psihološke karakteristike „stidljive“ skupine s obzirom na visok stupanj socijalizacije koji se očekuje u srednjoškolaca. Ako se radi o društveno-psihološki ranjivoj skupini, čak i ograničena uporaba društvenih mreža može predstavljati rizik od kibernetičkih prijetnji.

Najmanje rizična skupina je skupina atleta zbog njihova aktivnoga načina života, jasnog društvenog identiteta i ograničene instrumentalne uporabe internetskih društvenih mreža.

Opći zaključak prethodno spomenute studije eksplicitno ističe očito pomanjkanje edukacije srpskih srednjoškolaca o sigurnoj uporabi navedenih resursa te navodi da bi promoviranje sigurnosne kulture i internetskoga ponašanja povećalo razinu sigurnosti članova virtualnih zajednica, među kojima su mladi najranjiviji.

Procjena učinka medija na svijest učenika o rizicima korištenja internetskih društvenih mreža

Zaključak prethodno spomenute studije odnosi se na populaciju srednjoškolaca. Naša je namjera bila testirati istu hipotezu na studentskoj populaciji u zasebnoj studiji. Cilj je bio istražiti percepciju prijetnji i sigurnosnih rizika povezanih s korištenjem društvenih mreža u studenata. Također smo htjeli prikupiti informacije o tome kako su naučili osnovne činjenice o navedenim rizicima.

Metode

U ovome je radu upotrijebljena deskriptivna istraživačka metodologija s neeksperimentalnim fiksnim dizajnom i kvantitativno anketno istraživanje. Metodologija deskriptivnog istraživanja upotrijebljena je u kombinaciji s neeksperimentalnim fiksnim dizajnom jer su prednosti rada s postojećim činjenicama neometanje detalja koji su od istraživačkoga interesa (Robson, 2002). Neeksperimentalni fiksni dizajn može se definirati kao sustavno istraživanje u kojemu istraživač nema izravnu kontrolu nad nezavisnim varijablama jer su se one već manifestirale (Kerlinger, 1986). U fiksni istraživački dizajn uglavnom se uključuje neovisni istraživač kako bi se spriječio utjecaj glavnog istraživača na rezultate istraživanja (Robson, 2002).

Ova je studija kvantitativna jer se odgovaralo na pitanja o odnosima među mjerenim varijablama s ciljem objašnjavanja, predviđanja i kontroliranja pojavnosti (Leedy i Ormrod, 2005). Za samoizvještavanje ili anketno istraživanje upotrijebljeno u ovome radu bio je potreban upitnik, odnosno skupina pitanja na koje je odgovorila odabrana skupina ispitanika (Gay, Mills, i Airasian, 2006). Anketno istraživanje obuhvaća prikupljanje informacija o jednoj ili više skupina ljudi tako što ispitanici odgovaraju na pitanja postavljena u upitniku, nakon čega se njihovi odgovori tabeliraju s pomoću statističkih indeksa kako bi se izveli zaključci o pojedinoj populaciji (Leedy i Ormrod, 2005).

Ispitanici

U studiji su istraženi stavovi 100 studenata završne godine Fakulteta sigurnosnih studija Sveučilišta u Beogradu i 50 maturanata koji su prethodno aplicirali na spomenuti fakultet. Istraživanje je provedeno u razdoblju od travnja do svibnja 2012.

Korišten je uzorak s namjernim odabirom jer je istraživač želio proučiti stavove ispitanika i pri tome je na umu imao određenu svrhu. Uzorak s namjernim odabirom proces je odabira uzorka za koji se smatra da je reprezentativan za danu populaciju, a istraživač utvrđuje kriterije za odabir uzorka (Gay i dr., 2006). Istražene su obje skupine ispitanika jer ovo nije bilo istraživanje velikih razmjera. Primijenili smo naše iskustvo i stručnost sveučilišnih nastavnika u odabiru uzorka i proučavanju stavova ispitanika. Moglo bi se pomisliti da uzorak nije reprezentativan jer je istraživanje provedeno samo među ispitanicima jednog fakulteta, no to nije slučaj. Fakultet sigurnosnih studija Sveučilišta u Beogradu u Srbiji sa svojim kurikulom iz polja sigurnosnih studija jedinstvena je državna institucija u Republici Srbiji. To je jedna od rijetkih obrazovnih institucija čiji kurikul osigurava obrazovanje studenata u polju kibernetičkog kriminaliteta. Imajući na umu sadržaj kurikula sigurnosnih studija i činjenicu da fakultet obrazuje buduće diplomante s diplomama iz sigurnosnih studija, pretpostavili smo da će studenti završne godine studija imati jasniju svijest o prijetnjama koje predstavlja kibernetički kriminalitet od njihovih kolega s drugih fakulteta. Upravo zbog tih smo razloga željeli provesti istraživanje s ciljem procjene razine utjecaja medija, posebnoga obrazovanja i društvenoga okruženja na percepciju sigurnosnih rizika u navedenome uzorku studenata. Zatražili smo pristanak Sveučilišta u Beogradu – Fakulteta sigurnosnih studija za provođenje istraživanja prije nego što smo upitnik podijelili ispitanicima.

Instrument

Instrument upotrijebljen u istraživanju razvili su autori ovoga rada. Sudjelovanje je bilo dobrovoljno i anonimno. Upitnik je sadržavao 4 pitanja zatvorenoga tipa. Ispitanici su odabrali jednu od ponuđenih opcija. Svi su ispitanici odgovorili na dva od četiri ponuđena pitanja. Ta su dva pitanja bila zatvorenoga tipa, odnosno ponuđeni su bili odgovori DA i NE. Odgovori na preostala dva pitanja uvjetovani su odgovorima koje su ispitanici dali na pitanja zatvorenoga tipa. Opcije ponuđene za dva opcionalna pitanja predstavljene su u sekciji u kojoj su analizirani rezultati istraživanja.

Upitnik je sadržavao sljedeća pitanja:

1. „IMATE LI VLASTITI *PROFIL* NA NEKOJ STRANICI ZA DRUŠTVENO UMREŽAVANJE?"; to je pitanje bilo temeljno pitanje i pitanje zatvorenoga tipa.
2. „PRIMARNA SVRHA KORIŠTENJA STRANICA ZA DRUŠTVENO UMREŽAVANJE"; na ovo su pitanje odgovarali ispitanici koji su na prvo pitanje odgovorili s DA.
3. „MISLITE LI DA INTERNETSKE STRANICE ZA DRUŠTVENO UMREŽAVANJE MOGU ZNAČAJNO UGROZITI TJELESNI, MORALNI ILI PSIHOLOŠKI INTEGRITET OSOBE?"; ovo je pitanje bilo temeljno pitanje i pitanje zatvorenoga tipa.
4. „KAKO I IZ KOJIH IZVORA STE SE VEĆINOM INFORMIRALI O RAZLIČITIM RIZICIMA I OPASNOSTIMA UPORABE INTERNETA, KORISNIČKIH RAČUNA ELEKTORNIČKE POŠTE ILI STRANICA ZA DRUŠTVENO UMREŽAVANJE?"; na ovo su pitanje odgovarali ispitanici koji su na treće pitanje odgovorili DA.

Analiza

Za analizu odgovora ispitanika upotrijebljena je statistička metoda, a rezultati su izraženi kao brojčane vrijednosti i postotci. U ovome su radu karakteristični rezultati prikazani grafovima.

Rezultati i rasprava

Anketna su pitanja postavljena kako bi se utvrdilo koriste li se studenti i maturanti internetom, društvenim mrežama i ostalim globalnim mrežnim aplikacijama, kao i koje prednosti i rizike podrazumijevaju ti moderni mediji. 79 studenata i 35 maturanata izradilo je profile na nekoj društvenoj mreži. Većina ispitanika koji imaju profile (61 student i 30 srednjoškolaca) njima se koristi za virtualne kontakte i povezivanje više nego za promoviranje svojega znanja i vještina ili uspostavljanje kontakata u stvarnome svijetu. Pronašli smo gotovo jednak broj „Da" (56 studenata) i „Ne" (44 studenta) odgovora na pitanje „Mislite li da internetske stranice za društveno umrežavanje mogu značajno ugroziti tjelesni, moralni ili psihološki integritet osobe?" Na isto je pitanje 39 maturanata odgovorilo s „Da", a 11 s „Ne". Oni koji su na prethodno pitanje odgovorili pozitivno, trebali su odgovoriti na dodatno pitanje „Kako ste se informirali o opasnostima uporabe interneta, elektorničke pošte i društvenih mreža?" Mogući odgovori na to pitanje bili su: „razgovor s obitelji" (A), „u srednjoj školi" (B), „na fakultetu"– samo za studente (C), „iz osobnog iskustva i učenja" (D), „iz medija – vijesti, dokumentarnih i zabavnih programa" (E). Najčešći su odgovori bili: (D) – 24 studenta i 9 maturanata i (E) – 32 studenta i 30 maturanata.

Studenti i maturanti su također upitani o modernim vrstama medija kao što su internet i društvene mreže. Ispitanici su upitani imaju li takozvani profil na nekoj društvenoj mreži, na što je 79% studenata i 70% maturanata odgovorilo s „Da“. Većina njih koristi se svojim profilom za virtualnu socijalizaciju. Bez obzira na to imaju li ili nemaju profile, 56% studenata i 78% srednjoškolaca vjeruje da društvene mreže mogu kompromitirati tjelesni, moralni ili psihološki integritet osobe. Ti su podatci prikazani na slici 1.

Slika 1.

Većina studenata (njih 57%) saznali su o potencijalnim rizicima korištenja interneta i društvenih mreža iz medija, a 42,8% njih je o tim rizicima saznalo iz osobnog iskustva. Na isto su pitanje odgovorili i srednjoškolci; njih 76,9% saznalo je o spomenutim opasnostima iz medija, a njih 23% iz osobnog iskustva. Ti su rezultati prikazani na slici 2.

Slika 2.

Odgovori na posljednja dva pitanja pokazuju da studenti i maturanti imaju zadovoljavajuće znanje i potrebne vještine za korištenje globalnom mrežom i povezanim proizvodima, no i da su svjesni potencijalnih opasnosti i rizika tih modernih medija.

Zaključak

Društvene mreže nužan su oblik bežične globalne komunikacije i istodobno predstavljaju jasnu potrebu modernoga društva. Kao i svako drugo postignuće, društvene mreže imaju za cilj učiniti svakodnevni život lakšim, kreativnijim i zanimljivijim. No, inovacije imaju svoje rizike i sigurnosne izazove. Danas Facebook i Twitter imaju desetke milijuna korisnika različitih dobi i interesa, ali i različitih motiva korištenja. Priroda nekih motiva je kriminal. S obzirom na to i imajući u vidu podatke o zlouporabi profita društvenih mreža, otežana je sigurnosna prevencija u odnosu na rizik. Stalna edukacija o sigurnom korištenju interneta i komunikacijskih portala opravdana je, potrebna i ima važnu ulogu u razvoju opće sigurnosne kulture.

Rezultati istraživanja pokazali su da je više od polovine studenata sigurnosnih studija i maturanata postiglo zadovoljavajući stupanj sigurnosne kulture s obzirom na korištenje društvenih mreža te da su znanje o rizicima i mjerama zaštite stekli uglavnom putem medija. Ispitanici-maturanti stekli su znanje o informatici i računalnim sustavima tijekom srednjoškolskog obrazovanja. Studenti-ispitanici bili su pri kraju četverogodišnjeg visokog obrazovanja iz sigurnosnih studija koje obuhvaća moderne rizike kao što je kibernetički kriminal. U svojim su odgovorima obje skupine ispitanika demonstrirale osobnu inicijativu i želju za samoobrazovanjem.

Međutim, usprkos svemu navedenome, rezultati istraživanja pokazuju da suvremeni mediji učinkovito utječu na stjecanje različitih vrsta znanja i kreiranje stavova. U ovome slučaju su mediji imali daleko veći učinak od obrazovanja i društvenoga okruženja na razvoj svijesti ispitanika o postojanju kibernetičkoga kriminala i sigurnosnim rizicima povezanim s korištenjem društvenih mreža. Takvi rezultati pokazuju da obrazovni programi, a osobito oni koji se odnose na sigurnosne studije, trebaju praktično poboljšanje obrazovnih procesa. Potrebno je učiniti prijenos znanja i poruka barem jednako izazovnim i zanimljivim, na način na koji to vrlo specifično rade mediji. U odnosu na obrazovne zadatke više pažnje treba posvetiti modernim sigurnosnim izazovima kao što su rizici povezani s korištenjem društvenih mreža, kibernetički kriminalitet i slične aktivnosti na globalnoj mreži. Mediji imaju važno mjesto u modernome svijetu i jasnu ulogu u kreiranju političke, kulturološke i sigurnosne svijesti ljudi, no edukacija mora biti usmjeren proces i adekvatan primaran izvor znanja i vještina potrebnih za društveni život u zajednicama.