THREATS AND THE PROTECTION OF ELECTRONIC INFORMATION WITH REGARD TO SOCIAL NETWORKS

Matija Varga, mag. inf. univ. spec. oec. Media University, Croatia
maavarga@gmail.com

Red. prof. dr. sc. Vladimir Šimović Media University, Croatia
simovic.vladimir@yahoo.com

Doc. dr. sc. Marin Milković Media University, Croatia
dekan@velv.hr

ABSTRACT

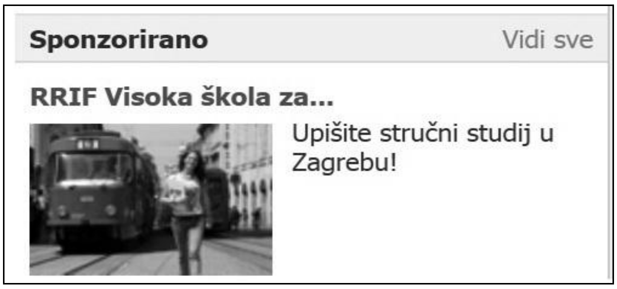
The issues which appear today on electronic social networks and which are trying to be solved are as follows: (1) suppressing the addiction to e-social networking and "online" games on electronic social networks; (2) reducing the number of identity thefts for the participants in e-social networks; and the issue of (3) protecting the electronic information. Addiction to e-social networking among young people exists, while a lot of older people are becoming addicted to electronic social networks. Based on the domestic and foreign research results and their analysis, the paper proves that the addiction to e-social networks exists. The paper presents ways of fighting the addiction to e-social networking. One way of dealing with addiction to the Internet and "online" games on e-social networks, which is described in detail, is setting up parental controls in the operating system (used by addicts) by IT professionals. Today, besides this method of protection from addiction to e-social networks, a number of interesting protection activities, projects and lectures are to be implemented. When it comes to protecting user accounts on e-social networks, users should frequently change their password, and set a strong password. To prevent attempts of an attack on the user through computers, the systems for managing local computer network and the control of electronic information flow are implemented; thus the flow of e-information of social networks users is controlled, which is also described in detail in this paper. In the conclusion, recommendations are made and explanations are given whether to use or not to use e-social networks, considering all the negativity.

Keywords: addiction to e-social networks, attempts of preventing an attack, control of the information flow, e-information protection, internet.

INTRODUCTION

The first part of the paper presents explanations and commentaries of the conducted research results on people addicted to e-social networks, the e-social networks users' abuse, and other threats on e-social networks.

The second part shows the possibilities and ways to protect e-social networks users and to protect electronic information. Nowadays, the Internet and e-social networks are necessary for self-promotion of users, the promotion of products, services, many faculties and their programs, and other organizations.



Sponzorirano Vidi sve

RRIF Visoka škola za...

Upišite stručni studij u Zagrebu!

Figure 1. *Using e-social network for the promotion of University College in the Republic of Croatia*
Source: Facebook. Retrieved on 26th April 2012 from http://www.facebook.com/profile.php?id=1139563573.

Figure 1 presents the promotion of University College RRIF, i.e. a sponsored ad. It is not hard to see why organization for tertiary education use the possibility of such promotions via e-social networking. One of the reasons is the number of users of e-social networks, especially high school students. Today, there is almost no high school student who is not a user of at least one social network. The Internet and e-social networks are an important resource for all users and activities, as well as for their e-learning process. It is necessary to pay great attention to computer security and computer security mechanisms, to the protection of the Internet and e-social networks users, and to the protection of electronic data about all the Internet and e-social networks users. The same way in which young people must be protected, it is necessary to protect elderly people (the Internet and e-social network users), especially teachers who are also exposed to dangers on the Internet and e-social networks. All users need to be guided when using the Internet and e-social networks towards benefits provided by broadband networks. On the Internet, as a new medium, and on e-social networks not everything is negative; there are positive and useful sides of the Internet and e-social networks.

The aim of this paper is to protect the users of e-social networks from threats, addiction, and the possibilities of abuse that they are threatened with on the Internet as the most popular youth medium and e-social networks by making recommendations and methods of protecting electronic information.

Paper Tasks

The paper tasks set on the topic of "Threats and the protection of electronic information on social networks" are as follows: (1) point to possible dangers and threats for the users of e-social networks that exist on the Internet; (2) to show the possibilities of protecting electronic information on e-social networks, to give advice on how to use a particular e-social network, to influence the users of the Internet and e-social networks in order to reduce false presentation on the Internet, and fighting addiction, to describe the combination of characters that comprise an optimum or a strong password. This paper seeks to influence the users of e-social networks by providing rules of conduct that should be respected; to warn the users of the Internet and e-social networks that information once published on the Internet and e-social networks remains on the Internet in most cases forever, (and that they are difficult to "remove" because there are web archives which memorize this information permanently, and that there is a possibility that the information in electronic form and e-documents remain on servers which are no longer parts of the Internet and are owned by the owner of a certain e-social network); to warn users of e-social networks to be cautious when sending data via chat, which is part of e-social networks, because the other party may present a false name; to make recommendations on the ways of dealing with violations of the rights of the users of the Internet and e-social networks; to alert users to the problem that the addiction to e-social networks and online internet games that are part of e-social networks presents; to display systems for monitoring and controlling the flow of data on the Internet (local networks); to display the privacy settings of certain e-social networks; and to mention how to set parental controls in operating systems to ensure the safety of users.

Research methods used

For the paper entitled "Threats and the Protection of Electronic Information on Social Networks" the following research methods were used: (1) direct observation method; (2) observation method (description of the current state of Internet users is given based on the experiences of the authors); (3) analysis, i.e. the method of content analysis; (4) survey (which extends the already conducted survey with new data collected from the Internet and e-social networks users); and (5) analysis of the results obtained from the survey that was additionally conducted from 20 eApril 2012 to 27 April 2012, in an elementary school (subject teaching) and in high school (in four-year courses).

THE INTERNET AND E-SOCIAL NETWORKS AS A MANIPULATION MEDIUM

The Internet is a global information communication system that connects computer networks of individual countries and organizations, and enables the computer owners, who are also users of the Internet and e-social networks around the world, to communicate with each other, to exchange information and to use many other services through their local and telephone networks (Dragičević, 2004, p. 28). Today, the Internet is a broad term, and there are its many definitions. The Internet is an uncontrolled medium, through which electronic information can be exchanged at high speed. By using the Internet and e-social networks certain information in a digital form is shared faster than via television or radio media. The Internet is a broadband widespread network which connects computers, regardless of their size or group they belong to, and which are connected to the Internet. The Internet can be touched easily if it is observed from the physical level.

The young people's opinion today is focused on playing entertaining games which can be found on the Internet in larger numbers than the educational ones. Older Internet users are also prone to games of chance, online betting and gambling. Based on experience, we can say that the students of vocational schools gamble more. The youth should be guided towards playing educational games, while the elderly users should be directed to use the Internet for useful purposes and gathering of electronic information that can be used for business purposes. Besides entertainment, the Internet is useful for more serious things. It allows finding an address or phone number of the person you wish to contact; buying and selling of personal items; listening to music; watching videos; journey planning; booking and payment of airline tickets; sending and receiving electronic mail using webmail or emails; e-learning; correspondence with other Internet users via web servers and e-social networks that have an IRC service; following the latest news; research; buying and selling securities, and tracking the shares value; distance learning; gathering data on historical figures; translating texts from foreign languages into a language understandable to the user; finding a specific location using geographic information systems; controlling the consumption of services using the Internet service providers; chatting with and watching a person far away; downloading files; publishing your photos and expressing your opinion via the web site; uploading web pages; CMS and LMS management; downloading free antivirus software. All of the aforementioned features are also the advantages of the Internet. Nowadays, the Internet as a medium can be used to influence public opinion and the opinion of a certain population. In the Republic of Croatia, the Internet as a medium has a very strong influence on the opinion of an average citizen. Numerous organizations as well as individuals now use the Internet and e-social networks as a tool to manipulate the public. It is known that numerous protests are organized through e-social networks, not only in the Republic of Croatia but also in other foreign countries.

Internet structure and the access possibilities

On the Internet, mail servers, web servers, FTP servers, local computers, desktop computers, laptop computers, mobile devices such as tablets and smart phones, and network components such as DSL modems, cable modems, routers and switches can be connected.

Connecting to the Internet is enabled by the ISP (internet service provider). The company, which is the ISP, gives its customers a device for the Internet access, i.e. router, and a username and password that the user can later change. Nowadays, access devices, such as cable modems and ADSL routers, and more rarely modems and ISDN adapters, are used for the Internet access. To access the Internet and e-social networks, three basic types of connection can be used: Dial-Up Connection, Subscribed Connection, and Shared Connection (Engst i Fleishman, 2004).

The Internet connects a growing number of nontraditional end systems such as TV sets, devices in cars, picture frames, household electronic and security systems, web cameras, refrigerators and microwave ovens (Kurose and Ross, 2005, p.2). Nowadays, access to the Internet and e-social networks is not a problem. Besides accessing the Internet from home, we can use it at work, in internet cafés, trams and even taxis.

Newer Internet services

In addition to the basic types of Internet services, such as WWW (World Wide Web), electronic mail, FTP (File Transfer Protocol), Telnet, IRC (Internet Relay Chat), there are tools for e-learning and e-social networks that could largely serve to promote products, services, organizations, faculties, and other educational organizations by using multimedia elements such as text, audio, video, graphics. Nowadays, most Internet users think that the World Wide Web is the Internet, but WWW is only one service on the Internet (global network). www is subdomain usually used to access web sites but it is not service mark. We can say that prefix http in web address represents certain service mark because it signals that we will use HyperText Transfer Protocol which is mostly used for loading of web pages.

PROBLEMS OF E-SOCIAL NETWORKS

E-social networks sometimes cause numerous problems to users and participants. Some users put too much personal information in electronic form in their profile on e-social networks. Malicious people can exploit posted electronic information. Employers can also use this information. Often some e-social network users publish the date when they go on holiday (e.g. I'll be at the seaside next week), which can be used by the burglars in the neighborhood. The problem of e-social networks is hacking Facebook profiles and mail systems and identity theft committed by malicious people. Pedophiles and murderers can also use the e-social networks information.

People addicted to the Internet and e-social networks and the causes of addiction

Everything that causes pleasure during consummation, and suffering because of its lack, we can call addiction. The causes of addiction are often derived from personal and social crisis, the lack of confidence, the need for conformity, boredom, affluence, or idleness (Pezo, 2011). Nowadays, almost all generations almost cannot function normally without the Internet technology. One of the serious dangers of the Internet and e-social networks which threatens all the generations is addiction to the Internet and e-social networks. Addiction to the Internet and e-social networks makes part of contemporary addictions. Addiction is today a major problem for users of e-social networks.

Who can be included in the group of the Internet and e-social networks addicts? All-day users of the Internet or e-social networks (communication with the purpose of solving problems) who are in some ways forced to work using the Internet are not at the same time addicted to the Internet. Addicts to e-social networks like “Facebook” do exist. Time passes by quickly while the addict is searching, viewing profiles, photographs and textual content on the profiles of their acquaintances, friends and famous people from private and public life. There is no end to checking the profiles of “Facebook” users. Each friend has friends whose personal profile contents can be viewed. There is the question: “Can we see a daily or frequent use of the Internet and e-social networks as the Internet addiction”? Today, the Internet is so powerful a medium; without it the business world, economy, banking, education, police, health, and other private and public sectors, including politics and political parties cannot function. People are forced to use the Internet as a medium in certain situations. Those users who due to certain life needs have to work longer hours on the Internet cannot be considered addicts. A group of Internet addicts may include: addicted to electronic mail; the users who are constantly reviewing “Facebook” profiles of other people interesting to them; the users who frequently watch some videos and video clips on “YouTube”; the users of online games which are not educational; the Internet users who frequently view pornography; the addicts to sexual discussions on the Internet; the users of chat services, who would correspond day after day; people who become frustrated if they cannot connect to the Internet for entertainment; the users of “online” gambling, betting and auction bidding; the users of information about other people; the viewers of movies on various online services; the customers who purchase through e-commerce; the participants in online card games; the addicted to downloading songs; the addicted to blogs, forums, etc. The most common causes of addiction to the Internet and e-social networks and online gaming on e-social networks among young people are as follows: (1) poor parental supervision; (2) not responding to viewing inappropriate content by Internet users; (3) passive environment; (4)

online games industry; (5) reluctance of teachers to respond promptly to fight the addiction; (6) not developing critical literacy among students when it comes to the media which manipulate children at schools.

Based on the research of the addiction to the Internet by using the "survey" method, a number of researchers have come to the conclusion that there are people addicted to the Internet and e-social networks based on established criteria.

A research in a neighboring country Slovenia, which was carried out in mid 2002 on the sample of 1194 participants *(N = 1194)* tells of the appearance and the slight increase of the number of addicts to computers and the Internet among young people in high schools. Already at that time, the author came to conclusion that the Internet offers many different options, i.e. services which reduce or make it difficult to control the time spent on the Internet. The author states that the Internet provides an opportunity to ease loneliness, rejection and social pressure (Jeriček, 2011). Studies on the addiction to the Internet and e-social networks have been conducted more frequently in the past fifteen years and even more in some countries. Andre Hanh and Matthias Jerusalem from the Humboldt University of Berlin, conducted a research on the Internet addicts based on a sample of 8,266 participants, of which 7,091 were from the Federal Republic of Germany. The study says that 3.2% of participants formally meet the criteria of the Internet addiction. The group which meets the criterion of addiction spent 34.6 hours a week on the Internet (thus 5 hours a day on average). The next group of Internet users, which is also risky, spends 28.6 hours a week on the Internet (thus 4.09 hours per day on average). Invisible web users use the Internet only 7.6 hours a week (www.onlinesucht.de/internetsucht_preprint.pdf, 2011). Three point two percent (3.2%) of the participants who are addicted (of total) is not much, especially in case of employees who work with Internet technologies within the company. If the aforementioned 3.2% of participants spend 5 hours a day on the Internet after working hours, it may present a significant problem for a person. Such a user necessarily requires abstinence.

Table 1. Addiction of the Internet users to services, in percentages

Internet addiction:				
Addiction to:	**Unnoticeable addiction**	**Potential addiction**	**Addiction**	**Total:**
correspondence	17.8%	26.6%	**35.1%**	79.50%
music	11.7%	14.9%	**14.7%**	41.30%
games, betting	5.4%	7.8%	**11.1%**	24.30%
pornography	6.9%	12.5%	**9.8%**	29.20%
other	21.4%	11.2%	**7.1%**	39.70%
online databases	16.6%	8.5%	**5.2%**	30.30%
online stores	5.6%	4.1%	**3.3%**	13.00%
communication systems	5.7%	4.4%	**3.2%**	13.30%
video-live streaming	2.7%	2.9%	**3%**	8.60%
online auctions	2.4%	2.3%	**2.9%**	7.60%
chat for adults	1.2%	2.6%	**2.8%**	6.60%

Internet addiction:				
Addiction to:	**Unnoticeable addiction**	**Potential addiction**	**Addiction**	**Total:**
Exchange	2.5%	1.8%	**1.7%**	6.00%
gambling with real money	0.1%	0.4%	**0.1%**	0.60%

Based on Table 1 (www.onlinesucht.de/internetsucht_preprint.pdf , 2011) shown by authors André Hahn and Matthias Jerusalem in their paper entitled "Internetsucht: Jugendliche gefangen im Netz", it can be seen that the Internet addiction can be divided into (1) invisible addiction; (2) potential addiction; and (3) addiction. When it comes to 'pure' addiction, on the basis of Table 1 it can be concluded that the Internet users are most addicted to: correspondence enabled by chat service (35.1%); music (14.7%); games and betting (11.1%); and pornography (9.8%). Thirty-four percent (34%) of the total number of surveyed people aged 15-29 years consider themselves addicted to the Internet. Internet users were classified as addicts (as stated in the study) because they spend more than 48 hours per week on the Internet, while being at risk the most are people who spend 10 hours a day on the Internet (Miliša and Tolić, 2011). Spending 10 hours a day on the Internet is too much so it can damage the users' health. Today, on the basis of short informative surveys that are not representative in most cases, it can be concluded that there is a certain number of Internet addicts. According to some estimates, it is stated that in Croatia in 2009 there were about 130,000 addicts to the Internet, aged between 20 and 30. As stated in the review article "The crisis of education and the expansion of modern addictions" („Kriza odgoja i ekspanzija suvremenih ovisnosti"), no one here has systematically dealt with such a problem in a multidisciplinary way (Miliša and Tolić, 2011). This certainly is not good. Practice in western countries is a little different, and experts deal with this kind of problems with the Internet users.

Computer addiction can cause numerous physical, psychological and social problems that need to be taken seriously not only for the young, but also for all generations. Addicted to the Internet and e-social networks often have problems with sleeping at night, disregarding obligations which are placed before them, with learning, and poor grades (the young), with weight, loss of will and motivation for other activities and hobbies. Nowadays, more and more young people learn and write seminar papers by using "copy-paste". Using such a method, young people sometimes do not read the contents and information of each web page on a certain topic, but copy the found content with little understanding, and this kind of work becomes their habit.

In order to protect young people from addiction to the Internet and e-social networks, interesting activities, projects and lectures are being organized. The police publish presentations on the threats of the Internet; articles on children addictions to the Internet are frequently published. Lectures for young people are held in schools on the topic of "Threats on the Internet", in the week with the day of the children safety on the Internet (8 February). Teachers who teach computer science in schools are advised by the heads of their section and representatives of the Education and Teacher Training Agency to organize classes on "Safety of Children and Young People on the Internet" at least one lesson, so that young people would not experience some form of abuse. These lectures are also useful for elderly users of the Internet and e-social networks.

Figure 2[1] presents the division of computer addiction according to the levels. If the computer user is addicted to e-social networks and “online” games, they are also addicted to computer. The bigger problem is the information that 89% of “online” games contain violent content. At the first level, there is the addiction to games on the local computer, Internet addiction and addiction to writing on the computer. During the lessons of computer science, young people often show interest in writing on the computer instead of their notebooks. At the second level, there is addiction to “online games”, addiction to e-social networks, web mail addiction, addiction to gambling on the Internet, addiction to blogs, forum addiction, Google search information addiction, cybersex addiction, and Internet shopping addiction. Addiction to e-social networks is divided only in the addiction to the most popular and most frequently used social networks.

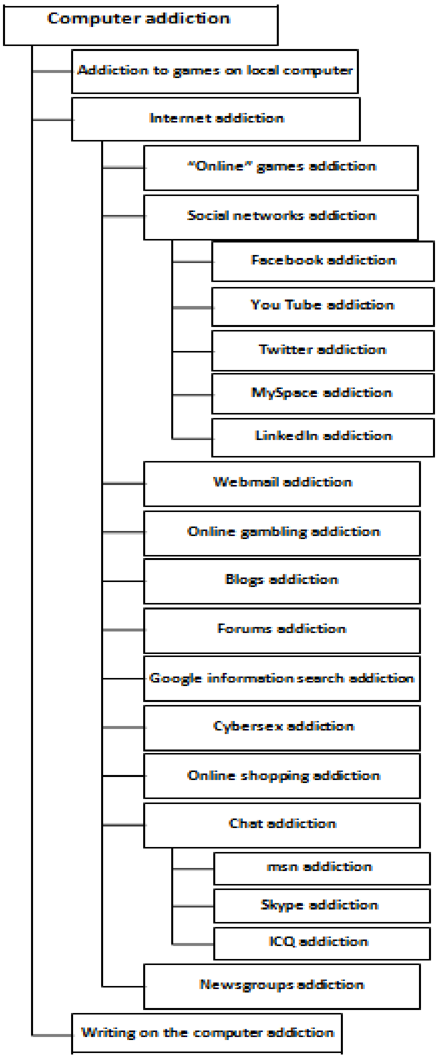


Figure 2. *Division of computer addiction*
Source: Varga, M., Šimović, V., Milković, M. (2012.) Zaštita elektroničkih informacija. Varaždin: VELV. p. 46.

[1] Creating an author. Decomposition addiction on the computer.

From the divisional diagram (Figure 2) (which shows the addictions on the Internet and e-social networks), we can compare the use, popularity and the amount of visiting web sites that contain e-social networks with the popularity and the amount of visiting web sites which contain pornographic content. According to the psychologist Sandra Milotti Ašpan (Milotti Ašpan, 2012) e-social networks have become more popular than web sites with pornographic content. This definition is not strange at all, but it is the evidence that the appropriate services "put an end to" pedophiles and malicious people who download forbidden content and photographs from pornographic web pages (web sites).

Identity theft of the e-social networks users

The cases of identity thefts in e-social networks have been tried to be suppressed by raising charges by the police (Ministry of the Interior) and by sending a special report to the public attorney for young people against malicious people who steal identity of the victim and in the person's name publish their personal information (http://dalje.com/hr-hrvatska/zbog-otvaranja-laznog-profila-na-facebooku-maloljetnik-kazneno-prijavljen/, 2011). Identity theft on e-social networks is also one of the forms of abuse and privacy violation.

Based on the published research by the authors of this paper, which was conducted in April and May of 2012, on the sample of 204 participants *(N = 204)* mostly school children, i.e. in primary and secondary schools in the Međimurje County aged between 13-19, came to the conclusion that the privacy of young people was at risk on the Internet. That was the aim of the research. Additional research was conducted in another two schools in the period from 20 April 2012 to 27 April 2012. The study was conducted in an elementary school (subject teaching) in the Međimurje County and in one high school in Zagreb (four-year programs). In this way, the research sample increased by 86 new participants *(N = 86)*. The total number after the additional research amounts to 290 participants (*N=290*). Young people who were interviewed represent a field sample of the population. This field sample is representative, which means that it has properties which are relevant to the subject of research. Besides the mentioned research objective, clear research tasks were as follows: to obtain information about the opinion of the participants in terms of security of personal information on the Internet and e-social networks; to obtain information on potential threats on the Internet and e-social networks consisting of false presenting of young people in certain schools; to obtain information on the specific number of identity thefts on the Internet and e-social networks from the selected sample; to obtain information on how much the participants publicly vilify on the Internet (since the Internet is a public computer network) and e-social networks; to obtain information on the number of spam received; to obtain information on the frequency of deletion of browsing history; the information on the participants' opinion whether it is good to keep a laptop in a place accessible to everyone. Based on the gathered information, computer science teachers should influence the youth in order to suppress (1) endangering the Internet users, (2) false impersonation on the Internet and e-social networks, (3) vilifying of young people on the Internet and e-social networks by that group of young people where the mentioned abuse is present. In the schools where the research was conducted, efforts will be made to have a positive effect on participants in order to reduce any other form of abuse of both younger and older Internet users. The results were processed and presented in 3D pie charts in MS Excel, a tool for analytical data processing.

Figure 3 shows that 79.3% of participants think that the electronic data placed on the Internet or e-social networks is not safe, while the remaining 20.7% thinks the opposite. Fifty-five point five percent (55.5%) of participants answering the second question agreed that their privacy is mostly compromised on the Internet; 13.1% of participants said they completely agree that their privacy is compromised on the Internet; 24.5% of the total percentage of participants stated that they generally do not agree that their privacy is compromised on the Internet and e-social networks. Privacy of Internet users is not compromised if the user does not allow malicious people to publish their personal and other data to compromise their privacy. Based on the above research, it was concluded that most participants do not make false presenting on e-social networks, which is good and deserves praising. Sixty-three point eight percent (63.8%) of the total number of participants said they had never falsely presented themselves on the Internet and e-social networks, while 36.2% of them falsely presented themselves.

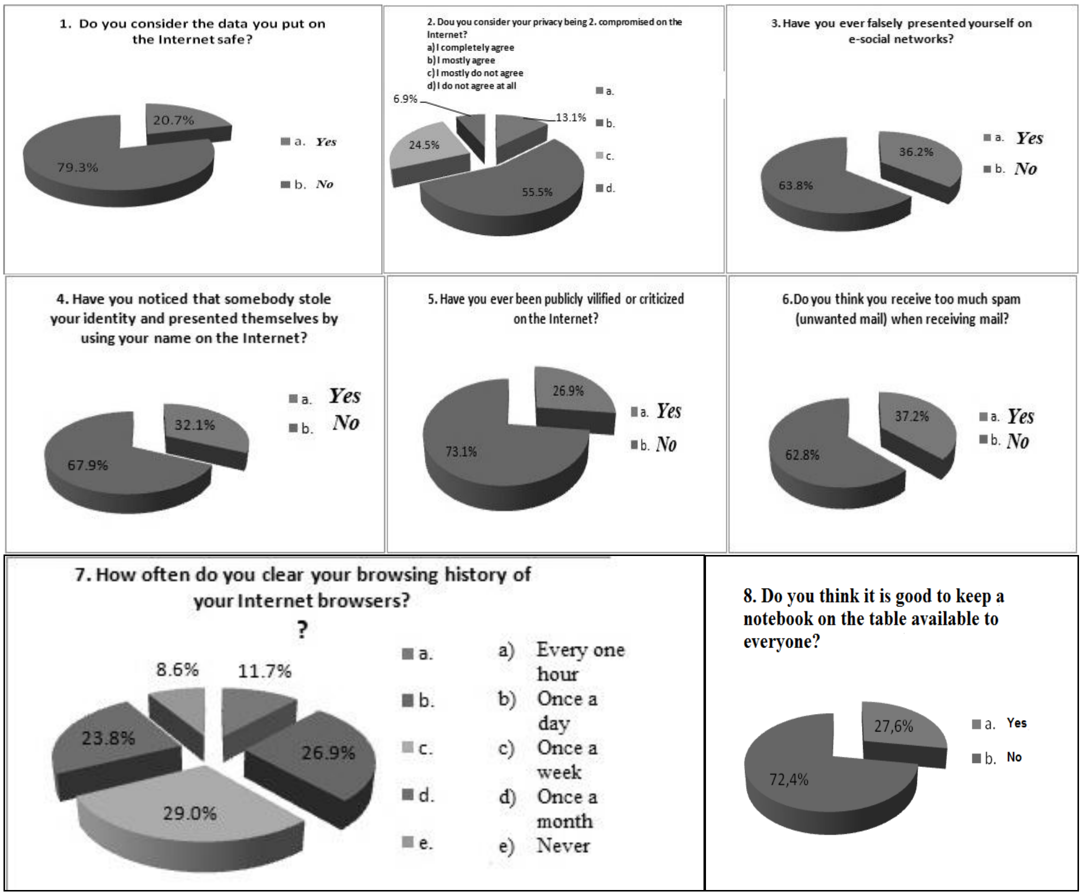


Figure 3. *The results of the survey obtained from the sample of 290 participants*

The situation with young people at schools (where the research was carried out) in terms of identity theft is not alarming (Figure 3). Sixty-seven point nine percent (67.9%) of participants responded that no one stole their identity on the Internet, nor has anyone presented themselves by using the name of the young people interviewed. Thirty-two point one percent (32.1%) of participants had an unpleasant situation when someone else (the attacker) wrote and communicated on the Internet and e-social networks in the name of the participant, at the beginning of communication without their knowledge. Seventy-three point one percent (73.1%) of participants have not experienced public vilification on the Internet, while 26.9% of participants experienced public vilification and criticism on the Internet and were abused in this way. Sixty-two point eight percent (62.8%) of participants felt that they have not been receiving too much spam in their inbox, while 37.2% of them thought that they did not get too much spam. Cookies are files that your Web browser stores on your hard drive for computer users. Cookies contain information about Internet users and their activities via a web-browser. Cookies are a risk as far as the protection of the system because they can find in it our personal data can get into the wrong hands. If the security system is of great importance, the prohibition of accepting cookies is the best defense.The largest number of participants deletes electronic information on browsing web sites once a week (29.0%), while 26.9% of participants deletes browsing history once a day. Browsing history is deleted once a month by 23.8% of participants, while browsing history is deleted every one hour by 11.7% of participants. Eight point six percent (8.6%) of participants never delete browsing history due to not having the option for remembering the visited web sites enabled in their browser and they do not keep records of browsing history (Pastore, 2004). Most participants think it best not to hold a laptop computer available to everybody (72.4%), while 27.6% thinks otherwise and their personal electronic information is not stored in this way.

Internet and e-social networks users' password safety

Everybody needs to have a user name and password to access a particular service or e-social network on the Internet, i.e. an Internet service provider. It is advisable to change your password every month, and if necessary, it should be changed several times a month. Quite often there are cases when a person finds out the password of another person, and then this malicious person causes them harm in the name of another person. Such a scenario represents one form of abuse of the Internet and e-social networks users. Optimal password used by users of online services should be a minimum of seven characters. It is preferred for a password to contain a combination of uppercase and lowercase letters and numbers. For greater security, sometimes it is necessary to put a character that is used very rarely in the password. It is by no means recommended to use first names, surnames, names of parents, children, date of birth, name of residence, street name, and the like for the password. Such simple passwords are the ones that young people usually use most often. It is not recommended to use for the password the same set of characters. For safety, information systems users should never write down their password on paper and leave it in a drawer to prevent their friends, siblings, or friends to gain access to data and to the user profile on e-social network. The most common attack done by malicious persons on passwords, i.e. the profiles of your friends, is by testing or guessing passwords. Password testing or guessing is an attack in which malicious individuals attempt to access a certain system by randomly guessing the password, where mostly the method of trial and error is used. Although this attack might seem naïve, sometimes it can be effective, especially when malicious person knows the person who set up the password well.

The second most common attack on passwords for Internet users is the so-called “phishing”. The user of a user account receives an unwanted mail written by a malicious person in which it is required to submit the user name and password in the next few days; it says “if you do not send your username and password, you can permanently lose the account”. The recipient of this e-mail has the feeling that the email was sent by the administrator of the web server which provides the service itself. The attacker uses the name of the ISP Internet service provider so that the mail would be more persuasive. Sometimes young people are gullible and fall for most of these mails. A recommendation to younger and elderly users is to not to fall for such mails, and to not send personal user data in response to such an e-mail.

Privacy settings on e-social networks with regard to Facebook

“Facebook” privacy settings can be adjusted by turning off and deleting. Turning off the “Facebook” profile of young people means that the data and content on the profile would be hidden from the other friends’ view, but are stored on “Facebook” servers, in case the user wants to re-activate his or her profile. The user name appears as black text on which you cannot click because the profile is hidden.

By deleting the “Facebook“ account, the page is permanently removed. “Facebook” center for help with personal information related to the user account states that permanent deletion deletes information such as a name, e-mail address and mailing address. Copies of some materials (photos, notes, etc.) may remain on the “Facebook” servers due to technical reasons. Permanent storage of photos by “Facebook” is not good for the e-social network users. All the materials on “Facebook” should be detached from any personal identifiers and completely inaccessible to other users. “Facebook” also does not use the contents associated with the accounts which are deactivated or deleted. Before all the data on “Facebook” is deleted completely, several days could go by because there is an option that in the meantime the user could change his or her opinion. When using the e-social network, the “Facebook” user should think twice about the finance policies of the e-social network, and whether they can make profit just by the means of traditional advertising, as well as how the web corporation “Facebook” has achieved such a high value. Facebook profile can be viewed by the executives of the company we work at, business partners we work with, prospect business and love partners, and colleagues, malicious persons, etc. No matter what protection is used on Facebook profile, there is surely someone who could forward our photo to a person who does not quite like us. Our photos can be forwarded by our best friends to their friends who could abuse our digital photograph. Information to be avoided giving on e-social networks are home address and number; photos from the party; admitting not to work and the like; the names of your children; pictures of the apartment and the house; information on the time of vacation; phone numbers because there are applications that display telephone numbers which are posted on Facebook profiles. With all this information, it is not desirable either to count down the days to going on vacation e-social networks.

RECOMMENDATIONS FOR THE PREVENTION OF VIOLATION OF THE INTERNET USERS RIGHTS

In order to prevent violations of the rights of users on the Internet, online services offer the privacy policy and terms of service. Recommendations are to carefully read the rules before using e-social networks and that users adhere to these rules. The user must confirm to abide by the set and stated rules when using online services when creating a profile or user account of electronic web mail. Each Internet service provider tends to set rigorous rules, but the users of Internet services rarely adhere to these rules, and in most cases young people do not read the rules but confirm them automatically by clicking the mouse.

The rule that all users should follow when using the services of correspondence on the Internet is that no activities related to drugs, alcohol and other narcotics should be promoted.

Each individual service provider on the Internet has rules that users must abide by, and these rules should not be mocked at or belittled. It is widely known that the providers of correspondence services do not allow URL addresses of sites and links with content linked to sex or illegal music be published in the writing area. On chat and in newsgroups links of crack sites are not allowed.

Identity theft on e-social networks is among the violations of the Internet users' rights. The way to fight against such violations of users on the Internet is enabling users to authorize themselves biometrically on the Internet services. In this way, it would be easy to identify malicious persons who present themselves by using the names of their colleagues and other users. The only problem with the introduction of biometric authentication system for Internet users is financial viability, and the existence of such a possibility and option for Internet services (the providers of certain Internet services). Nowadays, Internet service providers and the manufacturers of operating systems offer email addresses which the victims of identity theft can complain to and report the case, so as to stop these cases.

THE FORMS OF USERS' VIOLATIONS ON THE INTERNET AND E-SOCIAL NETWORKS

The most common form of user's violation is an abuse. The risks that exist on the Internet, which the users should avoid when "surfing", and which in some way interfere with communication on the Internet and users (especially young people) and can lead to danger are commercial, promotional, offensive, sexual, and value. Commercial risks and dangers that threaten young people include numerous advertising and promotional activities for drugs, alcoholic beverages and tobacco products. The risk for young people may be presented by unwanted mail through which strange and malicious content can be distributed together with sponsored ads. Disclosure of personal information of young people, stalking of young people, illegal downloading of certain content, financial frauds and gambling, are a big problem for Internet users. When young people browse the Internet, there is a risk of experiencing an attack by a malicious person. On the Internet, the users may encounter violence and hatred arousing. Internet users can encounter pornographic content, bullying and other harassment by third parties. There is a possibility that users, especially young people, meet a stranger with strange intentions. Internet and e-social networks users can create and set up inappropriate material and content on a web site (*upload*). The risks of widespread broadband network that Internet users may encounter include misleading electronic information or misinformation and tips; racist statements and aroused hatred for a particular race. On the Internet, with little negligence, users can hurt themselves. A number of cases exist in which a specific web site contains wrong electronic data that young people believe in, i.e. false information or misinformation that makes young people learn in the wrong way, and which makes their development go in the wrong direction. Misinformation is different from information by having no value for the Internet users.

In addition to these forms of the users' violations on the Internet and e-social networks, there are more violations in the form of disturbing and threatening messages, hatred arousing by the service user groups on correspondence services (IRC) directed to a specific person, encouraging further bullying, insulting and spreading violent and abusive comments, creating pages that contain images, drawings, stories and jokes at the expense of peers, sending inappropriate photographs of colleagues, mentioning personal data and information on family circumstances, spying Internet users via webcam of their computer. Spying young users via webcam of their computer is one of the most serious forms of violation. To make this kind of espionage function, the spy must have access to the computer user who is the target, and must have authorization on the target computer.

An example of this kind of abuse of young Internet users took place in America where school officials were spying their students via webcam. Young people in this case got their computers from the school in order to access the data/resources of that school (http://dnevnik.hr/vijesti/hrvatska/, 2011). In order to fight against this form of violation of young people on the Internet it must be taken into account who the computers are taken and bought from. If young people take or borrow a computer from a person they do not know well or from an organization which sells or services the computer, it would be advisable to pay attention to the possibility of such attacks, and to turn off the camera if they need not to use it.

THE CONTROL OF DATA FLOW ON THE INTERNET IN THE TEACHING PROCESS

In order to protect the Internet users from addiction and other negative sides of the Internet, specific tools that simulate parental supervision should be used, since it is impossible to be 24 hours with the child who browses the Internet. Today there are tools that block access to certain sites on the Internet. Such an option is provided by the tools for managing a classroom or local computer network. Tools to control the data flow can block e-social networks “Facebook” and “YouTube”. SynchronEyes Classroom Management tool is used in teaching by the teachers in schools in the Međimurje County to have supervision and data flow control of computers and computer networks, which students work in. These tools can be used to help students solve the tasks on the computer by taking control of the student’s computer.

The possibilities of certain systems of LAN network management

LAN is a local computer network in a smaller area, organization or institution that is intended for internal use. An example of such a network is the computer network in the classrooms. Teachers Network Management System computers offer many opportunities in the classroom. Systems such as SynchronEyes Classroom Management enable the presentation of content from your computer (screen) to all students in the class, then allow active involvement of students in the teaching by supporting the creation of students groups, and allow the presentation of some solutions on all the computers in class, JIT review of the student’s work, active control of the student’s work using the option of input units control, the creation and implementation of knowledge tests, as well as JIT evaluation of the results, distribution and collection of digital solutions made by students, teaching management in terms of allowing the execution of certain applications and the Internet access, classroom and student computers management, and the management of their works that are currently in digital form.

"Parental" protection of the operating system and OpenDNS

IT professionals can set parental protection on the computer in some operating systems, i.e. parental control over the computer. Since the vast majority of elderly parents especially is not literate enough when it comes to computers to set this type of supervision, for the benefit of users and young users, they should contact an IT professional or an IT company to set up parental control over the account. Through parental controls, the way that the users use the computer can be controlled. IT technician can set limits on the computer owner regarding the hours during which users are allowed to use the computer, the type of game that can or cannot be played, and programs that can be run. When parental control feature blocks access to the game or program, there is a notification that the program is blocked. Users can click a link in the notification to request permission to access a game or a certain program. The access may be allowed by entering the user information. To set up parental controls for the child, you need your own administrator user account. Before the start, it is necessary to check whether the users you want to set up parental control for have a standard user account. Parental control feature can only be applied to standard user accounts. With the control provided by Windows 7 an additional control of a separate provision of services can be installed, such as web filtering and activities reports. In the operating systems, the users' access and opening of specific programs to be used can be limited. OpenDNS allows filtering of web pages which the user wants to access, based on the URL addresses. There are two lists: (1) the list of allowed domains, and (2) the list of banned domains. The top ten contents blocked by OpenDNS include web pages containing pornography in 85% of cases; sexuality in 80.1%; unsavory content in 77.3%; Proxy/Anonimizer in 76.2%; advertising networks in 69%; nudity in 69.2%; discrimination and hatred in 58.7%; lingerie in 58.5%; gambling in 58%; and drugs in 57.3%. E-social networks "Facebook", "MySpace", "YouTube" (www.opendns.com/pdf/opendns-report-2010.pdf, 2010) enter the top three blocked web sites. Based on the research, it can also be concluded that there is addiction to cybersex, social networks, listening to music, chat, etc., because they are not unreasonably blocked and filtered by OpenDNS sites in most cases with the mentioned content. A bad example of blocking certain e-social networks by employers, with the purpose of future employment, is that employers seek from their future employees a username and password of the e-social network they are users of.

CONCLUSION

It is not difficult to conclude that the participants would most often falsely present themselves on those online services and e-social networks they use most. In organizations where the research was conducted (the Međimurje County and a high school in Zagreb) the tendency will be try to have a positive impact on the young Internet e-social networks users with the aim to reduce false presenting on the Internet. With this paper and examples, the existence of violence among users on the Internet and in reality, and (based on the research results) of the Internet and e-social networks addiction in the Republic of Croatia and abroad has been proven, on the basis of a sample of 290 participants *(N=290)*. The next problem that is trying to be solved today is fighting against addiction to the Internet and online gaming on e-social networks. One of the ways to suppress addiction to the Internet that was mentioned in the paper is to place parental monitoring by IT professionals using the options of the operating system and OpenDNS. Moreover, to protect young people from the Internet and e-social networks addiction, interesting activities, projects and lectures tend to be organized. The publication of presentations on the subject of child protection on the Internet and privacy protection also affect the suppression of the threats on the Internet and e-social networks. Croatian Ministry of Interior[2] also frequently publishes articles on the protection of children on the Internet. In schools, numerous lectures for young people on the topic of “Threats on the Internet” are held. In the week with the day of the children safety on the Internet (February 8), the teachers who teach computer science in schools are advised by the heads of the section and representatives of the Education and Teacher Training Agency to dedicate one lesson on the topic of “Safety of Children and Young People on the Internet”, so that young people would not experience some form of abuse mentioned in the paper. When it comes to protecting user accounts on young people e-social networks, young people should frequently change the password, and set the optimal strong password. When it comes to preventing attacks via computers, systems for the management of local computer network (LAN) are often introduced. In this way, the flow of electronic information of young people on the Internet is controlled. Finally, we ask ourselves whether to use e-social networks at all. Our recommendations are to use e-social networks, regardless of any negativity. It is necessary to be cautious with personal information in electronic form and we advise not to believe everything what is said on the Internet or e-social networks. Do not write unverified information about other people. It is necessary to carefully choose which photos from the party you will put on e-social network. It is necessary to take into account possible false presenting of a malicious person, and it is necessary to determine, if possible, which electronic information the social network sells or makes available.

REFERENCES

1. Dragičević, D. (2004), Kompjuterski kriminalitet i informacijski sustavi, Zagreb, IBS.
2. Engst, A., Fleishman, G. (2004), The Wireless Networking Starter Kit, Second Edition, Berkeley, Peachpit Press.
3. Jeriček, H. Internet i ovisnost o internetu u Sloveniji, Medijska istraživanja, 8(2),85-101.
4. Kurose, F., Ross, W. (2005), Umrežavanje računala. Wesley, Računarski fakultet, Sveučilište Masačusets & Bruklin: Politehničko sveučilište, CET, Pearson Addison.
5. Miliša, Z., Tolić, M. Kriza odgoja i ekspanzija suvremenih ovisnosti. Društvo, 4(8), 135-164.
6. Milotti Ašpan, S. Društvene mreže – blagoslov ili prokletstvo, Retrieved on 26th April 2012 from http://www.zdravi-grad-porec.hr/strucne_teme_drustvene_mreze.php.
7. Pastore, M., Dulaney, E. (2004), Security+. Study Guide, Second Edition, Exam SYO-101, IndianaPolis, Wiley Publishing.
8. Pezo, A. Na putu k stvarnoj zaštiti djece na internet, Savjetnica pravobraniteljice za djecu, Retrieved on 31th May 2011 from http://www.slideshare.net/PogledKrozProzor/na-putu-ka-stvarnoj-zatiti djece-na-internetu.
9. Varga, M., Šimović, V., Milković, M. (2011), Zaštita elektroničkih informacija, Varaždin, VELV.
10. Internetsucht: Jugendliche gefangen im Netz. Retrieved on 11th June 2011 from http://www.onlinesucht.de/internetsucht_preprint.pdf.

11. Kaznena prijava (2011), Retrieved on 3th June 2011 from http://dalje.com/hr-hrvatska/zbog-otvaranja-laznog-profila-na-facebooku-maloljetnik-kazneno-prijavljen/362144.
12. OpenDNS 2010 Report. Retrieved on 24th June 2011 from http://www.opendns.com/pdf/opendns-report-2010.pdf.
13. Sponzorirani oglasi. Retrieved on 26th April 2012 from http://www.facebook.com/profile.php?id=1139563573.
14. Špijunaža djece web kamerom (2010), Retrieved on 8th June 2011 from http://dnevnik.hr/vijesti/hrvatska/skola-spijunira-ucenike-web-kamerom.html.