International Journal of Business, Human and Social Sciences
ISSN: 2517-9411
Vol:8, No:11, 2014

General Awareness of Teenagers in Information Security

Magdalena Naplavova, Tomas Ludik, Petr Hruza, Frantisek Bozek

***Abstract*—**The use of IT equipment has become a part of every day. However, each device that is part of cyberspace should be secured against unauthorized use. It is very important to know the basics of these security devices, but also the basics of safe conduct their owners. This information should be part of every curriculum computer science education in primary and secondary schools. Therefore, the work focuses on the education of pupils in primary and secondary schools on the Internet. Analysis of the current state describes approaches to the education of pupils in security issues on the Internet. The paper presents a questionnaire-based survey which was carried out in the Czech Republic, whose task was to ascertain the level of opinion pupils in primary and secondary schools on the issue of communication in social networks. The research showed that awareness of socio-pathological phenomena on the Internet environment is very low. Based on the results it was proposed appropriate ways of teaching to this issue and its inclusion a proposal of curriculum for primary and secondary schools.

***Keywords*—**Cyberspace, educational system, general awareness, information security, questionnaire, socio-pathological phenomena.

I. Introduction

THE new period brings new opportunities and new technologies. Not long ago, personal computer was a big hit nowadays is owned mobile devices with access to the Internet connection necessary part of the equipment of every person. Cyber environment surrounds real world and it is very closely connected.

Internet is the most famous part of cyberspace. At the beginning, the Internet was only a working tool which serves to communicate distant groups and source of information. Currently, the Internet provides many opportunities to use it. It still remains a source of information, but communication lends an entirely new dimension. Communications between two or more persons in real time use communication software and social networks. Software designed to communicate offers also the possibility of a telecommunication or even the possibility of implementing video calls. Just video calls become the most used tool in recent years. Use them and broadband connection to the Internet can be overcome thousands of kilometers away magically. Globalization has caused mass expansion of companies around the world. And how can remotely manage all these subsidiaries? They manage with the support of information systems.

Unfortunately, the Internet and cyberspace generally has its downsides. Not only has it become a place for communication and entertainment, but it is also a place for a new kind of crime: cybercrime. Cyber-attacks are conducted at international and national levels, which can lead to the threat of cyber terrorism and cyber warfare. The aim of these attacks become national governments, government agencies or international companies, but very often become the target of attacks by ordinary citizens.

The most vulnerable groups are mainly young people who have become targets of socio-pathological phenomena. Children are acquainted the existence of a risk on social networks in the course of instruction in primary and secondary schools, both in individual subjects or lectures representatives of the Police. Even though the issue is gradually becoming recognized by the children and their parents, number of victims is increasing. For this reason, it should be on issues of safety behavior on the Internet becoming more and more emphasis.

M. Náplavová, T. Ludík, P. Hrůza, and F. Božek are with the Department of Emergency Management, University of Defence, Brno, Czech Republic (e-mail: magdalena.naplavova@unob.cz, tomas.ludik@unob.cz, petr.hruza@unob.cz, frantisek.bozek@unob.cz).

II. State of Art

In parallel with the existence of the real world surrounds us and virtual environment, which is made by using modern technology, such as computers or telecommunications networks. This virtual world is called cyberspace. Cyberspace has global coverage and affects the behavior of companies around the world. [1]

Cyberspace may be understood as a virtual space which was created with the help of interconnection of computer systems in the network. In this area of the interacting entities without the need for physical activity, information can be shared in a particular time or with any delay. [2]

The Internet is the most important inventions of modern times. Pupils and students use it to learn, and therefore the Internet an integral part of every modern home.

The origins of the Internet can be dated back to the 60s of the 20th century. Initially the Internet was created to enable communication between experts and selected universities. Already in the 70s, the network quickly grew and began to involve other universities and two European institutions have become part. For while the Internet was intended only for the academic community, but due to later legislative changes could also be used commercially . The second problem was the contemporary nature of the applications. Experts made up the application, so it was barely usable for laymen. [3], [4]

A crucial turning point was the creation of services WWW (World Wide Web). This service was established in the Geneva Center for Nuclear Research – CERN. They used are known principle of hypertext, which is a set of texts which are

interconnected by links. This principle also added a communication protocol called HTTP (Hyper - Text Transfer Protocol). The first web server was running in 1990 at CERN. Another significant milestone in the development of the Internet has been completed development of a graphical client that resembled certain features of the current modern web browsers. [3], [4]

A. The Illegal Activities in Cyberspace

One of global threats is cyber terrorism. Cyber terrorism is a crime that is committed by using IT technologies in order to induce fear [4]. Another way to abuse a cyberspace is the management of cyber warfare. The attackers, who lead cyber war against the state, they are no longer classical hackers, but it is an organized group of people or even a small army of experts in the field, whose main advantage over conventional army is their ability to work in the virtual environment, which means that they can move anywhere worldwide.

Another way to abuse cyberspace is the management of cyber warfare. The attackers, who lead cyber war against the state, they are no longer classical hackers, but it is an organized group of people or even a small army of experts in the field, whose main advantage over conventional army is their ability to work in the virtual environment, which means that they can move anywhere worldwide.

Cyber terrorism and cyber warfare take place on an international level. Attackers focus on non-governmental organizations, international and national organizations. However, more frequent targets of attackers become individuals. Craker uses the malware for attacking of networks, which is malicious, dangerous software. Among the malware can be classified as viruses, Trojan horses, spyware. [5]

B. The Socio-Pathological Phenomena in the Environment of Social Networks

One of the possibilities that Internet allows, is communication via social networks. A social network is an interconnected group of people who can influence each other, while they need not even be related. The social network is made on the basis of common interests, friendship or family ties or because of other reasons, for example economic, political, cultural or religious. [6]

Each individual immediately becomes a member of a certain social group after his birth. There is the interaction of all members in the group. Each individual is usually a member of several groups, which may otherwise identify, act or communicate.

Among the most popular social networks are mainly Facebook or Twitter. Internet social networks may enable us to communicate, but they are also very dangerous place, especially because here there are socio-pathological phenomena such as cyberbullying, cybergrooming, cyberstalking or social engineering. Guaranteed protection from perpetrators of crimes such as cyberbullying, cyberstalking or cybergrooming unfortunately does not exist. In this context it is necessary to pay attention to prevention. Most people on the Internet environment behave differently than in the real world. People are more open, not afraid to disclose information, publish photos or videos. But not all such material remains the only shared with friends. Very often leads to abuse of information that they are the basis for the later crime. [7]

Cyberbulling is type of bullying using electronic means such as mobile phones, emails, pagers, internet, blogs and similar for sending harassing, offending or attacking mails and SMSs, creation of pages and blogs defaming selected individuals or groups of people. [8]

The difference between traditional bullying and cyberbullying is that cyberbullying takes place in a virtual environment, which may cause even more problems. This may be happen anytime and anywhere, because virtual space is omnipresent. The victim is always possible to state if there is a connection to the Internet or mobile network. For this reason, it is very difficult to hide from the attacker.

III. Applied Methods

The work was carried out using several scientific methods. In analyzing the current state of background research was used mainly literature that provided theoretical basis for solving the problem. Method comparison provided us compare the results of the questionnaire survey, which was carried out in primary and secondary schools in the Czech Republic.

The actual questionnaire survey, which examined the relationship of primary school pupils and secondary school students completed graduation exam to safety on the Internet. Another surveys carried out by independent research organizations around the world. Descriptive research was carried out using a questionnaire survey and in electronic form. The questionnaire was then distributed through publication on social networks and leadership sent randomly selected schools in the Czech Republic. The data from the questionnaire survey was conducted after collectively and anonymously processed and statistically evaluated. On the basis of statistical evaluation with the help of induction was made general statements on the issue.

IV. The Results

Population 10+ years on the Internet environment is 71 % in the Czech Republic. The number of people who use the Internet grows at an average rate of 4% per year over the last two years. Older people use the Internet less than young people. Internet penetration in people over 55 years is 37.2 %. There is great potential and the greatest growth will continue in this age group, although to a lesser extent than in previous years. On the Internet there are more men than women, with increasing age, the proportion of men increases and the proportion of women decreases. While among users under 25 years is almost 60 % of women, who are over 55 years it is only less than 30 % of women. The exact data can be seen in Table I. Users use to connect to the Internet also your mobile device or tablet. Czech number of mobile Internet users in the last year almost doubled. [9]

TABLE I
THE AGE STRUCTURE OF THE INTERNET AND THE REAL POPULATION [9]

Age	Internet population	Real population
10 – 14	432 000	456 000
15 – 24	1 064 000	1 170 000
25 – 34	1 367 000	1 525 000
35 – 44	1 579 000	1 683 000
45 – 54	1 068 000	1 345 000
55 +	1 201 000	3 234 000

The persisting phenomenon of the Internet is still social networks. Without them, the young generation can only barely imagine communication with friends and sharing information. Younger children crave create a profile account on any of the social networks that they can keep in touch with friends and family. The reason for the registration of the social network is primarily a desire to communicate with others, meeting new people, having fun, but also a desire to be integrated into the team and not to be deprived of selected information. Teenagers do not appreciate their privacy. If the information once published information exists forever. Although teenagers this information deleted , for example, from your profile or page of your site, there is a possibility that this information just someone saved and the information is stored on the server and is ready to abuse. These are mainly personal photo that children are sent to each other. There is no guarantee that their friend does not abuse this photo.

Unfortunately, social networks also have its downside. It is a place where children can result in considerable danger. The danger is hidden in unknown people with whom children communicate. Unfortunately, as is evident from the questionnaire survey, pupils do not realize this risk. Teenagers are willing to share information about themselves publish their photos, photos of family or pets. But never think of the fact that the information may be misused.

The survey, which was carried out on the territory of the Czech Republic, showed that most teenagers publish on its website or on social networks photographs of family, residence or pets. It has a very similar character as the disclosure of personal information. Photos can become a guide for the offender, who can use photographs for mapping the neighborhood around its victim.

Disclosure of personal photographs that can even erotic subtext is very popular among teenagers. It has to do with a new phenomenon, which is called sexting. The aim users are using erotic pictures capture the attention of the other person, of which manifest an interest. Photos can be sent directly to another person or also just published through social networks. These photos can be used for further distribution or can also be misused to blackmail the occupants. In the second half of 2014, the Czech Republic began to multiply instances of abuse photos. Photos of naked girls collectively publish on social networks without the consent of the person. These are mainly erotic photographs of young girls.

The role of school facilities is to educate children, not only in maternal language or mathematics. Computer literacy of students is very high. Children learn to operate the new technology much faster than older generations. Therefore, it was also included in the curricula of education on the field of information technology. Here children receive a comprehensive explanation of what actually serves information technology and teaches them gradually working. They are familiarized with the characteristics of the hardware, software and Internet environment. However, before children are admitted into the environment in which it runs a high amount of risk, they should be acquainted with the principles of safety behavior in the environment.

Currently, a large trend is adaptation lessons needs of the child. The school aims for pupils to develop their hobbies and interests. Therefore currently absent strict curriculum that exactly say what, in the subjects they teach pupils. A very common phenomenon is unfortunately draining just basic information. In the computer science education is primarily about leaving out essential information on safety behavior on the Internet. Students are acquainted with the latest technologies, develops their practical activity, but the basics are missing. Unfortunately, just these basics are very important because they could serve students is on their work life.

Lessons of information technology in the Czech Republic incorporated into the education of pupils in 5th grade of primary school. This means that the child learns the basics of information technology in the age of 11-12 years. But there are exceptions. Lessons of information technology in selected educational institutions incorporated immediately at the beginning of schooling. These schools reflect that the children in kindergartens are confronted with smart mobile phones or tablets. These children come to school with a basic knowledge of operating these devices. Children aged 11-13 years can create their own e-mail address and send e-mails from this e-mail address. A valid e-mail address is a necessary requirement to register on a social network.

V. DISCUSSION

Unfortunately, many teenagers come home and turn on their laptops and aimlessly are browsing the Internet. However, this activity may cause damage to the computer. Attackers saved malware especially for websites with erotic themes, and also the pages that are used for free software downloads. Fake websites and fake profiles of famous people are very popular place for attackers. Here, attackers can store their malicious programs. After infecting computers with malware, the mechanism starts getting personal user information that an attacker collects and misuse. Teenagers also increase the level of risk to their irresponsible behavior. A large percentage of teenagers give other users an overview of their personal data, photos and videos and even in denial that this information could be misused.

Fake profiles or websites of celebrities may not only be a source of malware. The attackers pose as a celebrity and try to lure students to the conversation. Teenagers believe that they correspond with a celebrity and develop the conversation. The attacker takes advantage and collecting personal information from teenagers. Result of the conversation can be a personal meeting. These personal meetings very often end in rape or

kidnapping of the child.

With the increasing number of cases of cyber-attacks begin school react to the situation. Schools are trying to educate their teachers on this area. Teachers also have a large amount of supporting material. Schools also utilize the help of various organizations that deal with this issue. In schools teach externally Police workers or experts. They provide for teenagers good basic information and also offers them the possibility of communication. The key is to inspire confidence in students so that they can with their problems without fear entrust whether teachers or just an external lecturer.

It is also very important to adapt the teaching of Internet safety to students. Teachers should use modern technology and students to approach this area with videos, interactive games or using other methods. Proven way is tasking the students to work done on the issue. The students must seek information and process it.

The problem is the inclusion of the topic in teaching. There is no curriculum, according to which teachers should manage and classify the issue in teaching. It depends on the teacher's decision whether this issue will devote more or less attention. The level of computer literacy among teenagers is very high, but is also a high risk of cyber-attack.

Another way, how to reduce the number of victims, is also understanding the needs of teenagers why they want to be part of Facebook. Parents and teachers should not prohibit this activity, but to help create a safe profile. There are many guides to create a safer profile on social networks. Just pick up the literature and start. Unfortunately, many teachers do not know the possibilities.

Parents of teenagers should be educated on the issue of socio-pathological phenomena in the social networks. Although computer literacy of parents grows, they can prevent the abuse of their children. Parents also used many patrol programs. The aim of these programs is to map user activity on the Internet. It can also set the blocking of selected websites. One possibility of patrol programs is also creating a certain time availability of computers for teenagers. Parent can set a certain number of hours for which a child has accessed the Internet. Unfortunately, in modern times, many teenagers own a computer, tablet or smart phone with Internet access.

VI. Conclusion

The issue of safety behavior on the Internet is very extensive. Compared with previous years, this section focuses more and more attention. Unfortunately, even in this context, that despite all the efforts of parents and teachers, the number of victims is increasing of cyberbullying, cyberstalking or cybergrooming. Students are beginning to understand one important thing, and that the best solution is to entrust with the problem of kin, which will immediately inform the Police, which will handle the disposal of the attacker.

Cooperation of selected web portals and Police of the Czech Republic began to develop in the Czech Republic. The web portal called "seznam.cz" is most interested in the issue of security in the Internet environment. A large number of projects created under its auspices. Their goal is to educate teenagers, parents and teachers. The most famous project is entitled "Meet safely". The project is a video, which displays the cases of abuse of children on the Internet. This video is distributed to all primary and secondary schools in the Czech Republic. Internet portal "seznam.cz" performs a wide range of research. The output is a mapping behavior in children and teenagers on the Internet.

Equally important is the education of teachers and parents, especially in the matter. They are the closest people to students. Parents should not prohibit their descendants activities associated with the use of the Internet, but rather to learn comprehension and understanding of the purpose for which students in these activities.

An important factor is to stimulate students' interest in this area, because attacker's victims can become virtually anyone. The school should also not focus only on the fact that students are becoming victims of attacks, but should be understands that students are often the attackers, especially when it comes to cyberbullying or bullying in the real world.

Unfortunately, it is a common phenomenon that the children themselves become victims of their own criminals guilty. It is mainly about finding friends through social networks and agreeing on meetings for different purposes. These students are encouraged to engage in activities usually because of financial hardship or just a desire for experience adrenaline experience.

References

[1] Andress, J., Winterfeld, S., Rogers, R. *Cyber warfare: techniques, tactics and tools for security practitioners*. 1st Ed. Boston: Syngress/Elsevier, 2011, pp. . ISBN 15-974-9637-5.

[2] Hruza, P., Winterfeld, S., Rogers, R. *Cyber Security II: techniques, tactics and tools for security practitioners*. 1st Ed. Brno: University of Defence, 2013, pp. 8-17. ISBN 978-80-7231-931-2.

[3] Palovsky, R. *Information and communication networks*. 1st Ed. Prague: Oeconomica, 2010, pp. 32-61. ISBN 978-802-4517-292.

[4] History of the Internet. *How the internet*. (online). (2014-09-29). URL: <http://tm.m.idnes.cz/blog/clanek.248339.idn>.

[5] Hruza, P., Novak, L., Pozar, J. *Cyber Security: Cyber security glossary*. 1st Ed. Brno: University of Defence, 2012, pp. 11-20. ISBN 978-80-7231-914-5.

[6] Pavlicek, A. *New media and social networks*. 1st Ed. Prague: Oeconomica, 2010, pp. 42-69. ISBN 978-802-4517-421.

[7] Eckertova, L., Docekal, D., Pozar, J. *Child Safety on the Internet: Mentor responsible parents*. 1st Ed. Brno: Computer Press, 2013, pp. 54-78. ISBN 978-802-5138-045.

[8] Jirasek, P., Novak, L., Pozar, J. *Cyber security glossary*. 2st Ed. Prague: Czech branch AFCEA, 2013, pp.57-72. ISBN 978-807-2513-970.

[9] Kolar, P. *Audit of Internet visits*. (online). (2014-10-31). URL: <http://www.netmonitor.cz/sites/default/files/iac_2014_-_netmonitor_rocenka_2013.pdf>.