Sabira S. Ojagverdiyeva
Institute of Information Technology of ANAS, Baku, Azerbaijan
allahverdiyevasabira@gmail.com
DOI: 10.25045/jpis.v09.i1.09

ENSURING CHILD SAFETY IN INTERNET ENVIRONMENT

The article outlines the dangers faced by children on the Internet, their classification and ways to protect them from these dangers. The article provides information on the behavior of children in the digital world, taking into account their age characteristics. The article describes existing approaches to this problem at the International level. The activities of National Safer Internet Centers are investigated. Furthermore, the implementations to solve this problem in Azerbaijan are analyzed and some suggestions are made.

Keywords*: child safety, cyber threat, Internet addiction, National Safer Internet Centers, safer Internet.*

Introduction

With a rapid evolvement, Information and Communication Technologies (ICT) have become an integral part of our lives. One of the most promising areas of ICT - the Internet, is a space where people communicate more quickly and easily with each other and share information. Using a platform of the *WEB 2.0* on the Internet has dramatically expanded opportunities for learning, creativity and social communication, and has led to the emergence of numerous social networks. This has attracted more users (primarily children and adolescents) to the Internet. Children and adolescents are referred to the category of the society and require much more protection. The widespread use of the Internet by children and adolescents has resulted in many problems with their information security [1].

Availability of the sites full of harmful information on the global network can lead children to face the content propagating sexual abuse, aggression and violence. They are deceived on the Internet, exposed to violence and unethical behavior, and face technical and social-psychological threats. Thus, they become the victims of cybercriminals.

The Internet pushes children away from their loved ones making them to behave not as they are brought up by their family, but "dictated" by the virtual world. Children approach the global world as cosmopolitans. This process changes young people's outlook to the world and creates the feelings of 'homelessness'. The information acquired from the global network directly affects a user's perception, promotes his/her will to diverse society and lifestyle, encourages a heartwarming, "happy environment" or "habits". This is a kind of "brain wash" of children [2].

The article comments on the approaches to addressing international issues related to child safety in the virtual environment. The activities of the National Safer Internet Centers and their policies, the threats faced by children in the Internet environment and their solution ways are investigated.

Classification of hazards faced by children on the Internet

The use of the Internet exposes children to different security threats, both personal and safety. These hazards can be classified as follows:

- ✓ becoming a target of criminals;
- ✓ awareness about malicious information;
- ✓ Internet-dependency;
- ✓ harmful games;
- ✓ *phishing* technology;
- ✓ malware.

Being a target of criminals. Since the communication on the Internet is built with a virtual person, the participants are not physically presented, i.e., they are presented differently in the virtual

world. The criminals are studying child's psychology, interests, age requirements paying attention to them, caring for them, establishing "friendly" relationships with them, trying to realize own plans and to meet with more children in real life. A survey shows that about 30% of children aged 9-16 have chatted online with people they do not know before and have confirmed that it is risky, but fun. Even though children aged 9-10 have a close relationship with the virtual world, they are reluctant to date in the real world, and even 31% of those them are concerned about such dating [2].

Awareness about malicious information. Those who share malicious information disseminate information on religious, race, nationality and social hate and sexual exploitation through the Internet. This includes information on the use of drugs and their preparation, the arrangement of various harmful and explosive substances at home, and the encouragement to terrorism [3]. The web pages contain animated video clips and films, attracting teenagers to terrorist groups, and the attractive advertising videos, non-ethical phrases and slangs, and immoral habits can direct children's attitudes to a completely unhealthy environment.

Internet addiction. Some children surf on the Internet and play games on networks all day long, [4]. Their excessive interest in technology disrupts their health and psychology. Children who spend their time against computer are physically changing, and their pacing system brakes, which causes the appearance of various diseases, as if they are becoming "penguins".

Watching the computer at the nearest distance disrupts the focus of eyes. As a result, the user loses his/her eyesight. On the other hand, their interests deepen and make them dependent on the Internet. People exposed to information dependence on the Internet can act as both subject and object of the cybercrime [5].

Communicating with "acquaintances" and "friends" in the virtual world every day and eagerness to interactive games distracts children from the phenomena as time, space, reality, creates distrust in surroundings, breaks daily routines, and lowers their study. They are so addicted to this world that they feel depressed without computers and addicted to them. The Internet has already been regarded as a disease in many countries [6].

Parents can save children from the Internet by developing their talent in sports, painting, etc. In order to avoid the Internet, children's information culture should be shaped, and information and behavioral norms should be promoted [7].

Malicious games. The presence of educational, intellectual, logical, illustrated and entertaining games that develop children's thinking on the Internet, including the games that damage them can affect behavior and health of younger generation [8].

Harmful games may also include gambling with real money. Ideological games propagate violence, severity, religious and racial discrimination, influence children and adolescents pushing them to behave aggressively, grow up as criminals and have bad habits [9]. Games deliver a message to user, promote alien cultures and take younger generation away from national values and traditions.

Phishing. Another danger is phishing used by Internet fraudsters [10]. Created by hackers this method encourages a user to open a fraudulent e-mail. The user activates malicious software by selecting a link from the email, and hackers use it to get personal information. Virtual fraudsters deceive computer users attempting to obtain credit card numbers, passwords, account numbers, user code used in the Internet banking.

Malware. Obviously, when creating web pages, ads and free software are automatically downloaded to memory. These programs include "back door", keyboard-spyware, Trojan horses, and so forth. Computer viruses are also malicious programs. Every day, hackers build hundreds of malicious software as macro viruses, download viruses, scripts, scripts for *MSWord, MS Excel*,. These programs can either damage user computer and information, or destroy it completely.

Threats Preventive Methods at technological level

Various technological methods, mechanisms and software are used to prevent malicious information and direct threats to the Internet users. Content filtering is used to combat malware. This method is used by both companies and families [11].

Starting with the *Windows 7* operating system, *Microsoft* has developed software called "*Windows Family Safety*", which enables parents to protect and control children from malicious websites on the Internet. Through this program, parents are able to set limits and restrictions on several sites while using the Internet [12].

Security issues in operating systems prior to *Windows 10* were solved by additional software. Whereas *Windows 10* operating system does not have this problem and uses "*Windows Hello*" software integrated into the system.

Rapid data exchange and frequent network access also activate viruses on computer. In addition to virus protection, there is a great need for filtering. Popular antivirus programs as *McAfee, Norton, Avg* also perform filtering functions.

Parental control over children can also be provided through McAfee Family Protection and *Norton Family*. These programs perform the following functions:

- ✓ web site filtering;
- ✓ social network filtering;
- ✓ search engine filtering;
- ✓ data sending and receiving control;
- ✓ online purchase and sales safety, etc.

The monitoring conducted by experts from Kaspersky Lab in early 2015 showed that the Parental Control Module, which was used by users for Internet threats against computers, was re-applied in 2014 [13]. The main objective was to identify threats faced by children on the Internet and detect the main source of threat. As a result, the following results were achieved:

- "Parental Control Module" is applied, at least once a year, by *Kaspersky Lab* user and run 127 times on average;
- More than a quarter (26.6%) of those who are eager to play online games and one of every five users cannot resist this kind of "weapons" of sites and fall into traps;
- Russia, India and China are among the top three countries in terms of Internet threats. China, the United States, Germany, the United Kingdom and Russia are the most frequently applying the "Parental Control Module".

It is possible to identify how close children are to threats by clarifying the threats facing the Internet and revealing their main sources.

Children psychology and behavior in digital environment

Research on dangers faced by children on the Internet reveals that using the global network at most cases they share their impressions not with their parents, but with friends and fellows. More than half of children facing threats do not share ideas about this matter. As in real life, children using the Internet differ for age groups. This difference is represented both in relation to social networks or virtual objects. Experts group the Internet users by the following interval [15]: under 7; aged 10-13; aged 14-17. The dangers facing children in certain age groups are briefly reviewed below.

Internet security of children under 7. Children under 7 love playing games and they are good at using virtual objects. They cannot surf the Internet since they have just learned to read and write, and therefore they access websites only together with their parents.

Internet security of children aged 7-10. Experts believe that, depending on the psychology of children of this age group, children simply like to do what they want. Children of this age rapidly learn technology, and are eager to visit the sites and chats prohibited by their parents and to download non-ethical videos, malicious and dangerous files and programs. When they are in search for a "friend" on the Internet, they may encounter dangerous people and sexual exploits. Parents should set up a "White

List" together with their children to ensure their information security. The "White List" is a list of child-friendly sites. Thus, these sites are intended to ensure children safety.

Internet security of children aged 10-13. Children of this age group are aware of the Internet and information available there. There are enthusiastic to obtain, read, and hear that information. In most cases, the children aged 10-13 use the Internet to do homework. Children play network games becoming dependent on computer [16]. In this regard, duration of working on the computer must be determined by parents. Computer connected to the Internet should be under parental control in the common room and the parental control program should be written on computer.

Internet security of children aged 14-17. Children of this age group are more likely to communicate through the Internet rather than their parents. The control over them is becoming more and more complicated for parents. Therefore, there should be some kind of agreement between parents and children to comply with the Internet safety rules. At this age, adolescents actively use search engines, e-mail, instant messaging, download music and movies, play games, and so forth. Boys aged 14-17 are interested in everything and prefer aggressive games and look at images that are unsuitable for their age. Whereas, the girls of the respective age group prefer to communicate online rather often and use inappropriate information and content [16].

Parents should review the reports of their children's activity on the Internet. They should show how to be protected from spam. Parents should advise their teenager children to log in the actual e-mail address on the Internet, not respond to unwanted messages, and use special mail filters. Parents should be unquestionably acquainted with the sites accessed by their children.

Children should not be absolutely forbidden to use the Internet. Parents should explain their children what is harmful or harmless, and how and how long to use the Internet, rather than forbid it.

Security policy of National Secure Internet Centers

The problem of preventing cybercrime on the Internet, and at the same time, the problem of cybercrime aimed at children, who are less experienced members of society, is one of the major issues that concern many countries around the world. The European Union (EU) supports children's protection in all areas of the Internet and realizes appropriate policies to prevent threats. In 1999, the European Commission "The Safer Internet Program" was developed and covered the years 2009-2013 [17]. The program has been launched since 2013 under the name "Better Internet for Kids".

Security policy within the program is implemented through the Safer Internet Centers (SIC) developed in the EU member countries. In order to enlighten European population about the threats on the Internet, the *Insafe* Safer Internet Centers Network (SICN) has been established [17]. It includes SICs operating in 31 European countries. Typically, SICs include the following services [17]:

Awareness Center informs authorized people, parents, guardians and teachers to identify potential risks and safeguard the children and adolescents when using the Internet [17].

Youth Panel is made up of young people who are well-aware about online threats. Group members hold meetings with the leaders of the National Internet network in the country attracting the authorized people to focus on these issues and benefit from their advice and experience. They prepare video clips and tutorials on useful and harmful aspects of the Internet [17].

Youth Panels Members traditionally invite each member of SICs and *Pan-European Youth Panel* to attend annual forum. The young people aged 12-18, Awareness Center members, business representatives, politicians and other stakeholders attending this event discuss various issues related to the use of media and share information on digital issues.

Helpline is coordinated by the organization "*Insafe*". They individually inform children and adolescents, parents, teachers and guardians about safety of children on the Internet [17].

Hotlines receive information about illegal content (involving to terrorism, vandalism and hate, illicit drug use, etc.) and specific facts about sexual exploitation of children. When the content is found to be illegitimate, hotlines contact law-enforcement agencies, including Internet service

providers, and take actions in accordance with the procedural guidelines. If the illegal content is stored in another country, the hotline of that country is informed [17].

Centers traditionally organize annual Safer Internet Forum celebrating the "Safer Internet Day" on second Tuesday of February and bringing together government agencies, media, non-governmental organizations, and societies. Hotlines are coordinated by the International Hotline Association (*INHOPE*) through the *website www.inhope.org* [18].

One of the typical European NSICs is the UK's Safer Internet Center [18]. Center cooperates with 3 organizations and implements motivating projects:

- *South West grid for learning* - teaches using the Internet and works with teachers;
- *Childnet* – responsible for the security on the Internet;
- *Internet Watch Foundation (IWF)* - acts as a hotline and fights with criminal content.

The Center launches large-scale campaigns for safe use of the Internet and other technologies, and involves professionals in the country to create a safe electronic environment for children. It takes measures across the country against online criminal content and is responsible for the organization of Safer Internet Day, and develops online resources for children, parents, and teachers.

The UK NSIC provides stimulating projects, guides the children, parents and guardians, including teachers from different age groups. Based on an agreement with the country's 4 Internet providers, the center propagates the application and connection ways of proposed "family control" packages offering users the tools and recommendations on security issues and benefitting from the experience of professionals.

In Germany, NSIC was established in 2008. This NSIC includes a helpline for both children and parents, two hotlines (*www.internet-beschwerdestelle.de* and *www.jugendschutz.ne),* an awareness center (*Klicksafe*) and a youth business center. The center deals with parents, guardians, teachers and children from different age groups and protects the rights of children [19].

Russian NSIC has been operating since 2008 with the support of the Regional Public Center for Internet Technology, the Coalition "*Angel*" and the Consortium of Human Rights Movement "*Soprotivlenie*" supported by Russian non-governmental organizations. The Center is supported by the administration of the Russian Civil Chamber and the Office of Children's Ombudsman [20].

As in other states, the architecture of the Russian NSIC includes helplines, hotlines, awareness center, and youth services. Working with children and teenagers through the website, the Center comments on Russia's leading experts and analysts about various types of cybercrime and provides consulting services to users.

Each of above-mentioned SICs works in conjunction with 31 Safer Internet Centers connected to SICN. They celebrate the "Safer Internet Day" each February, participate in forums, share information and experiences, make reports, and conduct social surveys to achieve better Internet environment.

Implementations in the field of Internet security of children in Azerbaijan

As in all other areas, Azerbaijan focuses on solving the problem of children's Internet security. In recent years, the problem of children's safety on the Internet has attracted more attention of the society, state and competent authorities.

"The National Strategy for the Development of Information Society in the Republic of Azerbaijan for 2014-2020" approved by the Decree of the President of the Republic of Azerbaijan dated April 2, 2014, sets out the provision of information security and the protection of the threats that may arise in the electronic environment as a separate task. The "Development and Implementation of a "Safe Internet" mechanism for the protection of children against the illicit and dangerous content specified in the National Strategy stimulates the implementations to ensure the safety of children in the electronic environment in Azerbaijan.

In 2008, the Internet Forum of Azerbaijan, the Ministry of Education and the *Microsoft* Office Azerbaijan launched a project entitled "Children's Security on the Internet". The goal of the project was to provide methodological and information support for teachers, parents and children about children's safety on the Internet and their protection against malicious information, and to draw public attention to this problem [22].

Since 2012, Internet service provider *Sazz,* jointly with education network *AzEduNet,* has been implementing the project "*Safer Internet for Schoolchildren*". The mission of the project is to protect children from unwanted content, such as resources containing violence, extremism, obscene lexicon, in an electronic environment [2].

With the support of the Ministry of Transport, Communication and High Technologies of the Republic of Azerbaijan, the Ministry of Education of the Republic of Azerbaijan has installed a filtration system at educational institutions, conducted informational awareness-raising activities in the society, and realized several trainings at some schools [2].

All these activities carried out by certain authorities aim at raising the awareness of children living in Azerbaijan about the dangers on the Internet and preventing them from cybercriminals.

Conclusion

Children on the Internet are less protected than they are in real life. The first task of parents is to raise their own computer literacy and abilities to use Internet resources. To protect children from dangers on the Internet, they should install "family control systems" and antivirus programs on their computers restricting the children's access to certain contents.

Establishing NSIC in Azerbaijan is one of the key issues to be solved. There is already a need for awareness-raising activities on cyber security and improving the culture of safe use of information and technology. Enhancing awareness about the cybercrime in the society, launching helplines and hotlines, and developing mechanisms for protecting children against illegal and dangerous contents are the topical issues to be tackled in this area.

Family-school-state cooperation should be integrated for the protection from the threats on the Internet. The following measures should be taken in this regard:

- strengthening the public awareness about the psychological harm to children and teenagers posed by dangers on the Internet through media;
- studying and introducing international experience;
- establishing cooperation with the organization *Insafe*;
- designing a website for child safety on the Internet;
- training a scientific personnel specialized in the relevant field;
- creating social networks intended for children;
- preparing educational guidelines for children;
- organizing the aids, brochures, booklets on internet security issues for parents and teachers;
- shooting videos illustrating harmful consequences created by hazards;
- including the topics on the Internet dangers into curriculums;
- celebrating "Safer Internet Day" at schools, holding various competitions, meetings, seminars on pupils' problems, which can lead to positive results.

Parents, schools, and relevant competent authorities can safeguard children from the dangers on the Internet or contribute to the correct solution of this problem through various means to prevent potential threats.

References

1. Sokolov I.A., Kolin K.K. Development of the information society in Russia and actual problems of information security // Information Society. –2009, No 4-5, pp.98-106.
2. Allahverdieva S.S. Problems of Children's Security on the Internet, Express-Information, Baku, Information Technology, 2016, 91 p.

3. Çelen F.K., Çelik A., Seferoğlu S.S. Çocukların İnternet Kullanımları ve Onları Bekleyen Çevrim-İçi Riskler // Malatya Akademik Bilişim, 2011, 2-4 Şubat, s.645–652.
4. Dombrowski S.C., Gischlar K.L., Durst Th. Safeguarding young people from cyber pornography and cyber sexual predation: a major dilemma of the Internet // Child Abuse Revue, no.3, pp.153–170.
5. Chou C., Condron L., Belland J.C. A Review of the Research on Internet Addiction // Educational Psychology Review, 2005, vol.17, iss. 4, pp.363–388.
6. Alguliyev R.M., Mahmudov R.Sh. Information addiction problems and ways to fight with them. Express-information, Baku, Information Technology, 2009, 61 p.
7. Young K. Internet addiction: the emergence of a new clinical disorder // Cyber Psychology & Behavior, 1998, vol.1, pp. 237–244.
8. Voiskounsky A.E. Internet: Culture, Diversity and Unification // Javnost – The Public. Journal of the European Institute for Communication and Culture. 1999, vol. VI (4), pp.53–65.
9. Bogdanova D.A., Fedoseev A.A. Attention - Internet / / Open Education, 2010, No2, pp.89–99.
10. Buckingham D., Whiteman N, Willett R., Burn A. The Impact of the Media on Children and Young People with aparticular focus on computer games and the Internet. Centre for the Study of Children, Youth and Media, Institute of Education, London, 2007, pp.77.
11. Lord N. What is a phishing attack? Defining and identifying different types of phishing attacks, http://www.digitalguardian.com
12. Content-filter, http://www.ru.wikipedia.org
13. 7 Windows 10 Security Features & How to Use Them, http://www.microsoft.com
14. Reports in Kaspersky Anti-Virus 2015, http://www.support.kaspersky.com
15. Egorov A. Yu., Igumnov S.A. Behavioral disorders of adolescents, St. Petersburg: Rech, 2005, pp.436.
16. Griffiths M., Hunt N. Dependence on computer games by adolescents // Psychological Reports, 1998, vol.82, pp.475–480.
17. Safer İnternet Programmer, http://www.saferinternet.org
18. http://www.inhope.org
19. UK Safer Internet Centre, http://www.saferinternet.org/united-kingdom
20. Germany Safer Internet Centre, http://www.saferinternet.org/germany
21. Russian Safer Internet Centre, http://www.saferunet.ru
22. The National Strategy for the Development of Information Society in the Republic of Azerbaijan for 2014-2020, http://www.president.az
23. Azerbaijan launched a project entitled "Children's Security on the Internet", http://www.azertag.az