Cyber safety prevention methods for children

Marharyta Melnyk
Doctor of Philosophy, Associate Professor
Department of Radio Engeneering Divices
Odessa National Polytechnic University
ORCID: https://orcid.org/0000-0003-0619-7281

Serhii Yevseiev
Doctor of Technical Science, Senior Research
Department of Cyber Security and Information Technology
Simon Kuznets Kharkiv National University of Economics
ORCID: http://orcid.org/0000-0003-1647-6444

Abstract. *In the of rapid technological development, it is impossible to imagine the life of a modern person without internet technologies. Therefore, it is important not to avoid those innovations, but to use them correctly. In this article, we want to pay attention to the ways of providing the safety of children and middle school children in internet. We want to offer an educational family game board as a tool for the training of cyber security of children.*

Keywords: *cyber security, cyber safety, internet technologies, internet, devices with internet access, digital security*

Introduction

The internet is not as harmful as it might be seen at first glance. Nevertheless, you need to take care of the safety of the child by following some rules of behavior on the Web.

The problem with young users of smart phones, tablets and other devices with internet access is not only that children can accidentally see, read or download something inappropriate at their age, but also because of insufficient life experience and knowledge, they are very vulnerable to the actions of attackers. Even worse: children can be not only the victims but also a scam tool. What to do with this?

Parents are fully capable of providing children (and, therefore, the whole family) with digital security. It is most reliable to apply an integrated approach combining the educational component and software, then there is a chance to protect children from the cyber threats and, at the same time, keep the opportunity for them to enjoy all the advantages of the digital world. Further, we will give some recommendations that will help you to minimize risks. But first, let's figure out what specifically can pose a threat to a child on the internet.

Let's review some of the most common cybercrime scenarios.

Smart House. A growing number of families use internet devices (IoT) at home: smart doorbells, baby monitors with access to the internet, surveillance cameras, and

other devices. But what will happen if fraudsters gain access to them by penetrating the network through children's devices?

Free public Wi-Fi and School Wi-Fi. Parks, fast-food restaurants and other public spaces with free Wi-Fi are a real bait for teenagers who like to hang out in such places after (or instead of) classes [1, 2].

Untrustworthy applications and viruses. You can pick up virus software not only on adult sites. Malicious code can also be hidden in ordinary applications downloaded from P2P resources or even from Google Play which is also used by children.

Phishing emails. Phishing messages are often disguised as official letters or even come from friends whose accounts have been hacked, so it's not always easy to recognize them even for adults. If you open such kind of a letter, you can get very unpleasant software to your gadget that will steal important information or extort the money.

Excessive dissemination of information on social networks. Critical thinking is not the strongest side of adolescents, so they are not always picky about relationships. Children do not think with whom they are "making friends", how much information they share and what excessive openness in social networks can lead to. And the consequences can vary – from easy embarrassment to large-scale internet harassment.

Material and method

Even parents in the families with the most trusting relationships sometimes can't notice the impending danger to the child in time and, moreover, they don't always know how to prevent it.

Here is what parents should pay attention to in order to notice in time that the child has become a victim of cyberbullying/intimidation, humiliation, bullying, physical and mental terror aimed at causing fear and submission in others:

- Restless behavior Even the most reserved student will worry about what is happening and will necessarily betray himself with his behavior. Depression and reluctance to go to school are the most obvious signs that the child is being subjected to aggression.
- Hostility against the internet If the child loved spending time on the internet and suddenly stopped doing it, you should find out the reason. In very rare cases, children are really bored of spending time on the web. However, in most cases, a sudden unwillingness to use the internet is associated with problems in the virtual world.
- Nervousness under receiving new messages A child's negative reaction to the e-mail sound should alert the parent. If your child regularly receives messages that upset him, talk to him and discuss the contents of these messages.

Today the problems of the so-called "internet addiction" (synonyms: internet addiction, virtual addiction) and dependence on computer games ("gaming") are

becoming more and more relevant. The first who came across with them were psychotherapists, as well as companies that use the internet and suffer losses in their activities if employees have a pathological attraction to staying online.

According to Kimberly Young, the harbingers of internet addiction are:

- obsessive desire to constantly check e-mail;
- the anticipation of the next online session;
- increase in time spent online;
- increase in the amount of money spent online.

Recommendation for parents.

And what to do? You should start with a thoughtful conversation with your child: share your concerns, tell about unsafe behavior, give some tips to help him stay safe. At the same time, it is important not to go too far, showing the child that you are driven by anxiety and the desire to protect him, and not the desire to control his life.

It is very important to teach your child not to download malware onto your computer Malicious programs can harm the computer and the data stored on it. They can also slow down the speed of data exchange and even use your computer to spread the virus, send spam on your behalf from an email address or profile of a social network.

Malware collision warning. Install special mail filters and anti-virus systems on all home computers to prevent software infection and data loss. Such applications monitor the traffic and can prevent both direct attacks by intruders and attacks that use malicious applications.

Use only licensed programs and data obtained from reliable sources. Most often, pirated copies of programs, especially games, are infected with viruses. Explain to the child how important it is to use only proven information resources and not to download unlicensed content. Periodically try to fully check your home computers. Regularly back up important data. Try to change passwords time after time (for example, from email) and do not use passwords that are too simple.

What to do if the child is still facing any risks. Establish positive emotional contact with the child, endear him to talk with you about what happened. Tell about your own concern about what is going on with him. The child should trust you and know that you want to understand the situation and help him, and not punish;

Try to listen carefully to the story of what happened, to understand how serious is what happened and how deep it could affect the child;

If the children are upset with something they saw (for example, someone hacked their profile on a social network), or they have fallen into an unpleasant situation (e.g. they spent their own or your money as a result of internet fraud, etc.) – try to calm them down and understand the situation together – what led to this result, what actions of the child were wrong, and where you did not tell them about the safety rules on the internet;

If the situation is related to the violence on the internet in relation to the child, then it is necessary to find out the information about the aggressor, the history of the relationships between the child and the aggressor, to find out if there is an agreement to meet in real life; whether there were such meetings and what the aggressor knows

about the child (real name, surname, address, phone number, school number, etc.), strongly insist on avoiding meetings with strangers, especially without witnesses, check all the new contacts of the child recently;

Collect the most complete information about the incident, both from the words of the child, and using technical means – go to the pages of the site your child attended, review the list of his friends, read the messages. If necessary, copy and save this information – in the future it may be useful for you (for example, for contacting law enforcement agencies);

If you are not sure about the seriousness of what happened with your child, or the child is not open enough with you or is not ready to make a contact at all, or you do not know what to do in such situation. Contact a specialist (helpline, hotline, etc.), where they can give you recommendations on where and in what form to apply if intervention by other duty services and organizations is required (police, for example).

So we also consider it important to mention Karpman Triangle. The Karpman Triangle is the most common model of relationships between people. It was first described by the classic of transactional analysis, Stephen Karpman in 1968. People manipulate each other, depend on each other and get very tired of it. Happiness in such relations is extremely small. Like the forces to make a difference. But there is a way out of this.

Two, three, and entire groups of people can spin in a triangle. But roles in there are always three: a victim, a controller-dictator, a savior. Participants of the triangle periodically change roles, but they are all manipulators and great spoil yourself and loved ones life.

Karpman Triangle using and working in cyberspace. Entry from the Karman triangle is possible. It is important to use preventive measures in order to avoid getting into the triangle.

We know Basic Rules of the safe internet for children:

- do not tell everyone in a row your private information (real name, surname, phone number, address, school number, as well as own photos, family or friends photos);
- do not open email attachments when you don't know the sender;
- do not send spam and "informational dirt";
- do not be rude, nitpick, put pressure – behave impolitely and aggressively;
- do not manage your family's money without the permission of your elders, ask your parents;
- do not meeting the internet acquaintances in real life can be dangerous: a criminal can be hiding behind a pseudonym.

Be careful:

- not everyone writes the truth;
- if you read a lie about yourself on the internet – report it to your parents or guardians;
- invite to chat, play, exchange – check if there is a catch;

- illegal copying of files on the internet it is not good;
- discovered something threatening – don't be afraid to call for help.

Children can:

- use "the nickname" (false name) in correspondence and negotiations;
- respect another user;
- if you use an internet source – make a link to it;
- met on the net and want to meet – take a piece of advice from an adult who you trust;
- open only those links in which you sure;
- the best way to use the internet when there is one of the parents nearby or someone who knows well what the internet is and how to behave in it correctly.

How to protect children from negative information?

Resulting from the development of new technologies in the field of virtual space, including the spread of the internet network, there arose a problem related to the access of minors to information of dubious content and contrary to generally accepted ethics. At present, any person, including a minor, who has knowledge in the field of computer technology, can access data stored on the internet or create his own web resource.

The lack of parental control over the children's use of the internet is one of the reasons for minors to access negative information. As a memo to the parents on the safe use of the internet by children following are the basic rules that will help protect your children from the information of dubious content and contrary to generally accepted ethics:

Rule 1. Parents should know the interests and goals of children who use the internet.

Rule 2. It is recommended that children use the internet in the presence of adults. Access to this information resource should be efficient and safe.

Rule 3. It is necessary to exclude children's access to the internet resources, the contents of which are contrary to the law, that can have a negative impact on minors.

Rule 4. In the case of independent access of children to the internet, parents should control the use of information by minors.

How to limit children's access to negative information on the Internet? To do this, you may need the following set of software:

- a program for parental control, which provides a limitation of screen time, blocking access to sites and applications, as well as the protection of "smart home" gadgets;
- a means of protection against phishing emails and sites that steal personal data, and minimization of the dissemination of information in social networks;
- a tool to protect your smart phone and tablet from email and web threats, as well as from malicious code hidden in applications;

– password manager that will help children (and adults) to create complex passwords and store them in a safe place – even if some of the children's accounts are hacked, the rest will remain protected.

Experimental results

In the era of rapid technological development, it is impossible to imagine the life of a modern person without internet technologies. Therefore, it is important not to avoid those innovations, but to use them correctly. In this work, we want to pay attention to the ways of providing the safety of children and adolescents on the internet.

Educational systems are one of the most dynamically developing types of software, the demand for which in the conditions of development of electronic and distance learning, the introduction of a continuing education system, advanced training, retraining, and digitalization of the educational sphere as a whole is constantly growing. One of the most popular category of educational systems is educational computer games. Environmental friendliness of information and the safety of the internet network should be ensured for all types of activities and occupations of the child (adolescent). We suggest digging into the nature of some presumptions about children and the internet. Some basic myths-speculations are presented in (Table 1).

Table 1. – Basic myths-speculations about Cybersecurity for children

Presumptions	Clarifications	Recommendations
1	*2*	*3*
Being on the internet is addictive.	Those who feel bad in real life go headlong into the games. If you forbid such a child to play, he will simply look for another way to get distracted.	As soon as in real life the child discovers something more exciting, you will not see him at the computer anymore.
To preserve the mental health of the child, it is better to protect him from the Internet.	The internet is an essential part of the modern world. Parents, restricting children from being online, deprive them of the opportunity to meet basic needs, in this case, social. Subsequently, this situation can cause a child's serious psychological problems.	Conduct outreach. Explain that the internet is useful, but can not be a substitute for real life. Parents' own example should be the main evidence.
Virtual friends can replace real friends.	The computer itself does not affect the growth of interpersonal skills. If the child's time to interact with people is spent	In order to gain important communication skills, children need visual and tactile contact with their parents.

1	*2*	*3*
	on the gadget, in the future it will affect family relationships, communication with other children, attitude to oneself and emotional intelligence.	The child must learn speech, recognize emotions and, finally, just spend time with mom and dad at useful games.
Physical health issues are related to internet technologies.	The use of gadgets stimulates low physical activity, problems with posture and overweight.	It is important to limit the time spent with children not only on the internet but also to limit the use of gadgets Give preference to interactive entertainment: let there be more educational applications than entertaining videos.
Sleep and mental health problems associated with the use of gadgets.	With all these dangers, mobile devices have many advantages for children's formation. Gadgets are the realities of our time and there is no escape from them. Therefore, the issues of the interaction of the child with devices should be approached without fanaticism. But do not forget that without reasonable restrictions, gadgets can serve parents and children poorly.	Children should not be allowed to play with mobile devices several hours before bedtime. Do not give your children a device when they are having a tantrum, and replace personal attention with gadgets.

It is important to offer children (teenagers) an alternative, to explain all the advantages and disadvantages. Explain the value of the time they spend on the computer. The easiest way to learn is the study in the form of a game, the most accessible way to explain is a learning game. For children (adolescents) it is important to carry out explanatory work at the stage of acquaintance and in the process of working with internet technologies.

From the point of view of psychology and the formation of personality structure game and imitation is one of the mechanisms of evolution. Therefore, gaming is one of the most effective tools for acquiring knowledge.

Nowadays, in the ascientific literature more and more attention is paid to the use of the game in order to increase the effectiveness of the educational process, but unfortunately, not all teachers are able to correctly use it in teaching.

The disclosure of the importance of gaming activities was developed by such educators and psychologists as L. Rubinstein, D. B. Elkonin, S. Freud, J. Piaget, and others. The role of the game in the growth of the personality and basic mental functions, in self-administration and self-regulation of the personality, and finally, in the processes of socialization underlie on the adoption and use of social experience by a person, as was investigated and substantiated in their works.

Therefore, explanatory work on the use of internet technologies and a game form of cybersecurity training is an effective tool for raising a mentally healthy generation, as well as preventing cyber addiction in adolescents

The game is a type of activity in conditions of situations aimed at the reconstruction and assimilation of the social experience, in which behavior self-management develops and improves. The therapeutic function of the game is to use it for the means of overcoming various difficulties that a child has in behavior, communication, and learning. The game therapy effect is determined by the practice of new social relationships that the child receives in a role-playing game. It is the practice of new real relationships in which the role-play puts the child with both adults and peers, relations of freedom and cooperation, instead of relations of coercion and aggression, ultimately lead to a therapeutic effect. The correction function is the carrying in of positive changes, additions to the structure of the child's personal indicators. In the game, this process occurs naturally, gently. The entertaining function of the game is perhaps one of its main functions. The game is strategically – only an organized cultural space of entertainment for children, where they go from entertainment to evolution.

Educational games are a large group of methods and techniques for organizing the learning process. The main difference between an educational game and just a game is that the first has an essential feature – a clearly defined learning goal and the corresponding pedagogical result. The symbiosis of science and technology always gives a better effect than the use of knowledge in only one area. Therefore, we believe that the development of an educational game that instructs the cyber safety for children is more effective than outreach. The game will include rules and simulate dangerous situations, ways to avoid dangerous situations and safe exits from such situations. The development of communication skills takes place in a playful way. The use of a desktop educational game is an effective tool for both training cybersecurity and improving the communication of children.

The tool for the training of cybersecurity for children

The choice of teaching methods is first of all determined by the content of the educational material and the learning objectives. The learning process forms the proficiency and skills needed in practical work. Therefore, in the learning process the methods that are suitable to bring children and teenagers closer to the real situation should be used first of all. All these requirements are best met by educational and psychological games [3].

The effectiveness of the game form of training has been proven both by educators and psychologists. An educational game is a form of activity of participants

that imitates real situations and helps to find a way out of them. Thus, the child (teenager) gets the skills to overcome difficult situations, learn to avoid them and improves the level of communication.

We want to offer an educational family game board as a tool for the training of cybersecurity of children and adolescents.

The advantages of the game are as follows:

- imitation of a real situation that can change under the influence of various factors;
- solving of complex problems, so by unraveling of the plot there is a dependence of subsequent actions on previous ones;
- the connection between behavior and communication, as it is based on specific behavior, actions;
- collective, group interaction;
- are functional, affect changes in behavioral factors.

This game complex includes: the theoretical part, a description of the situation (case), examples, illustrations, diagrams, questions, answers, and methodological recommendations.

The technology of the game includes possible game modeling – artificial creation of real situations and helping to get out of them, so the children (teenagers) will be able to resist manipulation if such a situation happens to them in cyberspace

The game as a method of constructing the learning process includes the following components:

- adoption of a role;
- game actions;
- game technology.

Educational game is an imitation of real situations, training to get out of them, teaching the rules of conduct in a cyber environment Thus, the educational game of cybersecurity training of children and adolescents can be an effective tool that will ensure security in cyberspace. The educational game on the cybersecurity training for children and adolescents is a unique mechanism for accumulating and transmitting collective experience and knowledge. With regard to the educational process in the game, practical (mastery of the ways of solving important problems) and ethical (digestion of patterns, rules and norms of behavior in various situations) experience is mastered. The active position of its participants finds its behavioral manifestation in the game.

The purpose of replacing a real event with an experiment (artificially constructed behavioral patterns) is education and training [4,5].

The model of the game is implemented, put into action using its rules. The rules reflect the ratio of all components of the game. They can be transferred to the game from the real situation in which the gameplay unfolds, or they can be invented.

Roles are prescribed to players by the terms of the game. Game actions can be set up in different ways: by a scenario, by the leaders (facilitators) of the game, or formed by the players themselves (children, adolescents) in accordance with their

own vision of the situation and the goals set for them. Therefore, the role actions of individual participants in the game can differ significantly from each other.

The leading component of the game is the role and its adoption. A role is a set of requirements, expectations, presented by a situation to a given person, his behavior. The performance of the role supposes the exact reproduction of human activities in a typical model of the situation in cyberspace. The adoption of the role is carried out at the cognitive, emotional and behavioral levels. Adoption is implemented through the appropriation of external traits and norms of behavior, as well as tasks inherent in the role, its execution.

Conclusion

The symbiosis of science and technology always gives a better effect than the use of knowledge in only one area.

Game form of education is the easiest for children to perceive information. By skillfully connecting the rules and situation simulators, we can ensure the cyber security of children.

The development of communication skills takes place in a playful way. The use of a desktop educational game is an effective tool for both training cybersecurity and improving the communication of children.

Board educational game is one of the effective methods of teaching cybrsecurity for children (teenagers).

References:

1. Ніколаєнко С. М. Якість вищої освіти в Україні: погляд в майбутнє / С. М. Ніколаєнко // Світ фінансів. 2006. – № 3(8). – С. 7–22.
2. Гуляева Е. В. Компьютерные игры в жизни дошкольников / Е. В. Гуляева, Ю. А. Соловьева // Психологическая наука и образование. 2012. – № 2. – С. 5–12.
3. Сурмина Ю. П. Ситуационный анализ, или Анатомия Кейс-метода / Ю. П. Сурмина // Київ: Центр инноваций и развития, 2002. – 286 с.
4. Галимов М. Геймификация в обучении: что, как и зачем / М. Галимов// [Electronic resource]. – Access mode: URL: http://freepublicity.ru/gejmifikacziya-v-obuchenii-chto-kak-i-zachem/
5. Белкин Ф. А. Геймификация в образовании / Ф. А. Белкин // Современная зарубежная психология. 2016. – Том 5. – № 3. – С. 28–34. Doi: 10.17759/jmfp.2016050303