

Justyna LIPIŃSKA¹

"NO" SECURITY OF INFORMATION TECHNOLOGY

Using the Internet is inseparably connected with building the awareness of its users, hence the tasks that arise for a modern man in relation to information technologies, especially in terms of online threats. Children are particularly vulnerable. The most common threats include: contact with pornographic content, contact with violent materials, contact with pedophiles, internet addiction, contact with online cheaters, unconscious participation in illegal activities, financial consequences, unconscious disclosure of information. The purpose of the article was to indicate tasks for parents along with identification of dangerous situations affecting children's behavior. Readers will also learn about forms of sexual abuse of children on the Internet and methods of filtering Internet content. The adopted research method is a qualitative analysis supported by the retrospective analysis technique.

Keywords: information technologies, Internet threats, child pornography on the Internet.

1. TASKS OF MODERN MAN TOWARDS INFORMATION TECHNOLOGIES

The intensive development of information technologies is primarily the development of a global computer network – the Internet. It is practically an unlimited source of information, an ideal way to communicate and work. A contemporary man is no longer enough to just find and process information, the ability to select, eliminate and build a coherent image from elements scattered in many areas and resulting from information available on the web is becoming more and more important. The basic problem today is the ability to communicate with other people and the products of their civilization. Therefore, not only an adult but also a small child using Internet resources must acquire and consolidate, throughout their life, certain universal skills. Learning from network information resources is a basic skill of learning how to use Internet resources in technical and logical terms. This skill forces the network user to master more and more ways of communicating using online tools. Communication via the network is not the same as communication in the real world. It requires the acquisition of new language and non-language skills and skills. The third skill necessary to master is the ability to process information on the web. There is information chaos in the network, from which in order to “shell out” one should have ways to filter this information. To be able to possess these skills, it is a must for every human being in the “information society” to meet the tasks posed by information technology. In the “information society”, the focus is above all on openness to new technologies and thus the ability to use them efficiently and the ability to choose. These

¹ Professor Justyna Lipińska, PhD, The Faculty of Management and Command, The War Studies University, I. gen. A. Chruściela „Montera” 103, 00-910 Warszawa-Rembertów; e-mail: j.lipinska@akademia.mil.pl. ORCID: 0000-0001-8233-6971.

tasks become indispensable features of a full and conscious member of the information society. They change our skills but above all change our mentality. For many people, these are great challenges that not only teachers, educators, but most of all parents have to face. These changes occur because children and adolescents require this from adults. In addition, the greater our awareness of the tasks ahead of us, the less unpleasant events can be encountered by children and young people using the resources of the Internet. The competition that parents and teachers involuntarily enter does not tear up today only in the fight against the media but, or perhaps, primarily on the Internet. This internet network creates an environment that modern parents and teachers must learn. In order not to be afraid of him, you should understand them. That is why it is so important.

- realizing that parents and teachers cease to be the main source of information for children and young people,
- realizing that there is competition with the media and computer forms of education, and it is much more difficult than fighting other addictions,
- accepting the fact that the teacher and parent should take on a new role – a guide to the world of information,
- teachers and parents learning counseling in the learning process using new media (<https://szkolnictwo.pl/>).

2. THREATS ON THE WEB

When using the Internet, we are often not aware of the threats it may pose. Despite the fact that we hear about Internet pornography, pedophile gangsters or scammers who are prowling the Internet, it seems to us that this does not apply to us and our loved ones. This is usually due to our (parents and teachers) ignorance of network threats. Therefore, you should be especially attentive on the Internet, especially when children use it.

The purpose of these considerations is to make parents and teachers aware of the importance of teaching children appropriate behaviors, shaping their habits and being sensitive to the dangers of the network.

The most common threats to which children are exposed include:

- contact with pornographic content,
- contact with violent materials,
- contact with pedophiles,
- Internet addiction,
- contact with online scammers,
- unknowingly participating in illegal activities,
- financial consequences (e.g. use of dialers, i.e. programs connecting the computer to the Internet via numbers 0-700),
- unconscious sharing of information (e.g. card numbers, addresses, passwords) (Barabach, http).

Unlike the Internet, the judicial institutions have strictly defined limits of impact, which is associated with the existence of different definitions of illegal content in different countries. In accordance with the law in force in Poland, it is prohibited to publish:

- pornographic content involving a minor, pornographic content related to the presentation of violence or the use of an animal;

- content publicly promoting a fascist or other totalitarian state system or inciting hatred against national, ethnic, racial, religious differences or because of religious denominations;
- content that publicly insults a group of people or an individual because of their national, ethnic, racial, religious affiliation or because of their non-denominational status (<http://statystyka.policja.pl/st/kodeks-karny/>).

In addition, it is unlawful to publicly present pornographic content in such a way that it may impose its reception on a person who does not want it and to present pornographic content to a minor under 15 years of age or to provide him with items of this nature or to disseminate pornographic content in a manner that allows a minor getting to know them.

The vast majority of psychologists are of the opinion that frequent contact of minors with pornography has a profound, multidimensional and harmful effect on them. Pornographic content is a source of experience that surpasses young people's adaptability and provides them with pathological behavior patterns. They shape a distorted and negative image of the world, interpersonal relations (e.g. instrumental treatment of other people), perpetuate a false image of femininity and masculinity. As a result of contact with pornography, eroticism of the child's psyche and its premature sexual arousal, as well as an increase in the level of anxiety in the child, tension, attention deficit hyperactivity disorder, and the occurrence of neurotic and depressive symptoms may occur. The correlation between the frequency of contact with violence and hard pornography and the strength of their impact is well documented.

The more often children in preschool and school age come into contact with violence in films or games:

- the more often he violates the law in adolescence and adulthood;
- the more often the conflict with the law results from the use of violence, the more violent it is, especially when under the influence of alcohol;
- the more often he also uses it in his future family – towards his spouse and children;
- the greater the tendency towards alcoholism, promiscuity, trivialization of cruelty;
- even more so in adult life, women are willing to accept men's violence against themselves and incorporate elements of violence into sexual fantasies and behavior (Wortal Jana Pawła II Wielkiego - Pokolenie JP2, <http://www.jp2w.pl/pl/42118/>).

It is also worth mentioning a number of other threats and examples of dangerous content that children and young people surfing the Internet may encounter:

- cyberbullying - this is violence based on challenging, ridiculing, blackmailing or spreading compromising materials on the network using information and communication technologies (messengers, chats, websites, blogs, SMSs and MMSes). Gemius (2007) research shows that more than half of teenage Internet users in Poland, aged 12–17, have been the victims of any of the above acts of cyberbullying;
- grooming – is the seduction of children by adults via the Internet. “Cybercriminals” mainly use instant messengers and chats to establish a close contact with children. They try to convince children to talk about sex, which can be an introduction to the further trapping and harassment of the youngest users. An adult, often pretending to be the peer of his victim, gradually gains her trust, personal data, photos, and sometimes becomes a “good friend”. He urges the child to watch pornography and

insists on meeting in the real world. When a meeting occurs, the child is usually sexually abused and often becomes a victim of the porn industry;

- content promoting religious movements considered sect;
- content promoting anorexia and bulimia as a lifestyle, not a serious illness;
- content inciting suicide or self-harm;
- content promoting drugs and other stimulants – most often by emphasizing their supposedly healing qualities or indicating that they open man to spiritual reality (<https://www.enisa.europa.eu/publications...>).

3. DANGEROUS SITUATIONS AND BEHAVIOR OF CHILDREN

The appearance of a new medium in the child's life, which is the Internet, can affect his behavior and way of looking at the world. For children, the web is a place where they can find both entertainment and knowledge (although they will usually look for the first one). Here he can also meet new friends. Such versatility of the Internet, abundance of information, potential contacts may affect the child's behavior or even his development.

A very important task for a parent is to pay attention to the behavior of the child who uses a computer connected to the Internet. Sometimes, noticing unusual behavior can prevent unpleasant and even dangerous events. Typical behaviors that can be observed by the parent at home and the teacher at school include such behaviors as:

- the child often talks about a new friend that you have never heard of before,
- the child spends a lot of time on the Internet, and each parting with the computer causes him sadness or anger,
- the child begins to use words that are negatively marked – terms that are directly or indirectly related to violence or sex,
- the child becomes aggressive towards the environment,
- the child talks about his new idol – a super hero who e.g. defeated all enemies,
- the child is contemptuous of their friends who do not use the Internet,
- the child tells strange, imaginary, amazing stories in which the motive is fight or violence,
- the child asks questions related to spheres that have not been of interest to him so far (e.g. questions related to eroticism or sex) Pastuch, http).

4. FORMS OF SEXUAL EXPLOITATION OF CHILDREN ON THE INTERNET²

The internet is currently the favorite site for victims of pedophiles and other scammers. They often impersonate children using chats and instant messengers, which the youngsters love to hang out on. As a rule, a child is trustful and gullible and can be tempted to meet.

A review of the literature related to the dangers of the Internet for its youngest users allows the specification of basic phenomena associated with broadly understood sexual abuse. Those are:

- presenting pornographic material on the Internet,
- producing and presenting child pornography on the internet,
- use of websites by pedophiles for the purposes of communication and exchange of information,

² See: Raport Fundacji „Dzieci Niczyje”: *Pedofilia i pornografia dziecięca w Internecie* – Ł. Wojtasik.

- the use of websites by pedophiles to contact potential victims (<https://depot.ceon.pl/bitstream/handle/123456789/3651/...>).

In accordance with the laws of most countries, presenting pornographic material on the Internet under appropriate conditions is not prohibited. In practice, most of the security of pages containing such content is ineffective, which results in the wide availability of this type of material for the youngest users of the network. This is a serious problem, often raised in debates on the safety of children on the Internet. However, this issue goes beyond the subject of this article and will not be analyzed here. There are two basic threats associated with the phenomenon of child pornography on the Internet:

- (1) children may be involuntary recipients of pornographic content of this nature and
- (2) may also become the subject of pornographic films and pictures (Calcetas-Santos, 2001)

An indirect threat is also caused by the fact that watching child pornography by adults may stimulate them to engage in sexual activity with minors (Jenkins, 2001). The harmfulness of the reception of child pornography by children, and even more the use of children in porn business is obvious. The distinction in such cases of the guilty and aggrieved party seems to be beyond dispute. However, there is some controversy in the situation of the more and more frequently noted phenomenon of intentional access of children to child pornography and their collection of this type of material. According to experts, such behavior is often associated with the fact that the child remains in sexual relations with the adult or is encouraged to do so, and pornographic materials suggested by the perpetrator are to tame them in such a situation. Therefore, a child should be considered a victim rather than a perpetrator. The issue of minors collecting child pornography in circumstances other than those mentioned above is more difficult to resolve, but it is postulated that in no case should children be treated as adults as perpetrators (Taylor, 2002). From a technical point of view, child pornography distributed via the Internet takes the form of text, graphics or movies. Its dissemination takes place via popular network tools enabling data transmission. The popularity of child pornography on the web consists of the following factors (Calcetas-Santos, 2001):

- frequent and easy updating of resources,
- coverage not provided by any other media,
- much cheaper than printing them, publishing digital photos,
- the quality of digital photos and videos, which do not deteriorate over time and as they are sent to others,
- recipients,
- the anonymity of distributors of child pornography and the possibility of avoiding the legal consequences of their actions.

In addition to the wide availability of child pornography, the Internet enables pedophile environments (Spiegel, 2003):

- constant contact with other people interested in sexual exploitation of children,
- an opportunity to discuss your sexual preferences,
- the opportunity to exchange information on how to obtain victims,
- support for your sexual preferences,
- constant access to potential victims,
- the ability to impersonate a potential victim,

- ease of obtaining data on potential victims (e.g. home address, e-mail address, telephone number etc.),
- the possibility of establishing long-term Internet acquaintance for the purpose of subsequent sexual contact with minors.

Pedophile activities on the Internet can be individual or organized into structures known as pedophile rings. Pedophilic vertebrae operate by applying appropriate security measures to prevent access to the structure by unwanted persons. Due to the specificity of the Internet, membership in organized pedophile structures is geographically unlimited.

5. INTERNET CONTENT FILTRATION - CONCLUSIONS

The results of the tests carried out regarding Internet content filtering programs allow the formulation of several general conclusions:

- 1) filtering applications are not able to monitor all Internet content. Their design is based on static solutions, while the Internet is a medium that is constantly changing. Effectively, you can only filter a section of the global network. The main limitation is the multilingualism of websites – the quality of filtering depends, among others, on a set of fixed criteria (keywords), the number of which is practically unlimited,
- 2) filters are not able to intelligently recognize the context and graphics. Illegal or harmful content can be mislabeled, placed in a neutral context, or described using neutral keywords. At the same time, the filtering application can block educational portals or encyclopedias due to the fact that passwords related to human sexual development will be identified by it as prohibited content,
- 3) filtering programs do not sufficiently recognize the content of Web 2.0 – social networking sites, blogs, photoblogs and portals containing music and movie files,
- 4) most applications do not contain a list of blocked categories, which may make it difficult for administrators (parents, guardians, teachers) to configure the program, which is desirable for the good of the child,
- 5) it is good practice to create independent settings profiles for different users, which gives the administrator the opportunity to modify them (e.g. adjustment to the child's age) and allows him to better control the activity of individual users,
- 6) there is no universal, perfect technical solution that could replace a parent / teacher in the process of raising a child and learning to use the Internet carefully; in the absence of proper education, the effectiveness of the filtering application is significantly reduced – especially for older children,
- 7) the filtering program is not able to convince the Internet user to avoid dangerous or laid-back online behavior, because a young Internet user does not necessarily have to be aware of the scale of potential threats,
- 8) an important element of the filtering application is the correct description of the page blocking message, which should perform not only a deterrent but also an educational function.

Using filtering applications can help you better protect children from unwanted and unwanted content on the Internet. Parents should use filter programs and at the same time be aware of what content or people their child may encounter while surfing. That is why they have the greatest responsibility for the online education of children. Parents should accompany children in the process of learning the Internet, sensitizing them to threats, and teaching them responsible and ethical behavior. They can conclude a type of “contract” for

using the Internet with their child, which will be the basis for shaping good habits (examples of contracts can be found at www.dzieckowsieci.pl). Parents should not, however, interfere excessively in the way a child uses the web. It should also be remembered that the advantages of the Internet outweigh its disadvantages, and the child's curiosity is natural.

Effective protection of children and young people against harmful and illegal content requires support from government institutions, schools and internet service providers. On April 11, 2007, the Sejm adopted a new law, which provides, inter alia, introduction of regulations regarding the problem of protecting children against content that may pose a threat to their proper mental and moral development.

REFERENCES

Barabach, M., www.junior.dialog.

Calcetas-Santos, O. (2001). *United Nations Documents Index: April-June, Vol. 4, Edition 1, Part 2*.

<http://statystyka.policja.pl/st/kodeks-karny>.

<https://depot.ceon.pl/bitstream/handle/123456789/3651/Toczyski-Jak-bardzo-niebezpieczny-jest-internet-2008.pdf?sequence=1&isAllowed=y>.

<https://szkolnictwo.pl/>.

<https://www.enisa.europa.eu/publications/CyberBullying%20and%20Online%20Grooming>.

Jenkins, P. (2001). *Child Pornography on the Internet*, Access on the internet: http://www.ncdsv.org/images/COPS_Child-Pornography-on-the-Internet_5-2006.pdf.

Pastuch, J., www.junior.dialog.

Raport Fundacji „Dzieci Niczyje”: Pedofilia i pornografia dziecięca w Internecie – Ł. Wojtasik. Spiegel, J. (2003). *Sexual Abuse of Males: The SAM Model of Theory and Practice*. NY: Brunner-Routledge.

Taylor, M. (2002). *The role of cognitive distortions in paedophilic offending: Internet and contact offenders compared*. Access on the internet: <https://www.tandfonline.com/doi/abs/10.1080/10683160601060564?scroll=top&needAccess=true&journalCode=gpcl20>.

Wortal Jana Pawła II Wielkiego – Pokolenie JP2, <http://www.jp2w.pl/pl/42118/>.

DOI: 10.7862/rz.2020.mmr.4

The text was submitted to the editorial office: March 2020.

The text was accepted for publication: March 2020.

