Introduction of Cybersecurity in the Educational System

Andreea DINU
National Institute for Research and Development in Informatics – ICI Bucharest
andreea.dinu@ici.ro

Abstract: The Internet has become extremely used, representing an essential tool in society, in all areas of activity, especially in educational systems, by students. Nowadays, the main trend of the society's evolution is the transposition of as many activities as possible in the online environment. Due to the COVID-19 epidemic, most of the learning activities were carried out on dedicated online platforms. Thus, cybersecurity has become an important aspect of daily activities due to the frequent cyber threats to which society is exposed. Recently, there have been many cyber incidents, especially among students because their access to information and methods of defense against these cyber-attacks are minimal or non-existent. This paper will present the current situation regarding general knowledge in the field of cybersecurity and will discuss the current situation in educational institution. Also, some solutions that aimed at raising awareness of the need to introduce the concept of cybersecurity and defense methods against cyber-attacks will be presented.

Keywords: Cybersecurity, Educational system, Educational institutions, Society, Students.

INTRODUCTION

In the last ten years, the time of using the Internet and online communication methods has increased exponentially, being used by various groups of people, from the elderly to children. In Romania, due to the epidemic with COVID-19, the educational system had to make a change, this consisting in carrying out activities in the online environment on e-learning platforms. This has led to the need to train teachers, parents and children in the use of video conferencing platforms such as Zoom, but also learning platforms such as Microsoft Teams, Google Classroom, etc. Also, major changes were made in the methodology of teaching and evaluating students. These actions have led to a much greater exposure to the cyber threats of all those involved in education, especially students.

Every day, children are exposed to threats in the online environment and it is necessary to inform them through a simple and intuitive method, which explains what they need to do to prevent dangers. The education system should consider the introduction of the concepts of cybersecurity and methods of defense against cyber threats, representing an academic environment that can easily disseminate information on a large scale. Due to the frequent use of the Internet by students, cyber attackers have developed many ways to infiltrate their systems and carry out malicious activities. At the same time, the parents of the students are not aware of the dangers in the online environment. They have various occupations, in different fields of activity and in most cases, they are not informed of the threats they may encounter in the online space. Attacks can occur from the most common activities such as accessing links received by email, browsing shopping sites, accessing documents on learning platforms and the list goes on.

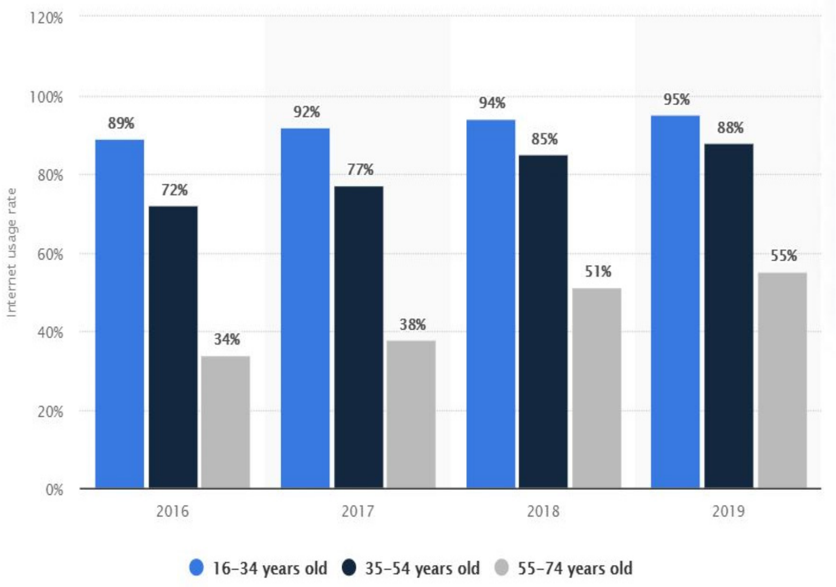


Fig. 1:Internet usage rate in Romania from 2016 - 2019, by age group [https://www.statista.com/statistics/1185593/romania-internet-usage-by-age-group/]

It has become clear that the Internet is constantly increasing the vulnerability of children to a large number of risks. In Romania, the most common problems in the online environment are harassment, abuse and blackmail. These problems can significantly affect the mental health of students, manifested by isolation and refusal to communicate with others. The information posted on the internet cannot always be deleted, and often it is used against us, by attackers in order to generally obtain money, but also other advantages.

POSSIBLE CYBER THREATS AND WAYS OF CYBERBULLYING

It is well known that in recent times cyberbullying and online threats have grown exponentially and information campaigns about them are extremely poor. The attackers use the most advanced methods so that they cannot be detected. In Romania, attacks have been observed that are more frequently used than others, as follows (CERT RO, 2016):

- **Drive-by exploits** - it exploits the existing vulnerabilities of the operating system and, by accessing websites, it can install malware through the vulnerabilities of the browser or computer.
- **Code injection** - this type of threat includes well-known attack techniques against web applications, such as SQL Injection (SQLi), cross-site scripting (XSS), cross-site request forgery (CSRF), Remote File Inclusion (RFI) etc. Attackers who generate such an attack try to steal data and accounts credentials, take control of the web servers or facilitate malicious activities through the exploitation of web application vulnerabilities.
- **Denial of Service** - an attempt to affect the availability of some computer or electronic communications systems / services.
- **Phishing** - a form of online scam that involves the use of specific techniques for manipulating the identity of some people / organizations to obtain some material advantages or confidential information.
- **Spam** - unsolicited electronic messages, often of a commercial nature, that advertise for products and services, being used by the e-marketing industry and by site owners with indecent content. Usually, spam

messages are sent by computers infected with Trojans, which are part of a botnet (a network of compromised computers used to send spam, or attacks on websites without the knowledge of computer owners). Spam messages, while not a malicious program in themselves, can include attachments containing such programs, and send users to dangerous websites.

- **Identity theft** – it is a real threat in the online environment that gets worse every day. Access credentials or personal data are today the target of the attackers. Once in their possession, the attacker can make fraudulent transactions (especially financial) or obtain confidential data.

These types of threats are present daily in the activity of students in the online environment. Also, another specific and common class of threats among students is cyberbullying. Cyberbullying is represented by activities of aggression, threat and humiliation of a person through technology. Every personal information, picture or video designed to hurt or embarrass someone else represent a tool for cyberbullying. (Ben-Joseph, 2018) The most common threats in this class, which are found on most online platforms used by students are (Williams, 2015):

- **Flaming**—writing content intended to evoke negative thoughts and feelings.
- **Harassment**—creating and sending offensive messages continuously, in order to scare the targeted person.
- **Denigration** - spreading or posting false information in order to damage the image of a person.
- **Impersonation** - using someone else's identity in online environment in order to ruin the relationships and to harm the targeted person.
- **Outing and Trickery** – force someone else to share private pictures, videos or messages in order to embarrass him/her.
- **Exclusion** – sending direct or indirect messages to exclude the targeted person from a group or from an activity.
- **Cyberstalking** - repeatedly sending threatening messages to harm the safety of the victim.

All these threats can affect students' lives, having negative effects on their behavioral and social development. As a result of cyber aggression, they may suffer from depression, loneliness and may have serious problems with confidence, self-esteem, adaptation and integration into the team. Also, some attacks such as sexual assault, discrimination and online threats can have much more serious consequences, which are crimes that can be punished in accordance with the law (Williams, 2015).

THE CURRENT SITUATION IN EDUCATIONAL INSTITUTIONS

Educational institutions have begun to use online methods more and more frequently for conducting classes. Due to the pandemic with COVID-19, the structure of the subjects was adapted to online teaching variants, using online grid tests, electronic reports, watching videos that explain the concepts of a subject, as well as teaching lessons on graphics tablets. Currently, within the education system there is no method by which students, parents and teachers are informed or taught how to avoid and retaliate against cyber-attacks.

The learning and teaching methodology are structured in compulsory classes and in optional classes, which are generally chosen according to a predefined list. Cyber security can be an optional subject in Romanian schools and high schools, which can be taught by computer science teachers of the respective institutions or by students in the IT field who would be willing to enter the educational system and make their skills and knowledge known. The concepts of cyber security required for students can be easily structured on the current approach of the courses, including modules of theory and practice, with a content friendly and adapted to the age of the students. The program of a cybersecurity course can be developed by a knowledgeable working group that can consist of cybersecurity experts, psychologists and teachers (Suciu, Piciorus, & Imbrisca, 2012).

It is essential to be aware of the need for basic knowledge in the field of cyber security, for students, as well as for teachers and parents. They can also benefit from a module dedicated to them in order to learn how to protect themselves and their children from cyber threats that are becoming more real and obvious. These problems can be taken seriously by the population only if their representatives are entities that have a great impact on society, influencing its development.

The study conducted by the University of Bristol (Pencheva, Hallett, & Rashid, 2020) presents barriers encountered when introducing cyber education in secondary schools. This study was based on a series of workshops with teachers and children aged 12-16. Three interactive workshops were organized, where participants were encouraged to debate and discuss cybersecurity topics. The workshops had an average of 21 participants, most of them teachers and educators. These were supported by the researchers involved in the study, who summarized the events and conclusions of the workshops.

The workshops had topics such as the level of knowledge in cyber security, identification of malicious practices, exemplification of pedagogical methods and presentation of views on cybersecurity education. Following these events, the following needs were identified for the application of the concept (Pencheva, Hallett, & Rashid, 2020):

- We need to diversify young people's cyber security knowledge by providing substantial information.
- Parents and teachers should use appropriate pedagogical practices for children.
- We need to better promote career prospects in cybersecurity.
- We need to help educational staff teach cybersecurity concepts.
- We need to provide appropriate and useful materials for teaching cybersecurity.

Following this study, in addition to the barriers mentioned, multiple benefits were also discovered. Firstly, this will encourage and coordinate students to choose a profession in the field of cyber security, where trained and experienced people are currently needed. Secondly, collaboration between students, teachers, and parents on cybersecurity can be a way to tighten relationships, with students feeling more comfortable discussing issues with teachers or their parents. Communication channels for incident reporting can also be promoted. Cyber security in the educational institutions brings an opportunity for students with technical thinking and raises awareness for all involved. Students will be able to act in a safe manner in the online environment and will be able to position themselves for jobs in the field of cyber security. Bringing cyber security in secondary schools is a necessity for online safety and child development (Pencheva, Hallett, & Rashid, 2020).

TEACHING METHODS

When students have been victims of online abuse, they tend to shut themselves in and not tell what happened to them. This often comes from the fact that they are afraid that they will be scolded or punished, or that they are ashamed of what they have lived and do not want to be laughed at. In most cases of abuse, the victim considers that the situation they are in is to blame. Both victims and those who feel threatened by these abuses should consider the following (Williams, 2015):

- **Communicating the problem** - presenting the situation of an adult that the student trusts can help a lot to stop bullying or detect it. Adults can be parents, family, school counselors or teachers.
- **Avoidance and ignorance** - ignoring bullies is the best method for taking away their power, but sometimes it is very hard to concentrate on the good things.

- **Refrain from answering** - sometimes it is better to take a break from everything that means online so as not to be tempted to answer or consume yourself.
- **Report bullying** – cyberbullying is taken seriously when it comes to social media environment. All the social media applications like Facebook, Instagram, Linkedin and so on have the option to report any kind of harmful activity in the online space.
- **Block the bully** – most of the applications have all the necessary settings to block the users, who are doing malicious activity.
- **Online security** - it is recommended that passwords be different from account to account and be changed as often as possible. Also, 2-factor authentication is a helpful tool for protecting your identity.

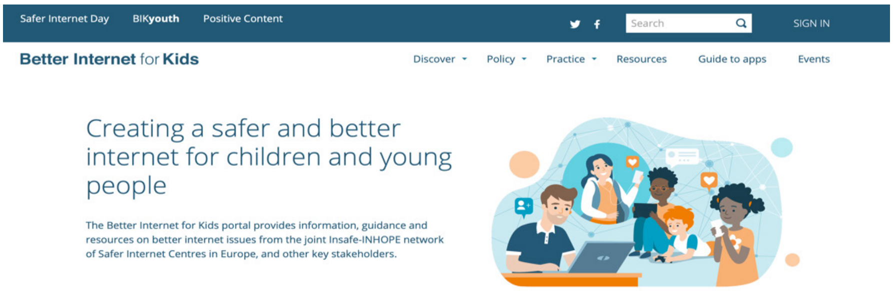
Also, the Cyber4Kids series of episodes, implemented by certSIGN, comes as a solution in educating children in the field of cybersecurity. They offer a weekly video on a topic of cyber security, for children to understand. At the same time, in addition to the good practices that children learn, they also offer a series of good practices for parents, which consist of basic knowledge in online security (certSIGN, 2021).

The educational episodes address the following topics:

- Episode 0 - Cyber City
- Episode 1 - Mobile Games
- Episode 2 - Personal data
- Episode 3 - False Identities
- Episode 4 - Dangerous Links
- Episode 5 - The Internet does not forget
- Episode 6 - Cyberbullying
- Episode 7 - Wi-FI or not?
- Episode 8 - Magic Passwords

***Fig. 2:**Cyber4Kids solution [https://www.certsign.ro/ro/cyber4kids]*

Internationally, Better Internet for Kids is an initiative of the consortium between the European Commission, Insafe and INHOPE in order to provide a portal that provides information and resources for the safest use of the Internet. This project has been adopted by 31 countries, including Romania.



Creating a safer and better internet for children and young people

The Better Internet for Kids portal provides information, guidance and resources on better internet issues from the joint Insafe-INHOPE network of Safer Internet Centres in Europe, and other key stakeholders.

Fig. 3:*Better Internet for Kids Platform*

At national level, this initiative has been implemented by Save the Children Romania, since 2008, and currently coordinates all three components of the program (Better Internet for Kids, 2020):

- Awareness Centre

Description (Better Internet for Kids, 2020): "The Ora de Net project promotes the safety of the Internet among children, parents, teachers and Romanian specialists by creating public awareness campaigns, by offering information sessions, tools and by improving the educational methods used in schools and also by proposing policies. and better legislation in this regard. The project also aims to combat illegal or harmful content and internet-related crimes (sexual abuse of children) and encourage the responsible use of the Internet and new communication technologies."

- Helpline

Description (Better Internet for Kids, 2020): "ctrl_AJUTOR is a line of communication that can be accessed by children, adolescents and parents when they encounter difficult situations in the online environment."

- Hotline

Description (Better Internet for Kids, 2020): "esc_ABUZ is a reporting service, a civil point of contact which provides its users with the opportunity to inform competent authorities, while keeping their anonymity, about child sexual abuse images they might encounter online. The hotline, esc_ABUZ, is a component of the Safer Internet Project that was taken over by Save the Children in 2015, from its consortium partner FOCUS – Centre for Missing and Sexually Exploited Children. In October 2015, the Romanian hotline also became a member of INHOPE, a global network that brings together 46 member hotlines with the aim of leading the fight against child sexual abuse material (CSAM) online."

According to Better Internet for Kids, since 2008, the Safer Internet Programme in Romania has achieved a number of relevant and important results (Better Internet for Kids, 2020):

- 486,000 children and 128,000 adults (parents and teachers) were involved in direct educational activities.
- 7,400 children, parents and teachers benefitted from counselling and advice related to internet safety issues.
- Over 9,100 reports of illegal content were received, processed and send to the relevant authorities.
- The first guide related to online safety in Romania was developed and launched alongside the Ministry of Education.
- 10,000 young people and teachers were involved in the Ora de Net volunteering programme.
- Over 3,600 educational institutions in Romania involved in collaborations and educational initiatives.

- 260 specialists in child protection across the country were trained.
- The first accredited training course for teachers related to the creative, useful and safe use of internet was created, with 104 teacher trainers across the country being involved in the activities.
- Multiple summer schools were organized and attended by over 200 children from Romania and 11 other European countries, who became ambassadors of Internet safety.

CONCLUSIONS

It is obvious that the current trend is to carry out all learning activities in the online environment. This has been done easily lately, but no one has raised concerns about the dangers that exist in cyberspace. It is the responsibility of the online platforms to develop methods and practices to ensure the security of systems, but also end users must comply with certain rules and good practices to contribute to the cyber security of the online educational ecosystem. All categories of people involved need cyber education, especially students, who access an extremely large number of resources on the Internet. They must recognize a risk or a cyber-attack and associate a mitigation method for the situation encountered. Students also need adult support to report attacks and abuse they have been or may be subjected to. It is crucial to be aware of the need in education about the phenomenon of cybersecurity and the existing dangers in cyberspace. This awareness campaign must be supported by the entities that have a significant impact in the development of education and society. The introduction of cyber security concepts in schools or through other educational methods can bring an evolution in the current educational system, thus increasing the level of education of the population.

REFERENCE LIST

Ben-Joseph, E. P. (2018). Cyberbullying. Retrieved from https://kidshealt.org: https://kidshealth.org/en/teens/cyberbullying.html

Better Internet for Kids. (2020, May). Romanian Safer Internet Centre. Retrieved from https://www.betterinternetforkids.eu/sic/romania

CERT RO. (2016). Generic threats to cyber security. Bucharest, Romania.

certSIGN. (2021). Cyber4Kids. Cyber education for children. Retrieved from https://www.certsign.ro: https://www.certsign.ro/en/cyber4kids

Pencheva, D., Hallett, J., & Rashid, A. (2020). Bringing Cyber to School: Integrating Cybersecurity Into Secondary School Education. IEEE Security & Privacy, 68-74.

Suciu, M.-C., Piciorus, I., & Imbrisca, C. I. (2012). Intellectual Capital, trust, cultural traits and reputation in the Romanian education system. The Electronic Journal of Knowledge Management, 13.

Williams, L. (2015). Cyberbullying & Cyber Threats to Young People. Retrieved from https://nonprofitrisk.org/: https://nonprofitrisk.org/resources/articles/cyberbullying-cyber-threats-to-young-people/