Cyber Security in Education

Nebojša Stanković and Vesna Ružičić *
University of Kragujevac, Faculty of Technical Sciences Čačak,
Department of Information Technologies, Čačak, Serbia
*vesna.ruzicic@ftn.kg.ac.rs

Abstract: *This paper presents an analysis of basic knowledge about cyber security in the education of high school students (from the first to the fourth grade of high school) and undergraduate students. The focus of the research is determining knowledge about cyber security, as well as identifying the desire of respondents to learn more about cyber security. The respondents were students of the Gymnasium and Technical School in Čačak and undergraduate students of the Information Technologies study program at the Faculty of Technical Sciences in Čačak, University of Kragujevac. An analysis of the conducted research on cyber security in education was carried out. Based on the results of the research, a discussion was given and conclusions were drawn in order to improve knowledge about cyber security in education.*

Keywords: *cyber security; education; survey.*

1. INTRODUCTION

Today's children have been surrounded by the Internet since childhood and have absolutely no fear of it, while, on the contrary, modern technologies cause fear in many adults. The fear of the dark, which has been characteristic of man since the paleolithic, is quite rational: our distant ancestors knew that if they went out into the forest at night, they could very likely be eaten by predators. What happens when you go online?

Children should be told about threats on the Internet, because the number of cybercrimes, is constantly increasing from year to year. Children should be taught to be "correctly afraid of the Internet" - that is, based on the knowledge of how the Internet works and how criminals can act, what stupid things they can do out of their own ignorance, and how to avoid it. The main thing that children need to understand and remember is that it is not the technologies themselves that are dangerous, but the people who use them for unscrupulous purposes. In the course of technological progress, only the tools of criminal change (improve), while their human nature remains unchanged.

New technologies are spreading so fast that textbooks and educational programs have a hard time keeping up with them, it has learned on the fly. Undergraduate students mainly use the Internet to solve the most primitive tasks - to communicate on social networks, watch videos, and much more. Just because students are constantly online doesn't mean they have a proper understanding of how to best use digital tools. Without a doubt, the digitalization of educational institutions is inevitable.

Clearly, cyber security for students is a growing concern. Do students need strict supervision when using digital devices? Do they need to be taught basic cyber security skills as early as possible? What is the students awareness of basic cyber security knowledge? These are the questions that need to be answered.

This survey aims to survey youth aged 15 to 22 to identify their knowledge and awareness of cyber security. A survey was developed on the topic "Cyber Security". 290 students of the Gymnasium in Čačak and the Technical School in Čačak and 96 undergraduate students of the Information Technologies study program at the Faculty of Technical Sciences (FTN) in Čačak, University of Kragujevac participated in the survey.

The aim of this paper includes the following:

- Investigate the basic knowledge of cyber security among students of the High School in Čačak, the Technical School in Čačak, and undergraduate students of the IT study program at the FTN in Čačak, University of Kragujevac;
- Identification of desire for respondents to learn more about cyber security.

2. RELATED RESEARCH

The ability to prevent successful cyberattacks on a nation's critical infrastructure depends on the availability of a skilled cyber-literate workforce, and thus an education system that can build such capabilities. Initiatives should include strengthening educator training and cybersecurity academic programs, as well as championing research (and development) capabilities and cybersecurity awareness. Recent revisions in the

higher education system of Ecuador and India offer a timely opportunity to advocate for the improvement of academic cybersecurity competencies [1,2].

Cyber security is of increasing importance due to the increasing reliance on digital equipment and software to manage our daily lives, including the transmission and storage of personal information. Research shows that an effective security awareness program is one of the most important steps toward increasing cybersecurity. The authors of study [3] began to monitor the current level of safety awareness among students and high school students in order to develop a module that will help raise their awareness.

There is a problem that internet users are still not aware of online risks. In one study, respondents were involved in the development of educational videos related to cyber risk topics using a storytelling approach. The participants in this study were teachers who were pursuing a master's degree in resource and information technology. The researchers came to the conclusion that it is of great importance to take into account the experience of the respondents, when planning and developing digital stories about cyber risks [4,5].

Despite the fact that the Internet has a positive effect on people's lives, there have been negative problems related to the use of the Internet. The authors found in their research that the level of awareness among Internet users is still low or moderate. One of the vital measures that should be taken is nurturing the knowledge and awareness of Internet users from an early age, i.e. from early childhood. Young children, especially, must be educated to operate in a safe manner in cyberspace and to protect themselves in the process. In the paper, the researchers analyzed why it is so critical that modern undergraduate students are educated about the risks associated with cyberspace. The researcher's proposal is to discuss how cyber security education can be implemented in schools through several strategies [6].

Awareness of cyber security is not only knowledge but also the transformation of learned things into practice. It is a continuous process that needs to be adjusted in subsequent iterations to improve usability as well as maintainability. This is only possible if the cyber security awareness program is reviewed and evaluated in a timely manner. The review and evaluation of the awareness-raising program offer insight into the effectiveness of the program on the audience and the organization, it is an invaluable piece of information for the continuous improvement of the program [7].

3. RESEARCH ORGANIZATION

This research uses a survey as a data collection tool. The survey was organized in such a way as to identify the level of knowledge about the cyber security of the students of the Gymnasium in Čačak, the Technical School in Čačak, and students of the Information technologies at the FTN in Čačak, University of Kragujevac. Research data were collected using an online survey.

The questions were created in order to achieve the previously mentioned objectives. The survey consists of 20 closed-ended questions. The other questions were demographic questions. The estimated time for filling out the survey is 15 to 20 minutes.

Questions are grouped into topics for easier identification, namely: private cyber security, cyber security knowledge, and cyber security in education. The questions were adapted to suit the age group of the respondents. In this paper, the questions of what knowledge about cyber security the respondents have been analyzed.
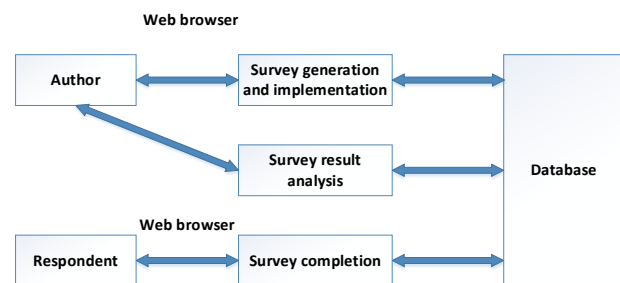
Figure 1 shows a schematic view of the planned research.

Figure 1. *Planned research*

4. RESULTS AND DISCUSSION

In order for respondents, students of the Gymnasium in Čačak and the Technical School in Čačak and students of the Information Technologies study program at FTN in Čačak, to be able to access the survey, a link to the survey was created using Google docs, and then distributed to them. The survey lasted for three months before it was closed, a total of 386 valid respondents completed the survey with no missing data. Other respondents missed the survey or left some questions blank, so they were filtered and deleted. Therefore, a total number of 386 respondents, 290 pupils, and 96 undergraduate students were used for this analysis.

4.1. Demographic data

Demographic data include age and gender, respondents are divided into two age groups:

- Group A: high school students in the final year, i.e. 4th year (born in 2003) and students (born in 2000, 2001, and 2002);
- Group B: first, second and third-grade high school students (years of birth 2004, 2005, and 2006).

Figure 2 shows the number of respondents by gender and age.
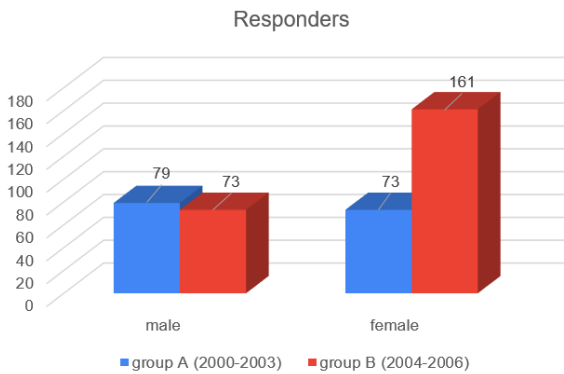
Responders

Figure 2. *Research participants by gender and age*

A total of 152 male respondents and 234 female respondents participated in the research. The number of men is similar in both groups, in the group of older respondents (group A - from 2000 to 2003) the number is 79, while in the group of younger respondents that number is 73 (group B - from 2004 to 2006), while the number of female respondents in group B is more than twice as high as in group A (161 compared to 73). Figure 2 shows that in age group A, men and women are equally as likely to learn or respond to cyber security awareness surveys (79 and 73). In the younger strict group (group B), the number of female respondents is twice as high as the number of male respondents (161 and 73), from which we can conclude that female respondents aged 2004-2006 are more interested in cyber security, that is, they want to learn about this issue.

4.2. Cyber security knowledge

The question "Do you consider yourself knowledgeable about cyber security?" was asked to find out the current level of awareness of students. Figure 3 shows the statistics of respondents' responses to this question.

Do you consider yourself knowledgeable about cyber security?
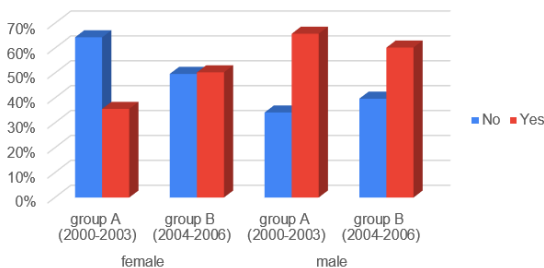
Figure 3. *Answers to Cyber Security Knowledge*

Figure 3 shows that among male respondents, almost two-thirds (63.2%) of students have some basic idea of what cyber security is, and this percentage is the same for both groups (65.8% and 60.3%). A little less than 50% of female respondents (45.7%) were informed about cyber security, while among younger students (group A) as many as 64.4% of them were not informed about cyber security, which confirms the conclusion

about the greater interest of female students of this age group. groups.

With the question "Did you know the difference between using HTTP and HTTPS protocols?", the respondents had an additional explanation of what is the primary difference between these two protocols, so that they could confidently answer (Yes/No) to this question. Figure 4 shows the respondents' answers to this question.

Did you know the difference between using HTTP and HTTPS protocols?
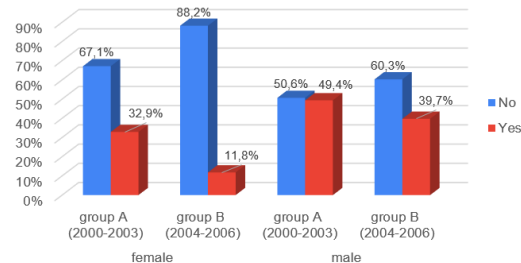
Figure 4. *Answers to the question about the difference between HTTP and HTTPS protocols*

A very small percentage of female respondents (81.6%) know the difference between HTTP and HTTPS protocols, while even 88.2% of female respondents from the younger group B do not know the difference between these two protocols. In men, the results are better, 44.7% of them know the primary difference between these two protocols, while almost 50% of group A men (50.6%) do not know the difference.

To the question "Did you know what (2FA) is and do you use it?", respondents could choose one of the three offered options: I do not know; I know what it is, but I don't use it; I know what it is, and I use it. As with the previous question, there is an explanation of what Two-Factor Authentication (2FA) is. Figure 5 shows the answers to this question.

Did you know what Two-Factor Authentication (2FA) is and do you use it?
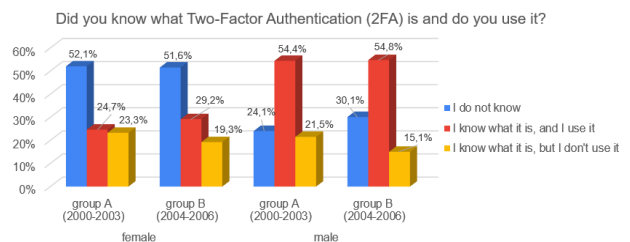
Figure 5. *Answers to the question about Two-Factor Authentication*

As with the difference between the two protocols, and with the question about Two-Factor Authentication, female respondents are much less familiar than men with this method of protection, I not know was answered by 51.7% of women, while the percentage of men was 27 %. An almost equal number of men from both groups (54.4% and 54.8%) know what 2FA is and use (I know what it is, and I use it) this protection process.

To the question "Did you know the meaning of the term phishing by now?" Have you been a victim of "phishing?" respondents could choose: I know what that means, I was not a victim; I know what that means, I don't know what that means, I wasn't a victim; I don't know what that means, I was a victim. The concept of fishing was also explained to the respondents. The answers to this question are given in Figure 6.
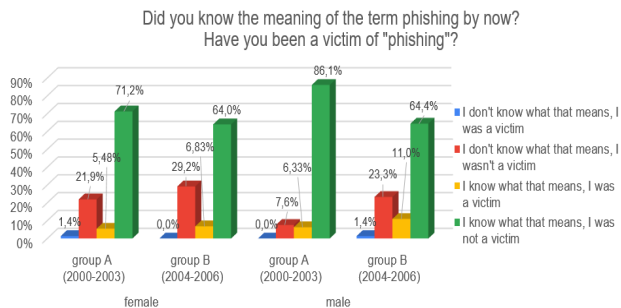

Figure 6. *Answers to the question about phishing*

Respondents of both sexes are familiar with the concept of phishing, for men that percentage is 84.2%, while for women it is 72.6%. Among them, the youngest male students (11.0%) were most exposed to phishing. A total of two people were exposed to phishing without knowing it was phishing.

To the question "Do you want to learn more about cyber security?", a large percentage of respondents declared that they want to learn more about cyber security, women slightly more than men, 75.2% compared to 66.5%. Figure 7 shows the answers to this question.
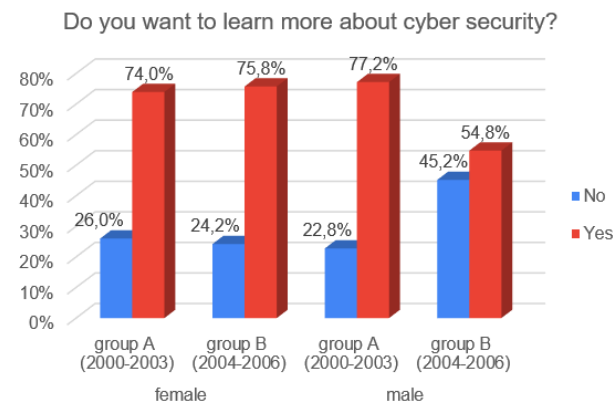

Figure 7. *Answers to the question of whether respondents want more information about cyber security*

To the question "At what age, in your opinion, can children register on social networks?" respondents could choose 4 ages: I can even 9 years ago; from 10 to 12 years; from 13 to 15 years old; over 15 years. The answers are given in Figure 8.
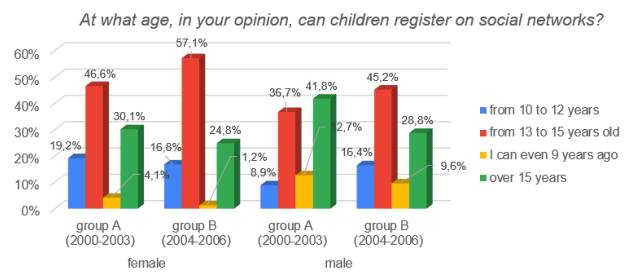

Figure 7. *Answers to the question of when children can register on social networks*

Respondents believe that the age of 13 to 15 is the best age for registering on social networks, only the male respondents of group A (younger students) believe that the limit should be moved to 15 years. A higher percentage of male than female respondents believe that children can register on social networks even before the age of 9 (11.2% compared to 2.1%).

5. CONCLUSION

Pupils and students need to understand cyber security and the most effective way to promote understanding is through active learning. Although pupils and students develop a high level of awareness of some cyber security issues, such as cyberbullying, sharing of personal information, and online banking, little information is given to them about other cyber attacks.

School administrations can establish cyber security organizations, such as various educational workshops, student clubs, or councils in the school. In this way, pupils and students can receive guidance from their teachers to learn more about cyber security. According to [8], students will learn how to navigate the learning management system. It is very important that teachers, parents, and the Government be more proactive in educating students about these areas.

Media, such as television and radio, must also play an important role in educating children through cyber security campaigns because such campaigns are more interactive and interesting for students to understand. Security awareness raising is one strategy that can promote cyber security education in school.

Based on the analysis of the research results, the following conclusions were established:

- it is very important to protect children through cyber security education,
- it is important that high school and college students are aware of the potential risks they face when using internet communication, such as social media, chat and online games.

There are several challenges to cybersecurity education. These include the level of teacher knowledge, lack of teaching expertise, funding, and resources. It is of great importance for all relevant parties, including teachers, parents, peers, and the Government, to work together to find the best

solution to protect of high school students and undergraduate students from cybercrime and cyberbullying, through cyber safety education in schools.

REFERENCES

[1] Frankie E. Catota, M. Granger Morgan, Douglas C. Sicker, (2019). *Cybersecurity education in a developing nation: the Ecuadorian environment*, Journal of Cybersecurity, Volume 5, Issue 1, 2019,

https://doi.org/10.1093/cybsec/tyz001

[2] Garba, A., Siraj, M., Othman S.H. & Musa M.A. (2020). *A Study on Cybersecurity Awareness Among Students in Yobe State University, Nigeria*: A Quantitative Approach. *International Journal on Emerging Technologies,* Vol. 11, No 5, pp. 41–49*.*

[3] Yesem Peker, Lydia Ray, Stephanie P da Silva. (2018). *Online Cybersecurity Awareness Modules for College and High School Students*, Conference: 2018 National Cyber Summit (NCS), June 2018.

DOI: 10.1109/NCS.2018.00009

[4] Fariza Khalid, (2020), *Teachers Experiences in the Development of Digital Storytelling for Cyber Risk Awareness*, (IJACSA) International Journal of Advanced Computer Science and Applications, 2020.

[5] Mai, P.T & Tick, A. (2021). *Cyber Security Awareness and Behavior of Youth in Smartphone Usage: A Comparative Study between University Students in Hungary and Vietnam*. *Acta Polytechnica Hungarica*, *Vol. 18, No. 8*, 67–89. DOI: 10.12700/APH.18.8.2021. 8.4

[6] Rahman N. A. A, Sairi I. H., Zizi N. A. M., and Khalid F., (2020). *The Importance of Cybersecurity Education in School,* International Journal of Information and Education Technology, Vol. 10, No. 5, May 2020.

[7] Sunil Chaudhary, Vasileios Gkioulos and Sokratis Katsikas, (2022). *Developing metrics to assess the effectiveness of cybersecurity awareness program*, Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Teknologivegen 22, accepted 12 April 2022.

[8] D. Nakama and K. Paullet, (2019). *The urgency for cybersecurity education: The impact of early college innovation in hawaii rural communities,* Information System Education Journal, Vol. 16, No. 4, pp. 41–52.