

ORIGINAL SCIENTIFIC PAPER

CYBERSECURITY EDUCATION FOR CHILDREN: DEVELOPMENT OF AN ONLINE APPLICATION AS AN INTERNET SAFETY TOOL

MRĐA Bojan¹, SOLEŠA Dragan², KRAŠNA Marjan³

¹ Belgrade Business and Arts Academy of Applied Studies, Belgrade (SERBLA) ORCID 0009-0000-5710-9048

² Faculty of Economics and Engineering Management, Novi Sad (SERBLA) ORCID 0000-0003-1185-7969

³ University of Maribor, Faculty of Arts & Faculty of Natural Sciences and Mathematics, Maribor (SLOVENIA)
ORCID 0000-0002-6089-1584

E-mail: bojan.mrdja@gmail.com; dragan.solesa@fimek.edu.rs; marjan.krasna@um.si

ABSTRACT

This paper explores the process of creating an application for educating children about cyber threats on the Internet. Cybersecurity is becoming an increasingly important topic in the digital age, and educating children on this subject is imperative for their protection. The goal of this paper is to propose a conceptual solution, along with the steps and principles involved in creating an application to educate children about cyber threats on the Internet. The application offers an interactive and engaging experience for children learning about cybersecurity. The research investigates the most effective approach to educating children by employing a survey. The acquired results are then assessed using the AHP method. Based on the results, we propose a conceptual solution for the most effective way to educate children, as well as suggestions for the creation and implementation of the online application. We provide a detailed proposal for the development of the "Cyber Heroes" application, including identification of the target audience, definition of functionalities, creation of interactive lessons, challenges and simulations, and the implementation of social interactions within the app. Furthermore, the paper explores gamification techniques integrated into the application to increase children's engagement and motivation to learn about cybersecurity. Through the analysis of results and discussion, the paper offers insights into an effective approach to educating children about cyber threats and contributes to the development of strategies for improving Internet safety among the youngest population.

Keywords: Cybersecurity education, Children, Online application, Internet safety

JEL:M15

DOI: 10.5937/intrev2501080M

UDC: 316.624-053.2:004.738.5

004.738.5.056-053.2

COBISS.SR-ID 172744969

INTRODUCTION

“The revolutionary development of the Internet and information and communication technology has led to changes in many aspects of life, and therefore education is gaining a new dimension”[1]. In today's digital era, characterized by the continuous integration of technology into daily life, children are facing the challenges of the online world at progressively earlier stages of their lives. Cyber threats are becoming increasingly sophisticated, ranging from scams and malicious software to inappropriate behavior on social media. The continuous development of the Internet presents parents, teachers, and society with the task of ensuring the safety of the youngest users and shaping their relationship with technology. Hence, the research and development of efficient educational tools emerge as essential protection against cyber threats. This paper is dedicated to the research and description of an innovative online application that is not only a source of relevant information about cybersecurity but also an interactive platform that adapts its content to the user's age. By combining interactive lessons, educational games, and quizzes, the application should create a dynamic environment that not only informs children about potential risks but also encourages them to actively learn through play. In order to effectively address the challenges of the online domain, the application should not only offer information about cybersecurity but also develop critical thinking skills, situation analysis, and responsible behavior. The comprehensive approach covers topics such as password security, fraud detection, privacy settings, and ethical online behavior. With this paper, we explore the need for a proactive approach to education about cyber threats, recognize the challenges children face on the Internet, and provide a conceptual solution for developing an innovative tool to raise the level of awareness and digital literacy among the youngest Internet users. Ultimately, we expect this approach to contribute to the creation of a safer digital environment for children and young people.

INTRODUCTION TO RESEARCH ON THE DEVELOPMENT AND EVALUATION OF AN ONLINE CYBERSECURITY EDUCATION APPLICATION

In the introduction of the research, we begin with the complex background of pervasive digitization in society and the increasing involvement of children in online activities. “This situation was largely contributed to, among other factors, by the COVID-19 pandemic, during which online education experienced expansion”[2]. We are also facing the challenge of cyber threats that are becoming increasingly sophisticated and often pose a serious risk to children's safety. We analyze various aspects of these threats, including malicious software, potentially inappropriate behavior on social media, and risks related to privacy. In the next step, we define the research objectives. Primary objectives include conceptualizing a solution for the development of an application that will integrate modules of interactive lessons, educational games, and quizzes tailored to the user's age group. Furthermore, we aim to evaluate the effectiveness of this application in increasing children's knowledge about cyber threats. To lay the groundwork for the research, we conduct a survey using Saaty's scale for three groups of respondents. The survey is then statistically analyzed using the AHP method and the corresponding software. Kendall's coefficient of concordance is also calculated. Following this, we describe the proposed conceptual solution for the development of the application, including content, quiz suggestions, interactive lessons, and the implementation of functionalities. This research model provides a comprehensive framework for studying the effectiveness of an online application for educating children about cyber threats and contributes to advances in Internet safety for the youngest users.

TYPES OF CYBER THREATS TO CHILD SAFETY

The swift advancement of Information and Communication Technologies (ICT) has entirely reshaped our surroundings, particularly the world of children. Based on statistical data from Eurostat in 2023, 59.31% of the population in the European Union nations used the Internet to engage with various social media platforms, indicating a considerable presence of children and young people within that online population[3]. In recent years, there has been a growing popularity of social networks among students[1].

When it comes to children, especially those of school age (8 to 17 years old), the role of parents in ensuring safe Internet usage and content consumption is of crucial importance. Previous research in this field has shown that awareness of Internet risks and risks of child exploitation through the Internet is quite low[5] “Although the available data relate to research conducted under the auspices of UNICEF in 2020, it is reasonable to expect that over the past four years, the level of Internet literacy among the parental population has improved to some extent”[6]. Cyber threats that can impact children include various types of risks online. Here are several key cyber threats children are exposed to:

- **Cyberbullying:**

Involves abuse, insults, or belittlement through social media, messages, or other online platforms. It can have serious emotional and mental consequences.

- **Internet Predators:**

Individuals who attempt to establish contact with children with the intention of abusing, blackmailing, or sexually exploiting them. Children need to be trained to recognize risky situations and protect their privacy.

- **Inappropriate Content:**

Exposure to inappropriate material, such as violent content, explicit materials, or drugs, through online platforms. Parents and guardians should apply content control tools and set restrictions on devices.

- **False Information and Disinformation:**

Exposure to false news, disinformation, and online scams. It is important to develop critical thinking skills in children so they can discern accurate information from inaccurate.

- **Cyberstalking:**

Online stalking or harassment, including sending threats, monitoring online activities, and similar behaviors. Parents should be aware of the signs of abuse and support children in reporting such incidents.

- **Ransomware and Malware:**

Children are at risk of downloading malicious software through games, applications, or suspicious links. It is important to encourage children not to download unknown files and to regularly update antivirus programs.

- **Presence on Social Media:**

Excessive social media exposure can lead to feelings of pressure, unrealistic standards, and reduced self-confidence. Children should be educated about the responsible use of social media.

- **Cybercrime:**

Children are potential targets of cybercrime, including identity theft, financial fraud, or unauthorized access to computer systems. They should be aware of the dangers and how to protect their personal information.

- **Technology Addiction:**

Excessive use of digital devices can lead to addiction, affecting children's mental health and social skills. Parents should set limits on the time spent online.

- **Challenges and Stunts:**

Engaging in social media challenges or exhibiting risky behaviors (e.g., recording and sharing dangerous stunts). Children should be informed about the dangers and consequences of such challenges.

MOST AFFECTED GROUPS OF CHILDREN

Answering this question is not simple. There is no single age group of children most affected by cyber threats, as these threats are diverse and can influence children of different age groups in distinct ways. A new global report from the Global Cybersecurity Forum (GCF) has found that 72% of children around the world have experienced at least one type of cyber threat online [7]. Nonetheless, certain age groups are more susceptible to specific types of threats. Here are a few examples:

- Younger children (up to preschool age):

These children often use Internet-accessible devices under parental supervision. Threats include inappropriate Internet content and risks of unauthorized device access.

- Elementary school children:

Children in elementary school increasingly use the Internet for school projects and entertainment. Cyber threats can include online violence, cyberbullying, and attempts to deceive children regarding personal information.

- High school students and adolescents:

This is the age when children become more active on social media and begin sharing content online. Cyber threats include cyberbullying, sexting, uncomfortable situations on the Internet, as well as an increased risk of falling victim to various other forms of deception.

It's important to note that every child is unique, meaning that various threats may impact them in different ways. Parents, guardians, and educators should tailor their approach to cybersecurity education according to the child's age, providing them with appropriate information and support to develop safe online habits.

On the website of the National Contact Center for Child Internet Safety, supported by the Ministry of Education of the Republic of Serbia, we have encountered the following statistical data:

- 72.9% of households in Serbia have Internet access
- 99.8% of businesses use the Internet for operations in Serbia
- 92.6% of the population uses mobile phones
- 94% of young people have profiles on social media

THE AIM OF THE RESEARCH

The aim of this research is to highlight the real dangers to children who are active online and to provide a proposed solution in the form of a conceptual design for developing an online application that will serve as a tool for preventing children's exposure to Internet dangers, with the goal of enhancing overall safety. Additionally, it aims to identify key findings and recommendations for future applications and research in this field. By conducting a survey, we gain significant insights into the awareness of parents and children about cyber threats. This approach ensures a comprehensive methodology that includes conducting, reflecting, and analyzing the issue of cyber threats among children. The research results should provide valuable insights into the effectiveness of this approach and contribute to understanding the most effective methods of cybersecurity education for the youngest Internet users.

SURVEY

During the survey process, we came up with the idea to allow different groups to fill out a survey addressing the same issues related to cyber threats on the Internet. The research included three groups: parents, children, and teachers. The total number of respondents was 125. A survey questionnaire in paper and electronic form (Google Form) was completed by a total of 44 parents, 40 children, and 41 teachers.

Guidelines – Example

The predominant method of educating children about cybersecurity on the Internet.

Saaty's scale:

1. Equal importance to both criteria
2. Minor dominance (compared to the opposite criterion)
3. Dominance (compared to the opposite criterion)
4. Strong dominance (compared to the opposite criterion)
5. Absolute dominance (compared to the opposite criterion)

Example:

You believe that game-based learning is a strongly dominant factor compared to classroom instruction.

Number 7 on the right side is marked – Game-based learning

What do you consider to be the dominant method of educating children about cybersecurity on the Internet?

EXAMPLE OF A GOOGLE FORM SURVEY

In the image below, we can see an example of a survey conducted via Google Forms.

The most dominant way of educating children in the field of cyber threats on the Internet

Compare the left factor with the right factor.
Mark only one value for the left or right factor or a number (1) if you consider the factors to be of equal importance.

Saaty scale

1. The same importance of both criteria
2. Low dominance (in relation to the opposite criterion)
3. Dominance (in relation to the opposite criterion)
4. Strong dominance (in relation to the opposite criterion)
5. Absolute dominance (in relation to the opposite criterion)

bojan.mrdjaga@gmail.com [Switch account](#)

Classes..... or Informing

9 7 5 3 (1) 3 5 7 9

Rank ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐

Classes..... or Game

9 7 5 3 (1) 3 5 7 9

Rank ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐

Figure 1. Online survey (Google Forms)

RESULTS

RANKING BY AHP METHOD

The ranking was conducted by comparing pairs using the AHP method. The calculation of the priority vector from the group matrix was performed using the method of eigenvalues. Survey codes where the calculated coefficient of (in)consistency exceeded 0.1 (indicating inconsistency in comparisons) were excluded from the study.

Initially, the ranking of four criteria was determined for each group separately, and then for each sub-cluster within the group. The calculation of priority vectors was done using a program called Expert Choice. Additionally, everything was verified using IBM SPSS Statistics software. Both tools are highly regarded in the market and widely used. The final presentation of the data is provided in MS Excel 365, which allows for easier ranking of the criteria.

	A	B	C	D	E	F	G	H	I	J	K
1	Parents and guardians										
2											
3	Comparison of pairs						K ₁ -Classes	0,171	2	Vector	Rank
4		K ₁	K ₂	K ₃	K ₄		K ₂ -Informing	0,137	3		
5	K ₁	1,00	1,25	0,25	3,64		K ₃ -Game	0,639	1		
6	K ₂	0,80	1,00	0,15	3,43		K ₄ -Training	0,053	4		
7	K ₃	4,04	6,52	1,00	8,60						
8	K ₄	0,27	0,29	0,12	1,00						
9		6,12	9,06	1,52	16,67						
10											
11	Standardized matrix										
12		K ₁	K ₂	K ₃	K ₄	Priority vector					
14	K ₁	0,163	0,138	0,163	0,218	0,171					
15	K ₂	0,131	0,110	0,101	0,206	0,137					
16	K ₃	0,661	0,720	0,659	0,516	0,639					
17	K ₄	0,045	0,032	0,077	0,060	0,053					
18						1,00					
19											
20	Calculatin CI and CR										
21		K ₁	K ₂	K ₃	K ₄	Sum	Sum/Priority vector				
22	K ₁	0,17	0,17	0,16	0,19	0,69	0,171	4,07			
23	K ₂	0,14	0,14	0,10	0,18	0,56	0,137	4,05			
24	K ₃	0,69	0,89	0,64	0,46	2,68	0,639	4,20			
25	K ₄	0,05	0,04	0,07	0,05	0,21	0,053	4,02			
26		Maximum eigenvalue of matrix				λ	max	4,08			
27		consistency index					CI	0,03			
28							CR	0,03			
29											
30											
31		Rank	1	2	3	4	5	6	7		
32		Random index	0,00	0,00	0,58	0,90	1,12	1,24	1,32		

Figure 2. Parents and guardians

The inconsistency index is 0.003, which is within the acceptable range. The upper limit of allowed inconsistency is 10%, or 0.1. The obtained index is 3%.

In Figure 2, the ranking of pairs by the AHP method is shown only for the group “Parents and guardians,” due to the scope of this paper.

We conducted the ranking in the same way for the remaining two groups, and the results are shown in Figures 3 and 4.

	A	B	C	D	E	F	G	H	I	J	K
1	Children up to the age of 16										
2											
3	Comparison of pairs						K ₁ -Classes	0,113	3	Vector	Rank
4		K ₁	K ₂	K ₃	K ₄		K ₂ -Informing	0,249	2		
5	K ₁	1,00	0,24	0,21	3,16		K ₃ -Game	0,589	1		
6	K ₂	4,10	1,00	0,23	4,90		K ₄ -Training	0,048	4		
7	K ₃	4,70	4,40	1,00	8,95						
8	K ₄	0,32	0,20	0,11	1,00						
9		10,11	5,84	1,55	18,01						
10											
11											
12	Standardized matrix										
13		K ₁	K ₂	K ₃	K ₄	Priority vector					
14	K ₁	0,099	0,042	0,137	0,176		0,113				
15	K ₂	0,405	0,171	0,147	0,272		0,249				
16	K ₃	0,465	0,752	0,644	0,497		0,589				
17	K ₄	0,031	0,035	0,072	0,056		0,048				
18							1,00				
19											
20	Calculatin CI and CR										
21		K ₁	K ₂	K ₃	K ₄	Sum	Sum/Priority vector				
22	K ₁	0,11	0,06	0,13	0,15	0,45	0,113	3,99			
23	K ₂	0,46	0,25	0,13	0,24	1,08	0,249	4,36			
24	K ₃	0,53	1,09	0,59	0,43	2,65	0,589	4,49			
25	K ₄	0,04	0,05	0,07	0,05	0,20	0,048	4,15			
26		Maximum eigenvalue of matrix					λ max	4,25			
27		consistency index					CI	0,08			
28							CR	0,09			
29											
30											
31	Rank	1	2	3	4	5	6	7			
32	Random index	0,00	0,00	0,58	0,90	1,12	1,24	1,32			

Figure 3. Children up to the age of 16

	A	B	C	D	E	F	G	H	I	J	K
1	Teachers										
2											
3	Comparison of pairs					K ₁ -Classes		Vector	Rank		
4		K ₁	K ₂	K ₃	K ₄	K ₂ -Informing		0,119	3		
5	K ₁	1,00	0,26	0,23	3,44	K ₃ -Game		0,285	2		
6	K ₂	3,91	1,00	0,31	6,35	K ₄ -Training		0,550	1		
7	K ₃	4,28	3,21	1,00	8,93			0,046	4		
8	K ₄	0,29	0,16	0,11	1,00						
9		9,48	4,62	1,66	19,71						
10											
11											
12	Standardized matrix										
13		K ₁	K ₂	K ₃	K ₄	Priority vector					
14	K ₁	0,105	0,055	0,141	0,174	0,119					
15	K ₂	0,413	0,216	0,188	0,322	0,285					
16	K ₃	0,451	0,694	0,603	0,453	0,550					
17	K ₄	0,031	0,034	0,068	0,051	0,046					
18						1,00					
19											
20	Calculatin CI and CR										
21		K ₁	K ₂	K ₃	K ₄	Sum	Sum/Priority vector				
22	K ₁	0,12	0,07	0,13	0,16	0,48	0,119	4,01			
23	K ₂	0,47	0,28	0,17	0,29	1,21	0,285	4,26			
24	K ₃	0,51	0,91	0,55	0,41	2,38	0,550	4,33			
25	K ₄	0,03	0,04	0,06	0,05	0,19	0,046	4,08			
26		Maximum eigenvalue of matrix				λ	max	4,17			
27		consistency index					CI	0,06			
28							CR	0,06			
29											
30											
31		Rank	1	2	3	4	5	6	7		
32		Random index	0,00	0,00	0,58	0,90	1,12	1,24	1,32		

Figure 4. Teachers

We eliminated 8 surveys due to inconsistency in comparison. In the group “Parents and guardians,” we excluded 6 surveys, as well as 2 surveys from the group “Children up to the age of 16.” There were no inconsistencies in the “Teachers” group. Inconsistency occurs when the consistency ratio (CR) exceeds 0.1. In one of our calculations, the CR was 0.18, which is higher than 0.1 and therefore should not be tolerated.

KENDALL'S RANK CORRELATION COEFFICIENT AND INTERPRETATION OF KENDALL'S RANK CORRELATION COEFFICIENT VALUES

Kendall's nonparametric rank correlation coefficient is calculated using the formula:

$$r''_{12} = \frac{12}{m^2 \cdot n} \cdot \frac{n \sum_{i=1}^n S_i^2 - \left(\sum_{i=1}^n S_i \right)^2}{n^3 - n}$$

In the formula:

m – the number of numeric series

n – the number of data points in each series

$S_i, i=1, 2, \dots, n$ – the sum of ranks across rows

This is an analysis that utilizes statistical programs to achieve the desired goals of scientific research accurately and efficiently. This method has been applied in economic research for almost a century.

Kendall's correlation coefficient indicates a potential relationship among more than two variables, where a change in the value of one variable affects the change in another. An increase in one variable stimulates an increase in another, resulting in a positive correlation. If an increase in one variable leads to a decrease in another, a negative correlation is observed. The coefficient of multiple correlation can range between -1 and +1. A greater number of variables provides more precise results. The application of this method to verify independent data, through twelve different criteria for four different clusters, contributes to the significance of the test, given that the p-value is close to average values, with minimal oscillations.

In Figure 5, we can view the formulas for calculating Kendall's rank correlation coefficient in the final result.

https://www.researchgate.net/		Parents and guardians:	Rank 1 level	Children up to the age of 16 years	Rank 1 level	Teachers	Rank 1 level				
2											
3	K1-Classes	0,171	2	0,113	3	0,119	3				
4	K2-Informing	0,137	3	0,249	2	0,285	2				
5	K3-Game	0,639	1	0,589	1	0,550	1				
6	K4-Training	0,053	4	0,048	4	0,046	4				
7		1,000		1,000		1,000					
8											
9		Calculated	Rank1	Calculated	Rank2			Rank3	Rank1 + Rank2+Rank3		
10	compulsory classes in school	0,387	0,066	5	0,351	0,040	7	0,360	0,043	5	17
11	facultative teaching at school	0,205	0,035	8	0,299	0,034	9	0,306	0,036	7	24
12	extracurricular activities	0,407	0,070	4	0,350	0,040	8	0,334	0,040	6	18
13	via social media	0,738	0,101	3	0,272	0,068	4	0,624	0,178	2	9
14	via print media	0,174	0,024	10	0,640	0,159	3	0,267	0,076	4	17
15	via educational shows on TV	0,088	0,012	12	0,086	0,022	11	0,109	0,031	10	33
16	quiz (questions - answers)	0,312	0,199	2	0,302	0,178	2	0,297	0,163	3	7
17	purpose-built board games	0,062	0,039	6	0,076	0,045	6	0,060	0,033	9	21
18	interactive stories - drawing conclusions	0,047	0,030	9	0,079	0,047	5	0,062	0,034	8	22
19	purpose-built online games	0,579	0,370	1	0,542	0,320	1	0,581	0,320	1	3
20	seminars - courses	0,679	0,036	7	0,365	0,018	12	0,345	0,016	12	31
21	online classes	0,321	0,017	11	0,635	0,031	10	0,655	0,030	11	32
22		4,000		4,000		4,000					
23											
24	Number of ranked elements	12		Numerator	12636						
25	Number of expert groups-m	3		Denominator	15444						
26				W	0,82						
27											
28											
29											

Figure 5.

The results mentioned above are confirmed using the statistical software IBM SPSS, where the calculated values are $W = 0.82$ and $p = 0.0045$.

W – represents the degree of correlation, or the coefficient of concordance

m – represents the number of groups of respondents, in this case, three groups

n – represents the number of ranked elements, which in this case is 12 criteria

p – represents the statistical significance of the test

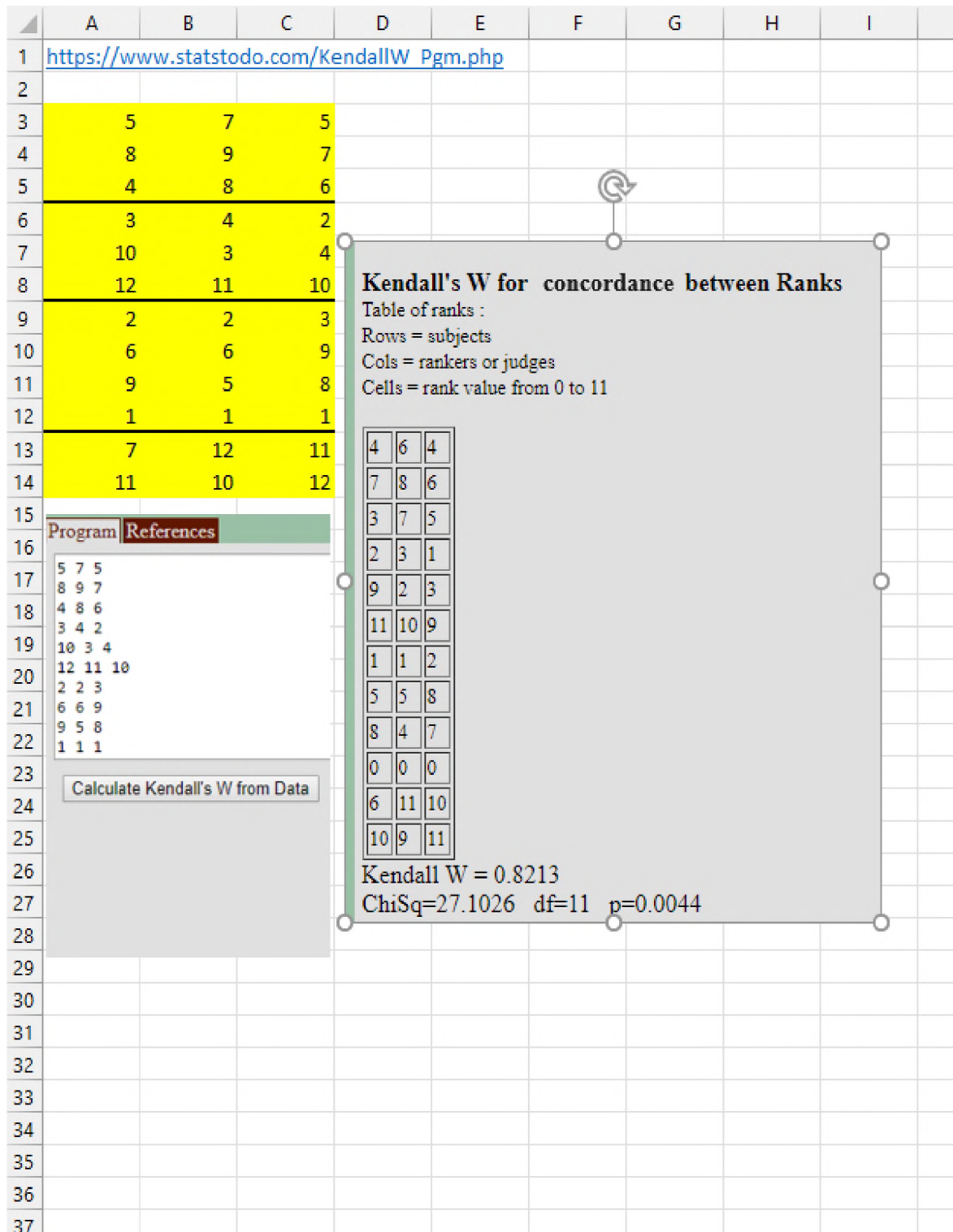


Figure 6. Kendall – calculation of concordance

GAMIFICATION

In recent years, the concept of gamification, defined as “the use of game design elements in non-game contexts”[8], has revolutionized the way people interact with various activities and content by applying game elements and mechanics. Through this practice, users are provided with an experience that promotes enjoyment, learning, and goal achievement, using mechanics such as competition, rewards, progression, and social interaction. This approach not only creates a more dynamic environment for users but also inspires them to actively engage in tasks or activities that may otherwise be less motivating or dull.

With the increasing adoption of gamification in various spheres such as education, business, healthcare, and marketing, the application of this strategy becomes increasingly significant. By using gamification, educational content becomes more enjoyable and interactive, allowing students to engage on a deeper level and more effectively acquire new concepts and skills. In the business world, gamification is used to increase productivity, motivate employees, improve customer engagement, and build brand loyalty.

In healthcare, gamification can be key to promoting healthy behaviors, motivating people to lead a more active lifestyle, adhere to therapy, or regularly undergo preventive check-ups. Additionally, gamification can be useful in marketing, enabling brands to create interactive campaigns that capture consumers' attention and encourage their engagement on social media or other platforms.

"Games are a crucial aspect of human culture and society and promote motivation and engagement"[12]. Essentially, gamification is much more than simply adding game elements—it is a philosophy focused on creating a positive, engaged, and productive environment through the creative use of gaming principles.

"Gamification in the context of learning can be referred to as gamified learning[10]. Learning through games and gamified learning uses the same literature as conventional learning methods. Additionally, the research approach and tools for creating educational games are the same as in conventional learning methods. Although these aspects are similar, the nature of the learning approaches differs. Game-based learning involves designing fully developed, or "serious," games, while gamification focuses on extending or modifying existing learning processes to create a new type of learning experience that users perceive as a game. Some students may not be familiar with the term gamification, so it is critical to provide them with some background information on this concept[11].

THE TECHNIQUES OF GAMIFICATION

"Gamification has been studied in different research contexts"[13]. The techniques of gamification utilize elements of games to increase motivation, engagement, and learning among users. In the context of educating children about cyber threats on the Internet, gamification can be useful in creating a fun and interactive learning experience. Learning types with a high level of interaction and challenge—such as game-based learning—have become widely used[14]. Children can progress through various levels or stages in the application, with each level representing a specific concept or aspect of cybersecurity. This level system can be accompanied by achievements, rewards, or special privileges as children progress. Setting challenges and tasks that require problem-solving and the application of knowledge about cybersecurity can increase children's engagement. These challenges can be designed to simulate real cyber threat situations and encourage children to apply their protection skills. Through collecting points or other virtual rewards, children can be motivated to actively participate in activities within the application. These rewards can be linked to achieving specific goals, successfully completing challenges, or engaging in user community activities. "Other gamification techniques, such as rewards, progress bar, challenges, feedback, and avatar, have been used either alone or along with other gamification techniques"[15]. Organizing competitions or ranking users based on their achievements can further motivate children to engage in learning about cybersecurity. Displaying a leaderboard of top users can foster healthy competition and encourage children to strive to improve their skills. Integrating an engaging and exciting narrative can enhance children's engagement with the application. Through a story or adventure, children can follow characters facing cyber threats and learn how to protect themselves from them.

By combining these gamification techniques, an application for educating children about cyber threats can become an interactive and enjoyable experience that encourages learning and the development of online protection skills.

THE APPLICATION OF THE OBTAINED RESULTS AS A PROPOSAL FOR THE DEVELOPMENT OF A MODEL FOR AN APPLICATION AIMED AT EDUCATING CHILDREN ABOUT CYBER THREATS.

Based on the survey results, we arrive at the most suitable solution for educating children about cyber threats on the Internet, which is the development of an online game, or in this case, an online application.

The proposed name of the application is “Cyber Heroes.” “Superheroes have the power to impact the real world. Their power lies in the adventurous, ambitious hearts and minds of children, who have the capacity to grow up to be the heroes they idolize the most”[16]. The scientific paper published in the Oxford Journal discusses how it's important for children to have their own superheroes because it helps them become better people, make more effort, distinguish between good and evil, etc. The application should contain interactive lessons on the basics of cybersecurity through engaging animations, comics, or short videos[16]. These lessons cover topics such as password security, privacy protection, recognizing email scams, and safe behavior on social media.

Interactive lessons within the “Cyber Heroes” application should be designed to be educational, engaging, and fun for children. Here are some examples of interactive lessons.

Animated comics: Children can follow the adventures of the main characters as they encounter various cyber threats, such as viruses, phishing attacks, or inappropriate behavior online. Through these comics, children will learn about Internet safety risks and how to protect themselves.

Challenging stories: Interactive stories can put children in situations that require making decisions about cybersecurity. For example, a story can pose questions like: “What would you do if a stranger sends you a friend request on a social network?” Children can then choose an answer and see how their decision could have different consequences.

Video lessons: Short video clips can show children concrete examples of cyber threats and provide them with useful tips on how to protect themselves. For example, a video lesson can explain how to recognize suspicious emails or how to share personal information safely.

Interactive quizzes: Children can test their knowledge of cybersecurity through interactive quizzes. After each lesson, questions can be asked to assess understanding of key terms and concepts. Based on their answers, children can receive feedback and advice for further learning.

Through these interactive lessons, children will have the opportunity to learn about cyber threats on the Internet in a fun and engaging way, which will help them develop protection skills and safely navigate online platforms.

Another segment of the application should also include **Challenges and Tasks**. Children face challenges and tasks that test their knowledge of cybersecurity. For example, they may be asked questions about how to recognize suspicious emails or how to create a secure password. For each successfully completed challenge, children can earn points or small rewards.

Challenges and tasks within the “Cyber Heroes” application can provide children with the opportunity to apply their knowledge of cybersecurity in practical situations and test their skills. This segment of the application could consist of four sub-segments. The first sub-segment should focus on identifying phishing attacks. Children can be challenged to identify suspicious emails or messages on social media that attempt to deceive users. The task could involve identifying key signs of phishing attacks and making a decision about whether a particular message is legitimate or a scam. The second part of this segment should focus on creating a secure password. In this segment, children can be challenged to create secure passwords for their online accounts. The task could involve devising a password that combines letters, numbers, and special characters and is long enough to be secure. The third part would be a simulation of online interactions. Children can simulate various online interactions and make decisions about how to react to different situations. For example, they may be challenged to recognize inappropriate behavior on social media and choose the appropriate, correct way to respond. And the final sub-segment would be knowledge testing. Children can be challenged to test their knowledge of cybersecurity through interactive quizzes or games. These challenges can cover various topics, such as privacy protection, safe use of Wi-Fi networks, or recognition of online threats.

Through these challenges and tasks, children will have the opportunity to apply their knowledge of cybersecurity in real-life situations and acquire practical skills that will help them stay safe online. These interactive experiences will further motivate children to engage in learning and raise awareness about cybersecurity threats.

Simulations of situations. The application can simulate various situations related to cyber threats, such as phishing attacks or sharing personal information online. Children learn how to recognize dangers and respond to them properly. This third segment of the application should include four sub-segments. Phishing attack, where children are placed in a situation where they receive a suspicious email trying to trick them into revealing their personal information. Through the simulation, children will need to recognize signs of a phishing attack and decide how to respond - whether to ignore the message, report it as a scam, or inform their parents or teachers. The second sub-segment should be sharing personal information. The simulation can put children in a situation where they are asked to share their personal information on social media or other online platforms. Through this simulation, children will learn about the importance of privacy protection and the risks of sharing personal information with unknown individuals. The third sub-segment would be password security. Children can be challenged to create a secure password for their online account and test it in a simulated situation. For example, they may be placed in a situation where they are subjected to hacking attempts and must rely on their strong password to protect their account. The fourth sub-segment could be cyber peer bullying. The simulation can depict a situation of cyberbullying on the Internet, such as cyberbullying on social media or through messages. Children will be challenged to recognize such behavior and learn how to respond to it - whether to turn to parents, teachers, or other authorities, or to support a friend who is a victim of cyberbullying.

Through these simulations, children will have the opportunity to practically apply their knowledge of cybersecurity and develop problem-solving skills in real online situations. This will help them become more aware of cyber threats and develop protection strategies that they can apply in their everyday online activities.

Role-playing: Through role-playing, children have the opportunity to take on the roles of different characters and make decisions about how to respond to specific cyber threats. This allows them to gain practical experience and develop protection skills online. Role-playing in the “Cyber Heroes” app can deepen understanding of cyber threats through active participation of children in various scenarios. Through these roles, children can put themselves in the shoes of different characters and face cybersecurity challenges from different perspectives. For example, children can take on the role of a victim of a phishing attack, as well as the role of an attacker trying to deceive others. This type of game allows children to better understand the motives and techniques of cyber threats, as well as develop empathy towards others who are victims. Additionally, through role-playing, children can experiment with different protection strategies and develop problem-solving skills in a safe and controlled environment. This interactive experience further deepens learning about cybersecurity and enables children to develop practical protection skills that they can apply in the real world.

Social Interaction: Social interaction within the “Cyber Heroes” application allows children to learn about cyber threats through collaboration, competition, and exchange of experiences with their peers. This part of the application would consist of four sub-segments. The first would be competitions. In this way, children can compete with their friends or other users of the application in solving challenges and quizzes about cybersecurity. Competitions could be organized on a weekly or monthly basis, with smaller prizes for the most successful participants. The second sub-segment would be clubs and group tasks. The application could enable children to join virtual clubs or groups where they would work together to solve problems and exchange advice on cybersecurity. These clubs could focus on specific topics or challenges, such as privacy protection or recognizing phishing attacks. The third sub-segment could be social networks within the application. The application could have social networking functionality where children could share their achievements, tips, and experiences with cybersecurity with other users. Through this interaction, children can build a supportive community and inspire each other to stay safe on the Internet. The fourth sub-segment would be collaboration on projects. Children can team up with their peers to work on collaborative projects or campaigns related to cybersecurity. For example, they can create educational materials together or organize events in their schools or communities to raise awareness about cyber threats.

Through social interaction, children have the opportunity to learn from their peers, exchange ideas, and support each other in the process of learning about cybersecurity. This interactive experience not only contributes to their individual learning but also strengthens their sense of belonging to a community that cares about cybersecurity.

This example illustrates how gamification can be used to educate children about cyber threats on the Internet through interactive lessons, challenges, simulations of situations, and social interaction. This type of application can be both fun and educational, motivating children to actively learn about the importance of cybersecurity and develop skills necessary for safe Internet use.

CONCLUSION

In conclusion, the “Cyber Heroes” application is designed to meet the needs of modern society by providing a comprehensive and interactive approach to educating children about cyber threats on the Internet. Through its wide range of features, this application will empower children to become responsible digital citizens, capable of recognizing, understanding, and overcoming cyber threats encountered in the virtual world.

In addition to providing a wealth of useful information, the “Cyber Heroes” application can also offer practical exercises through which children can test their knowledge and skills in simulated situations. Through role-playing, children will have the opportunity to step into the shoes of different characters and perspectives, allowing them to better understand how cyber threats manifest and how to respond to them appropriately. These interactive exercises will contribute to a better understanding of the complexities of cyberspace and strategies for effectively responding to potential threats.

An important aspect of this application will also be social interaction, which will allow children to connect with their peers, share experiences, and support each other in the learning process. Through shared challenges, competitions, and group activities, children will not only learn about cybersecurity but also develop skills in teamwork, empathy, and solidarity. This aspect will contribute to the creation of a more cohesive and informed community of young digital citizens.

Overall, the “Cyber Heroes” application will not just be a tool for acquiring knowledge about cyber threats but a platform for developing the skills, attitudes, and values essential for safe Internet use. Through this interactive, educational, and inspiring experience, children will be empowered to become informed and responsible digital citizens, ready to face challenges and adapt to changes in the digital world.

The “Cyber Heroes” application will represent a step forward in building a safer and more responsible online environment for all users. The platform is designed to bring long-term benefits to both individuals and society as a whole by promoting digital literacy and security from an early age. In this way, “Cyber Heroes” will play a key role in preparing future generations for the challenges and opportunities of the digital age.

REFERENCES

- [1] Đurica N., Soleša D., Šimović V., Đurica M., (2018), Students’ perception of the importance of using Facebook, *Croatian Journal of Education*
- [2] Aristovnik A., Karampelas K., Umek L., (2020), Impact of the COVID-19 pandemic on online learning in higher education: a bibliometric analysis. Available at: <https://www.frontiersin.org/articles/10.3389/feduc.2023.1225834/full>
- [3] EUROSTAT, (2023), Individuals using Internet for participating in social networking. Available at: <https://ec.europa.eu/eurostat/databrowser/view/tin00127/default/table?lang=en>
- [4] Đurica N., Soleša D., Percepcija i stavovi studenata prema obrazovanju na daljinu, (2017), *Ekonomija, teorija i praksa* at: <https://ec.europa.eu/eurostat/databrowser/view/tin00127/default/table?lang=en>
- [5] Unicef, (2018), Istraživanje o nivou svesti o potencijalnim Internet rizicima i zloupotrebama među roditeljima dece uzrasta 8 do 17 godina. Available at: <https://www.unicef.org/serbia/media/5756/file/Istraivanjesvestiopotencijalniminternerizicimaizloupotrebamairoditeljimadecuzrasta08do20godina.pdf>
- [6] Popadić D, Kuzmanović D. (2020), Korišćenje digitalne tehnologije, rizici i zastupljenost digitalnog nasilja među učenicima u Srbiji, UNICEF/Institut za psihologiju Filozofskog fakulteta Univerziteta u Beogradu
- [7] Deterding, S., Dixon, D., Khaled, R., & Nacke, L. (2021), From game design elements to gamefulness: defining “gamification”. In A. Lugmayr (Ed.), *Proceedings of the 15th International Academic Mindtrek Conference: Envisioning Future Media Environments* (pp. 9–15). New York: ACM. <https://doi.org/10.1145/2181037.2181040>
- [8] AL-Smadi M., (2015), European Summit on Immersive Education. *Immersive Education* p. 85–97

- [9] Krath J., Schurman L., F.O. von Korfflesch H., (2021), Revealing the theoretical basis of gamification: A systematic review and analysis of theory in research on gamification, serious games and game-based learning, Available at:
<https://www.sciencedirect.com/science/article/pii/S0747563221002867#bib74>
- [10] Armstrong, M. B., & Landers, R. N. (2019). An evaluation of gamified training: using narrative to improve reactions and learning. *Simulation & Gaming*, 48(4), p. 513–538.
<https://doi.org/10.1177/1046878117703749>
- [11] Quang C. L., (2021), Using gamification to teach and engage students in the act of summary writing, Available at:
<https://digitalcommons.uri.edu/cgi/viewcontent.cgi?article=1489&context=jmle>
- [12] Salier M., Homner L., (2019), The Gamification of Learning: a Meta-analysis, Available at:
<https://link.springer.com/article/10.1007/s10648-019-09498-w>
- [13] Ding, L., Er, E., & Orey, M. (2018), An exploratory study of student engagement in gamified online discussions. *Computers & Education*, 120, p. 213-226.
<https://doi.org/10.1016/j.compedu.2018.02.007>
- [14] Brown B., Nassirudin M., Cabral A., (2019), Childhood idols, shifting from superheroes to public health heroes. Available at: <https://academic.oup.com/jpubhealth/article/38/3/625/2239795>
- [15] Arlt F., Arlt. H.F., (2023), Gamification of life and gaming society, Springer
- [16] Davies V., (2022), Why Children Are Unsafe in Cyberspace. Available at:
<https://cybermagazine.com/articles/72-of-children-globally-have-been-victims-of-cyber-threats>

Article history:

Received 16 April 2024

Accepted 20 June 2024