



# The good practices for implementation of cyber security education for school children

Dana Ondrušková<sup>1\*</sup>

 0000-0001-9591-5673

Richard Pospíšil<sup>1</sup>

 0000-0002-1428-4038

<sup>1</sup> Department of Economic and Managerial Studies, Faculty of Arts, Palacky University Olomouc, Olomouc, CZECH REPUBLIC

\* Corresponding author: [dana.ondruskova01@upol.cz](mailto:dana.ondruskova01@upol.cz)

**Citation:** Ondrušková, D., & Pospíšil, R. (2023). The good practices for implementation of cyber security education for school children. *Contemporary Educational Technology*, 15(3), ep435. <https://doi.org/10.30935/cedtech/13253>

## ARTICLE INFO

Received: 19 Feb 2023

Accepted: 27 Apr 2023

## ABSTRACT

The increasing use of the Internet calls upon the need for adequate cyber security awareness to better face the risk and dangers connected with the online environment. This research presents an experiment that revealed the cyber security awareness of children at Czech primary schools. They were tested for their skills to distinguish different online risks. After the pre-testing children received training and with the time delay they filled in very similar questionnaires. The re-testing measured how well the children retained the training and their ability to use the skills in the virtual environment. The results show only a moderate level of cyber security awareness at the initial testing. The one-off training had only an insignificant impact on their online behavior. The research reveals an important finding. One-off training does not affect their responsive online behavior and is not a suitable solution for effectively improving online safety skills. The task is to involve cyber security awareness education in the whole educational process. Based on the literature and conducted research this paper provides a set of recommendations for the designers of the cyber security school curriculum.

**Keywords:** cyber security, online risk, education, curriculum

## INTRODUCTION

With the outrageous rise of digital technology and its affordability, the number of social network users is also increasing. Along with this, the level of danger moving into cyberspace is amplifying, with aggression, bullying, blackmail, and abuse. The profiles and posts published on social networks contain a large amount of personal data that may be another source of risks as they are fast and anonymous to carry out cyberbullying, cyberstalking, cyber grooming or even sexual attacks. The impact of risks and dangers is an increasingly debated topic, the more these practices are applied to children. Especially school children belong to that part of the virtual generation who get most of their entertainment and information from the Internet when being outside the classroom (Hourcade, 2015). Schools play a vital role in promoting and teaching online safety (Patterson et al., 2022). The teachers got into the new roles of online safety tutors with the hard task to wrestle with complex issues around not only false and misleading information as well as to focus on young people's understanding of the wider effects and risks of media. Awareness of the issue is widespread. Preventing the dissemination of fake news requires fast action and classrooms should be on the front line of battle (Talwar et al., 2019). Cyber security awareness education at schools has become a necessity as cyber incidents caused by human factors achieve the largest percentage of cyber security incidents causes.

### Cyber Security Awareness of School Children

Waldock et al. (2022) publish a report on developing cyber skills among children and young people. Mason et al. (2018) highlight the long history of fake news and its relation to the media technologies in which cultures

grow. Current iterations of this phenomenon are discussed alongside the effects of social media and offer a preview of the contents of this special issue on media literacy, and the challenge for democracy resulting from fake news Qiu et al. (2017). Mrah and Tizaoui (2018) state that a fair majority of teenage students are vulnerable to misinformation online due to overwhelming information. Alwanain (2021) identifies phishing as one of the main crimes perpetrated against the Internet users, because the sophistication of phishing attacks continues to develop alongside the expansion of the Internet technology and online services. Celliers and Hattingh (2020) have identified the decrease in cognitive abilities of individuals to be the reason for the fake news spread. Ascoott (2020) asserts that the persistent menace of fake news on the Internet requires real solutions in the form of cyber security awareness programs at schools to reduce cyber security attacks and incidents. Lastdrager et al. (2017) test the ability of both trained and untrained children to distinguish phishing emails and websites from legitimate ones. Increasing the ability to recognize phishing requires good awareness (Mitchell et al., 2020). The results show the more profound and complex the training is the better ability shows in recognize legitimate emails. McKnight et al. (2016) documents six common strategies used across the seven sites and identifies five roles that technology plays in enhancing teaching and learning, moreover they discuss how these strategies benefit teachers and learners. Several research has been published on how children experience and manage online risk. Quayyum et al. (2021) conducted a systematic review to identify cybersecurity risks, cybersecurity awareness initiatives, and the evaluation of these initiatives. These reviews demonstrate the substantial interest from the research community in supporting schools with evidence-based approaches for designing and implementing online safety education.

### **Involvement of Cyber Security Matters in School Curriculum**

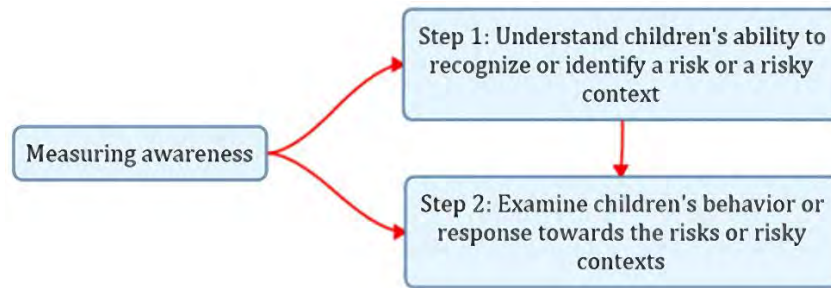
The importance of how the topic of cyber security is involved in the school curriculum is dealt with as well. As per Shamsi (2019) what makes the difference in students' learning and outcomes is the pedagogy being employed rather than the technology itself. The way the topic is exposed matters most (Haldane, 1990). As per Winter et al. (2021), effective use of technology in education poses challenges for teachers and highlights the technological requirements for successful online teaching. Lamond et al. (2022) explore the guidance and aspects of current school curriculum expectations on cybersecurity. Cybersecurity skills require mature cognitive abilities, which children only acquire after they start using technology (McKnight et al., 2016). This is the reason behind focusing attention on cyber security awareness in schools to reduce cyber security attacks and incidents. To be safe in a virtual environment, an appropriate set up of educational activities concerning online opportunities and risks, managing harms and threats online is necessary (Giannakas et al., 2019). Online safety education, also e-safety education, the Internet safety education, cyber safety education, and even 'cyber wellness' (Liao & Lin, 2017) involve more than digital and media literacy or teaching about privacy protection (Finkelhor et al., 2021). It extends to intentionally enacting behaviors that support healthy, respectful, and safe online interactions (Cortesi et al., 2020). Recent studies and discussions on the need for improving cyber security education show insufficient time to cover relevant topics, lack of a direction on what schools and teachers should aim at in cyber security education, and the pressure to prioritize more survival-focused skills than cyber security (Mehta, 2022; Waldock et al., 2022).

At school, various courses and lectures are organized with the aim to promote the cybersecurity awareness of children. These courses are organized either by the schools themselves or in cooperation with different public or private institutions, for example, banks or police. Lorenz et al. (2018) found out that schools need help with developing guidelines or strategies how to help students to remember the solutions to basic problems. The current situation at schools tends to involve cyber security training in the form of short-term and non-consecutive activities (Venter et al., 2019) notwithstanding the fact that effective cybersecurity teaching programs require both theoretical and practical skills that are necessary for boosting children's resilience and ability to resist the threats such including phishing attacks, online harassment or their trust in misinformation (Penncheva et al., 2020; Waldock et al., 2022).

### **Evaluating Cybersecurity Awareness**

From all these studies mentioned above a question concerning the evaluation of cybersecurity awareness arises. The researchers mainly use two techniques for evaluating children's awareness (Quayyum et al., 2021):

1. directly measuring the level of awareness/knowledge and



**Figure 1.** Measuring children's cyber security awareness (Quayyum et al., 202)

2. measuring the effectiveness of their approaches to raise cybersecurity awareness.

Cyber security awareness can be measured in two steps (Zhao et al., 2019). Firstly, the children's ability to recognize a risk or a risky context is found, consequently, the children's response or behavior towards the risks or risky contexts is explored in [Figure 1](#).

The above-mentioned information indicate a growing interest in the systematic implementation of cyber security skills into schools' curriculum.

### Purpose of the Study

The literature indicates a gap concerning the impact of one-off courses on the online safety of children. This study presents research to determine the consequences of training at schools on children's online behavior. The current study draws attention to the necessity of the growing concern attributed to the need for systemic cyber security education in schools. The research applies qualitative methods based on a questionnaire survey conducted repeatedly for collecting data demonstrating the cyber awareness of the school children and the impact of the training on their online behavior. It proposes evidence-based approaches for designing and implementing online safety education. The research is mainly dedicated to showing whether school children are responsive in their online behavior to one-off training lessons in the form of workshops given in the course of the school year. Firstly, the research gives an overview of the level of cyber security literacy of school children aged 13-15 years old. Consequently, it carries out a study on the effects of short training in cyber security on their online behavior. The results of the research are supposed to serve cyber security training designers when implementing online safety training into the school curricula in order to effectively implement cybersecurity training activities. Overall, based on the available literature and on the conception of the possibility to measure cybersecurity awareness Quayyum et al. (2021), this systematic literature review is guided by two research questions:

**RQ1.** What is the current level of cybersecurity awareness of school children?

**RQ2.** What is the impact of one-off cybersecurity training on school children's awareness?

The main findings from the research include:

- (1) data on the level of cybersecurity awareness obtained from a sample of school children,
- (2) data indicating the impact of one-off cyber security training lessons on the cyber security awareness of the sample examined, and
- (3) a set of recommendations for the designers of the cyber security school curriculum.

### METHOD

For the present research, a quasi-experimental approach using time-series data is designed. The quasi-experimental approach may induce some systematic errors in course of various stages of the research due to the absence of a randomized controlled trial and may consequently distort the conclusion. Intentionally, in the present study, the participants are not randomized as the conclusions are intended to serve policymakers, educators, and parents in developing effective cybersecurity awareness programs for school children, in general, to protect them from online risks. Anyhow it is possible to increase the reliability of the quasi-experimental research design by using some tools that are described, as follows.

To minimize the biases and confounders a comparison with a group that has similar attributes can be undertaken. This is not a suitable tool for the present paper. Another tool appropriate to avoid the lack of a quasi-experimental approach is a time series design involving the repetition of data collection in time before and after treatment. Using digital technology is particularly suitable for time series design because it enables the collection of data automatically and frequently. For the present research, a chosen tool to minimize the effects of not randomly assigning participants is a design with a before-after assessment. Moreover, by including before-and-after assessments, it is possible to minimize problems of the weaknesses of the quasi-experimental design, such as simple one-group before/after designs (Baldwin et al., 2010). Assessing participants before the questioning helps to decrease the influence of confounders and biases (Baldwin et al., 2010). In the case of the second test, the participants' scores may be influenced by repeating the same tests (Bloomfield, 1976). In the present research, the second round of testing was undertaken with a six-month delay and modified questions to decrease the influence of confounders and biases. On the contrary potential biases may occur due to the background that changes in pupils' lives. The actual mental state of the participants may induce misleading conclusions. For that purpose, a sufficient number of participants were involved in the research. Based on the above-mentioned assumptions in the analysis, the patterns of change over time are compared.

The study comprises school children attending second-degree of elementary schools in Czech Republic. The survey was carried out by the researcher in cooperation with the primary schools in Liberec Region, Moravian-Silesian Region, Olomouc Region, Pilsen Region, South Moravia Region, Vysočina Region, and Zlín Region, situated in Czech Republic and with local agencies for technological innovation. 770 children, resp. 35 classes from 21 different elementary schools participated in the form of three online games with closed-ended questions. Out of 770 children attending five classes that were chosen for the research 125 had to be excluded. The achieved response rate is 83.7 %. While 38 pupils were excluded due to their absence on one or two testing (5%), 87 pupils (11.3%) had to be excluded for not having finished the testing properly. Thus data collected from 645 pupils aged between 13 and 15 of which 330 girls and 315 boys are considered in the research. The collection of answers was delivered by the local agencies for technological innovation. The data were consequently assembled, analyzed, and assessed by the researcher. Each pupil was given a nickname to be identified when answering pre-testing, post-testing, and post-post-testing. The answers were recorded and assigned to be able to assess the progress.

The questionnaire was conceived so that it resembles ordinary online communication. The questions were constructed with an emphasis on the principles of cyber security rules (Maqsood et al., 2018). The respondents were supposed either to choose the right answers, recognize any form of risky behavior when communicated via social networks, or identify misinformation. The emphasis is given on extortion, blackmailing and misuse of trustfulness (McNair, 2018). The maximum total score of the right answer is 10. The questioning was compiled and verified by Czech Bank Association, National Cyber and Information Security Office, and Police of Czech Republic. The test is available on <https://www.kybertest.cz/> in Czech language, which is the mother tongue of questioned pupils. **Appendix A** gives some examples of interactive testing.

The aim of the questionnaire was to collect the score of the right answers proving cyber security literacy when keeping a critical mind set: the ability to recognize suspicious messages aiming at sensitive data, resistance to harassing messages, assess security risks when communicating on social network and being aware of the principles of safety connection to the public network. The first questionnaire was filled in by the pupils without any previous educational intervention in the classes. One week after the children attended two lessons of cyber-security training given by the lecturer in cooperation with the researcher and their teachers. The training course dealt with topics concerning social media use, mobile device security, passwords and authentication, phishing attacks, public Wi-Fi, the Internet, and e-mail use. The training methods were guided by suggestions proposed by Page (2019). The course given to the participants dealt with information literacy, information security, and related areas. The aim of the course was primarily to inform the pupils about the risks of social interactions on the Internet and the terms associated and secondly to emphasize the risk prevention, namely prevention of data and information loss, prevention of theft and misuse of personal data. The teaching methods were based mainly on face-to-face education practice combined with demonstrations and individual tasks on the pupils' personal mobile devices. By means of the demonstration and short videos,

pupils were supposed to consider the dangers of social networks with possible misuse of personal data. Pupils were told what cyberbullying, cyberstalking, and cyber grooming stand for and shown some bad examples from the practice. During the course, pupils could try to create an unbreakable password or tag faces in photoshops to see how easily their photograph can be misused. The training one-off training took two lessons, which is 90 minutes.

Consequently, six months later on, the participants were asked to fill in a similar post-test with modified questions. There was another time gap of six months to proceed with the final post post-testing and complete the final part of the research.

To answer the first research question: *What is the current level of cybersecurity awareness of school children?* a set of descriptive statistics is exploited. For calculation, the statistical data calculator DATAtab was used. In descriptive statistics, the mean, median and mode values are measures of location. Based on data collected for the sample, the measures of location provide information about where the "center" of the distribution lies. The mean rank is the average of the ranks for all observations within each sample while the median divides the row into equal parts. Compared to the mean, the median is much more robust against scattering. The standard deviation is the average amount of variability in the dataset. Thus information on how far each value lies from the mean is obtained.

Further and deeper statistical analysis enables to answer the second research question: *What is the impact of one-off cybersecurity training on school children's awareness?* To go into more detail and to find out whether there are statistically significant differences between three rounds of non-parametric Friedman statistical tests (Friedman, 1937) were carried out. Friedman statistical test is used to determine whether there is a statistically significant difference between the means of three or more groups in which the same subjects appear in each group or not. As the Friedman test is the non-parametric alternative to the one-way ANOVA with repeated measures, the test for normal distribution is done first. The most common analytical test to check data for normal distribution is Kolmogorov-Smirnov test. Before proceeding the test for normal distribution, the null hypothesis for testing is given, as follows:

Null hypothesis (**H<sub>0</sub>**): Data are normally distributed (a normal distribution is assumed) ( $p\text{-value} < 0.05$ ).

Friedman non-parametric test is applied to test the difference of the research sample in the pre-test, post-test, and the post post-test regarding the score of points that the respondents achieved. The hypothesis is set, as follows:

Null hypothesis: There is no difference between dependent variables pre-test, post-test, and post-post-test.

Alternative hypothesis: There is a difference between dependent variables pre-test, post-test, and post-post-test.

Friedman test proceeded by means of Datatab.net statistics allows to get a statement about whether the dependent groups differ significantly from each other, respectively it shows whether the two instructive lessons have any impact on the results achieved in post-testing and post post-testing. For the calculation of the Friedman test, not the mean values of the dependent groups are compared, but the rank sums. It is used to detect differences in treatments across multiple test attempts. The procedure involves ranking each row (or block) together, then considering the values of ranks by columns.

Consequently, Spearman correlation analysis is used to calculate the relationship between two variables that have an ordinal level of measurement. Spearman rank correlation is the non-parametric correlation analysis (Dickhaus, 2018). The calculation of the rank correlation is based on the ranking system of the data series. This means that the measured values are not used for the calculation but are transformed into ranks. The test is then performed using these ranks (Smalheiser, 2017). Again, it is convenient to set null and alternative hypotheses, as follows:

Null hypothesis: There is no association between pre- and post-test.

Alternative hypothesis: There is an association between pre- and post-test.

Regression is a statistical method that allows modeling relationships between a dependent variable and one or more independent variables.

**Table 1.** Basic statistical data analysis

	Pre-test	Post-test	Post-post-test
Mean	5.36	6.87	7.22
Median	5	5	5
Standard deviation	2.01	1.85	1.47
Minimum	2	4	4
Maximum	9	10	10

A certain probability of error that the null hypothesis is rejected even though it is actually true cannot be excluded. This probability of error is called the significance level or  $\alpha$ . The significance level is used to decide whether the null hypothesis should be rejected or not. To ensure a certain degree of comparability, the significance level is usually 5% or 1%, respectively not significant or highly significant. It defines whether the null hypothesis is assumed to be accepted or rejected. It is expected to identify if the result is statistically significant for the null hypothesis to be false or rejected.

While a p-value can tell you if there is an effect, it will not tell how large that effect is. In order to extend the comprehension of data results it is relevant to proceed with effect size (measure for effect size is Cohen's  $d$  (Cohen, 1960), a magnitude of the difference between groups calculated, as follows (Sullivan et al., 2012):

$$d = \frac{\bar{x}_1 - \bar{x}_2}{\sqrt{\frac{s_1^2 + s_2^2}{2}}}$$

where  $d$  is Cohen's  $d$  effect size,  $X_1$  and  $X_2$  means of the two groups,  $s_1$  and  $s_2$  are standard deviations of the two groups. An effect size is how large an effect is, it measures the effect size of the difference between two means: pre-test and post-test. A Cohen's  $d$  of 0.200 be considered a 'small' effect size, a Cohen's  $d$  of 0.500 be considered a 'medium' effect size, and a Cohen's  $d$  of 0.800 be considered a 'large' effect size.

A Pearson correlation is a statistical measure of the strength and direction of the linear relationship between two metric variables, in the present research it is the relation between the data resulting from pre-testing and post-testing. It measures the degree of association between two variables and indicates whether they are positively or negatively correlated.

Regression analysis is a statistical method that allows examining the relationship between two or more variables. The regression analysis examines the influence of one or more independent variables on a dependent variable. A linear regression analysis is performed to examine the influence of the variable pre-test on the variable post-test.

A particular regression model that is designed to consider the nested structure of the data is hierarchical linear modeling (Leyland & Goldstein, 2001). Hierarchical linear modeling can be used to find out what similarities are present in the data (Shi et al., 2021).

## RESULTS

Following lines present the outcomes of the statistical analysis of testing. **Table 1** gives an overview of obtained statistical data.

The median divides the number of correct answers into equal parts. In all testing rounds the median stays the same at number five. That's to say that the level of cybersecurity awareness stays at the interface. In the analyzed sample of school children, the level of cybersecurity awareness reports balanced values in the course of three stages of testing. The pre-testing shows that school children are directed consciously or by implicit habits in their online social media behavior but there are serious risks to be get attacked by any cyber risks mentioned in the introduction (Feng & Xie, 2014).

As per **Table 1**, mean slightly increases, which can be interpreted as a very moderate improvement in cyber security skills. In the case of pre-testing the standard deviation was the furthest from the mean, while the post-testing and post post-testing show lower standard deviation. In the case of pre-testing the level of differences in achieving the right answers differed more while after the training the rate of correct answers approaches. The smaller the standard deviation is the more the level of correct answers converges. This indicates that values are clustered closer to the mean.

**Table 2.** Data distribution

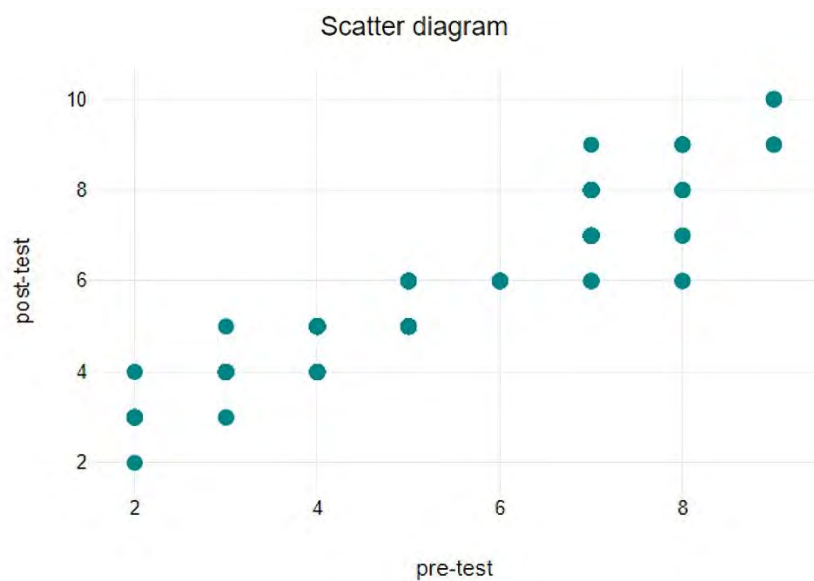
Kolmogorov-Smirnov test	Degrees of freedom	p-value
Pre-test	0.16	.005
Post-test	0.17	.002
Post post-test	0.20	<.001

**Table 3.** Friedman non-parametric test results

Study tools	Study sample mean rank	Chi-square	Degrees of freedom	p-value
Pre-test	1.5	39.86	2	<.001
Post-test	2.2			
Post-post-test	2.3			

**Table 4.** Spearman correlation

	r	p-value (2-tailed)
Pre- & post-test	0.94	<.001

**Figure 2.** Scatter diagram of Spearman correlation (Source: Authors, using DATATab)

The following results of tests for normal distribution, spearman correlation, and pairwise comparison enable to answer the second research question. Kolmogorov-Smirnov test was used to assess whether there is a normal distribution of data (Table 2).

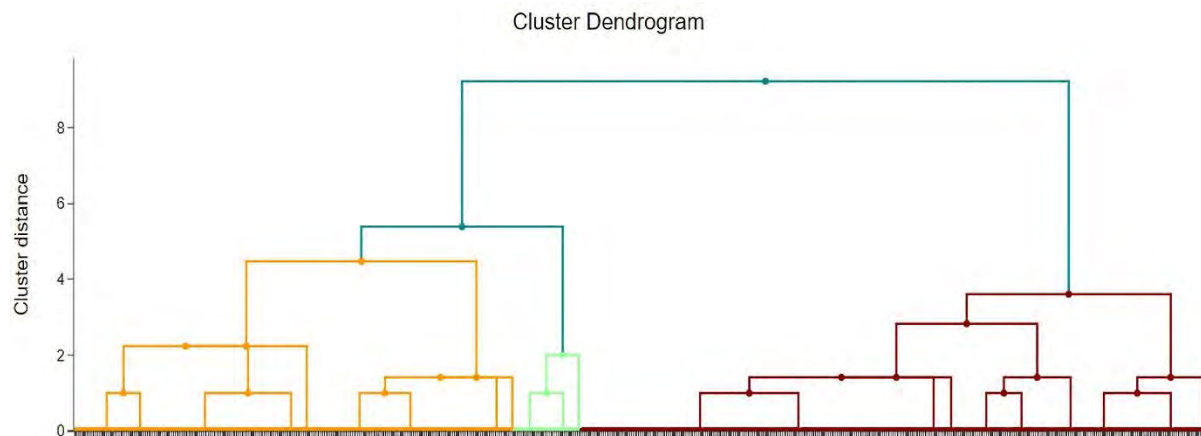
If the p-value is smaller than 0.05, there is a significant deviation from the normal distribution, and it is assumed that the data are not normally distributed. In this case, the null hypothesis  $H_0$  is approved, and Friedman test is employed to analyze the data for the closed-ended questions. Friedman test tests for differences between the different questioning when the dependent variable being measured is ordinal (Smalheiser, 2017) and whether there are statistically significant differences between three dependent samples: pre-test, post-test, and post-post-test. In the research sample, the values are dependent as the sample is drawn from respondents who replied three times. This is the case because the same person was tested at multiple time points. Table 3 shows the outcomes of Friedman test. There was a significant difference between the dependent variables,  $p \leq .001$  and level of significance is 0.05.

The mean ranks, which were 2.2 and 2.3, respectively exceed mean rank of the pre-test (1.5). This indicates a slightly positive effect of training on school children's cybersecurity awareness. A Spearman correlation was performed to test whether there was an association between pre- and post-test (Table 4).

The result of Spearman correlation showed that there was a significant association between the pre-test and post-test:  $r(101)=0.94$ ,  $p \leq .001$ . The scatter diagram shows the positive correlation (Figure 2).

**Table 4.** Pairwise comparison

	Test statistics	Standard error	Standard test statistics	p-value	Adjusted p-value
Pre-test × post-test	-0.71	0.14	-5.09	<.001	<.001
Pre-test × post-post-test	-0.71	0.14	-5.78	<.001	<.001
Post-test × post-post-test	-0.10	0.14	-0.70	.486	1.00

**Figure 3.** Cluster dendrogram (Source: Authors, using DATATab)

There is a very high, positive correlation between the variables pre- and post-test with  $r=0.94$  and there is a very high, positive association between pre- and post-test in this sample. Therefore, the null hypothesis is rejected. To complete the testing, a pairwise comparison is undertaken in [Table 4](#).

In each row, the null hypothesis (**H<sub>0</sub>**. There is no difference between the dependent variables pre-test, post-test, and post-post-test.) is tested. The “adjusted p-value” is obtained by multiplying the p-value by the number of tests. By means of the pairwise comparison, it is possible to determine whether there are significant differences between the dependent variables. The testing confirms the null hypothesis. Whereas association is a very general relationship: one variable provides information about another. Correlation is more specific; it describes the degree to which two variables move in coordination with one another. Moreover, a Pearson correlation was performed to test whether there is an association between pre-test and post-test. The result of the Pearson correlation showed that there was a significant association between pre-test and post-test,  $r(643)=0.84$ ,  $p\leq.001$ . Therefore, there is a very high, positive correlation between the variables pre- and post-test with  $r=0.84$ .

To indicate the standardized difference between the two means Cohen's  $d$  was used. The calculated difference between the means of outcomes of pre-testing and post-testing is 0.25, which is reported to be small. This means that the results of respondents' answers after the educational intervention resulted in only a very small effect and thus the improvement of cyber security awareness is insignificant.

The regression model showed that the variable pre-test explained 71.24% of the variance from the variable post-test. An ANOVA was used to test whether this value was significantly different from zero. By means of the DATATab calculator it was found that the effect was significantly different from zero:  $F=1,592.54$  (F-test tests the overall significance in regression models, determines whether a set of means are all equal),  $p\leq.001$ . The obtained regression model is, as follows:  $\text{post-test}=2.71+0.78\times\text{pre-test}$ .

When all independent variables are zero, the value of the variable post-test is 2.71. If the value of the variable pre-test changes by one unit, the value of the variable post-test changes by 0.78. By means of the regression model, the dependence of the dependent variable is found to be significant, which means that the achieved results in the post-testing manifest strong dependence of data obtained from pre-testing on data obtained from post-testing.

A particular regression model that is designed to consider the nested structure of the data is hierarchical linear modeling. It represents the relationships between independent and dependent variables, respectively scores of pre-testing and post-testing, and shows how the total score is clustered at different levels (Leyland & Goldstein, 2001). Hierarchical linear modeling can be used to monitor the determination of the relationship



between a dependent variable, which is the test score in the present study and an independent variable, which is gender. The clusters are visually represented in a hierarchical tree called a dendrogram. The dendrogram visualizes two key pieces of information about the measured group: which points are grouped together and the similarity of members of the group. Groups are shown through the X line; the Y line shows the distance between the group members. The cluster dendrogram is shown in [Figure 3](#).

Branches of dendrogram are called clades. While the arrangement of the clades tells which leaves of the dendrogram are most similar to each other, the distance between the subsuming clusters is recorded in the y-axis. The height of the branch points indicates the similarity or dissimilarity: the greater the height, the greater the difference. [Figure 3](#) shows that there is a number of pairs of samples under cluster distance two that are fairly close, while there are some entirely separated samples from all others. As maximum method is used, all samples clustered below a particular level of dissimilarity will have inter-sample dissimilarities less than that level. Consequently, five is the point at which samples are exactly as similar to one another as they are dissimilar, within each cluster the samples have more than 50% similarity. The hierarchical linear modeling analysis reveals that the post-testing score is supposed to be very close, similar to the pre-testing score.

### Summary of the Results

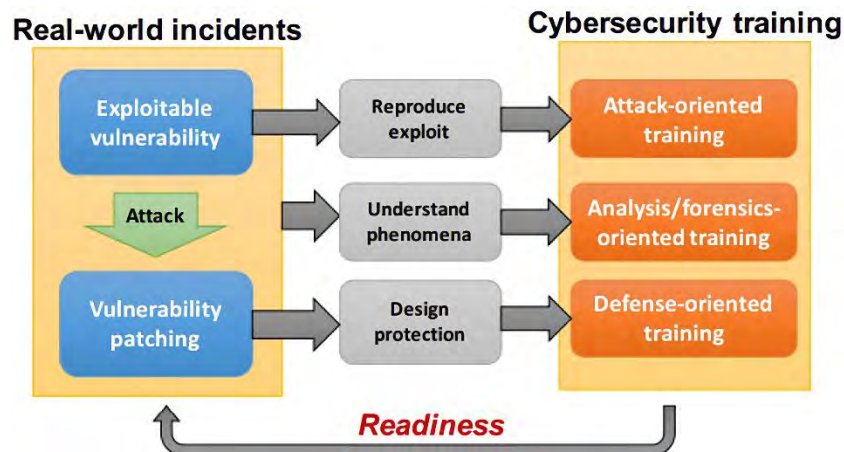
The described statistical indicators give an answer to the first research question. The level of cybersecurity awareness of school children stays at medium levels. Children have basic knowledge of cybersecurity risks, but they are guided more by their intuition as the level of correct answers does not change significantly in the course of three testing levels. Their behavior in an online environment is directed mainly by their intuition, respectively by the unconscious emotional information emanating from the body or brain such as instinctive thinking or sensation (Khalifa, 2000). But this cannot be considered to be the safe method for detecting online risks and has no empirical grounding (Al Zou'bi, 2022).

In response to the second research question, the results of the pre-test identified statistically significant differences between the averages of the measures (pre- and post-tests). The results of this research highlighted only the negligible impact of instructive lessons on children's cyber security awareness. This aligns with the findings of research done on adults that used interventions to raise cybersecurity awareness (Amo et al., 2019, Vanderhoven et al., 2015). These studies also performed comparisons on adults between different types of interventions adopted two time-based approaches; one was a 60-minute workshop and the other one was a five-day long cybersecurity camp. The results show that the longer five-day intervention demonstrated promising results, whereas, in the short and less intense intervention, the students did not demonstrate growth in cyber awareness. By means of applying the hypothesis testing an insignificant positive impact of even short-time training on enhancing children's cybersecurity was revealed. The pairwise comparison shows that after the children received the cyber security training the results from the post-test and post post-test do not change significantly. This demonstrated that it is necessary to pay attention to more systematic and structured training in school-age. Correlation analysis confirms strong dependence of tested variables, which shows only a small effect of the training. Moreover, the cluster analysis demonstrates that the post-testing score is supposed to be very close, similar to the pre-testing score and thus manifest important similarities.

As per Tsirtsis et al. (2016), the risks like online harassment, privacy invasion, technology-based threats are significant cyber security risks for children. The significant finding of the current research is that cyber security awareness among Czech school children stays the medium levels. Children are aware of risks resulting from virtual environment, but they behave intuitively and do not seize the variety of risks, which spreads through the virtual environment. With the short time training, it is possible to focus only on a few specific risks. Thus, the results of the testing confirm that there is an urgent need for more robust, deep and complex interventions in the cyber security training.

## DISCUSSION

The present paper clearly shows the importance and need for cyber security training at schools. It shows the insufficient level of cyber security awareness of school children. The findings are helpful to both the schools when adapting their curriculum to implement courses involving cybersecurity matters and to the



**Figure 4.** Paradigm of strategies (McGettrick, 2013)

tutors who design the content of training for children. The present research confirms that it is useful to concentrate on different techniques to raise awareness of various cyber security risks. There is an urgent need for structured and more developed models and frameworks for designing the training including different approaches along with conventional training or classroom teaching to raise cybersecurity awareness to strengthen, increase or maximize the effectiveness.

### Implications for Research and Practice

Having explored the outcomes and the impact of one-off cyber security training and based on the literature the following lines give an approach to an effective cyber security education for school children. The aim of the present paper is also to give examples of good practices to settle a new approach for effective involvement of cyber security matters in the daily teaching routine.

First, it is necessary to identify what are the addressed risks for children. To be sure to cover most of the risky behavior it is useful to copy reality and to concentrate on real-world incidents, on what are the weaknesses and the vulnerable areas of school children. Based on this identification it is useful to investigate continuously how to attract children's attention. It is important to keep in mind when creating learning strategies that children do not wait or rely on the classes to learn new online skills (Taylor et al., 2017). On the contrary, they behave intuitively and dive into every online adventure themselves and hardly anytime wait for school to discover. That is in line with the outcomes of the present research that shows only a limited impact of the one-off training courses on online behavior. That kind of training did not transfer enough cyber security awareness skills. On the contrary, good multi-task preparation for risky cyber environments deserves a multi-task wide range of activities realized over the course of the whole school year and throughout all the subjects taught at school. The applied strategies might exploit different techniques and strategies. These might be storytelling (Lastdrager et al., 2017), digital comics (Zhang-Kennedy et al., 2017), or games (Chugh & Turnbull, 2023). Children are more interested in games and media, and using gamification for training seems to be a good and effective technique for them (Kaban, 2021).




To be sure to cover most of the risky behavior it is useful to copy reality and concentrate on real-world incidents, what are weaknesses, and vulnerable areas. **Figure 4** shows the paradigm of strategies to elaborate appropriate techniques to work on.

The activities should be focused on a critical evaluation of the information that children consume online. The increasing use of social media for information sharing calls upon the need for information literacy education to better prepare students to effectively process information.

### Examples of Good Practice

The task is to make young people behave naturally and cautiously, promote skeptical, and save judgments about the content they encounter. This would allow them to better identify outright lies, scams, hoaxes, selective half-truths, and mistakes and to encourage independent thinking.

**Table 5.** Examples from the teaching practice

Practice	Couse	Question	Example
Fact-checking	Science	Can you meet them?	 <p><a href="https://www.brainson.org/episode/2022/04/26/what-makes-tiny-tardigrades-tick">https://www.brainson.org/episode/2022/04/26/what-makes-tiny-tardigrades-tick</a></p>
Magic of photograph	Arts	Einstein: Bicycles as a-bomb explodes?	 <p><a href="https://www.snopes.com/fact-check/einstein-bicycle">https://www.snopes.com/fact-check/einstein-bicycle</a></p>
Find mistake	Languages	What is wrong?	
Who earns most?	Mathematics	What bank deposit would you choose ?	<p><u>You have 100 USD.</u></p> <p>Bank A offers me 1 USD per month tax included.            Bank B offers me 10 USD per year tax excluded.            Bank C offers me 1% per month tax excluded.            Bank D offers me 10% per year tax included.</p>

It is a set of complex activities that are supposed to be brought up repeatedly and from different points of view. It is as well important that all members of the teaching staff are involved and implement the cyber security teaching practice in their everyday teaching routine.

**Table 5** shows examples of implementing cyber security task in different lessons. To process of building and strengthening critical thinking can be promoted across all school subjects and can be thus much more efficient on cyber security awareness.

The activities might be involved different tasks. For example, during the lessons of Arts children may play with their own photographs and edit them so that they know how easy it is to fake the pictures. The lessons of mathematics may change in the financial market, where children trade with financial assets and explore the law of supply and demand and balance risks and profits. The variety of activities and creating immersive learning experiences by living the true stories promote the spirit of self-education to grow. This is the key point of the new approach to cyber security awareness. Tasks must be designed to develop critical thinking and to make children feel the need to check the information or message on their own. They are based on continual self-development by promoting curiosity and to start to look at things from different points of view.

## CONCLUSIONS

Over the last decades, the Internet has been considered a powerful and great source of information, distraction, and a tool of communication. The impact on society including children in the form of risks and dangers is increasing. On the one hand amount of material available at the click of a mouse can be both useful

for education and instruction on the other hand the virtual world is a source of danger. The present study reported the high importance of cyber security training in schools.

This paper investigated the effects of one-off training courses in cyber security awareness on a sample of 645 school children. The questionnaire with certain variations was presented in the form of a current online communication in three rounds with an intervention of the cyber security training after the first round. The results are greatly affected by the children's self-awareness of cyber security while being resistant to sophisticated cyber-attacks. The consequences of the outcomes of the training are affected by other limiting factors such as personal experiences or lack of concentration when realizing the testing. These factors could be hardly restrained and may cause potential biases when interpreting the results of the one-off training effectiveness. It should be considered as well that 38 participants out of 770 that had initiated the survey had to be excluded due to their absence while 87 pupils (11.3%) had to be excluded for not having finished the testing properly. This limitation is partly eliminated by a large number of respondents.

The level of cyber security awareness that was found achieved medium values before training. The short time training did not show any significant impact on children's knowledge compared to the knowledge acquisition before the training. The effectiveness of short-term training is reported to be low and not satisfactory. These results are consistent with the research done by Lastdrager et al. (2017). The reasons for these poor results include the contradiction of the variety of risks spreading in the virtual environment on hand and superficial and insufficient time devoted to the training.

Nowadays, children of school age live in digitally mediated environments and digital technologies are an integral part of their lives. Therefore, digital technologies must become as well an integral part of the educational processes. It is essential to implement the educational elements for online safety directly into the lessons to create and extend safer online environments. The framework for online safety education should be based on recognizing, acknowledging, and understanding rights and responsibilities especially among school-age children and teenagers. In the present research, the separate teaching about the risks of harm in cyberspace did not appear to be effective. On the contrary, the implementation of online safety education in the lessons seems to frame better the use of technology when building awareness of factors that decreases the risks of harm. An important message results from the present research for policymakers. The framework for cybersecurity education must be shifted from separate courses directly towards daily teaching lessons in a consistent manner. For successful implementation, it is necessary to adopt as well an effective tool for the assessment of the cybersecurity capabilities of pupils as the dangers and risks gradually increase. As the future evolution of the risks deserves the evaluation of cyber security awareness in a more consistent manner adopted and carried out on the national level the attention of future research should be directed towards effective metric tools to detect the weaknesses of new potential online risks and dangers.

**Author contributions:** All authors were involved in concept, design, collection of data, interpretation, writing, and critically revising the article. All authors approve final version of the article.

**Funding:** This article was supported by the Grant of Faculty of Arts, Palacký University Olomouc: IGA\_FF\_2023\_024 Entrepreneurial solutions to social problems.

**Ethics declaration:** The authors declared that the study's use of data is from the existing literature that is freely accessible and did not require ethics committee permission.

**Declaration of interest:** Authors declare no competing interest.

**Data availability:** Data generated or analyzed during this study are available from the authors on request.

## REFERENCES

---

- Al Zou'bi, R. M. (2022). The impact of media and information literacy on students' acquisition of the skills needed to detect fake news. *Journal of Media Literacy Education*, 14(2), 58-71. <https://doi.org/10.23860/JMLE-2022-14-2-5>
- Alwanain, M. I. (2021). How do children interact with phishing attacks? *International Journal of Computer Science & Network Security*, 21(3), 127-133. <https://doi.org/10.22937/IJCSNS.2021.21.3.17>
- Amo, L. C., Liao R., Frank, E., Rao, H. R., & Upadhyaya, S. (2019). Cybersecurity interventions for teens: Two time-based approaches. *IEEE Transactions on Education*, 62(2), 134-140. <https://doi.org/10.1109/TE.2018.2877182>

- Ascott, T. (2020). *Is media literacy the magic bullet for fake news?* The Interpreter.
- Celliers, M., & Hattingh, M. (2020). A systematic review on fake news themes reported in literature. In M. Hattingh, M. Matthee, H. Smuts, I. Pappas, Y. K. Dwivedi, & M. Mäntymäkin(Eds.), *Responsible design, implementation and use of information and communication technology* (pp. 223-234). Springer. [https://doi.org/10.1007/978-3-030-45002-1\\_19](https://doi.org/10.1007/978-3-030-45002-1_19)
- Chugh, R., & Turnbull, D. (2023). Gamification in education: A citation network analysis using CitNetExplorer. *Contemporary Educational Technology*, 15(2), ep405. <https://doi.org/10.30935/cedtech/12863>
- Cortesi, S., Hasse, A., Lombana-Bermudez, A., Kim, S., & Gasser, U. (2020). Youth and digital citizenship+ (plus): Understanding skills for a digital world. *Berkman Klein Center Research Publication, 2020-2*, 1-91. <https://doi.org/10.2139/ssrn.3557518>
- Feng, Y., & Xie, W. (2014). Teens' concern for privacy when using social networking sites: An analysis of socialization agents and relationships with privacy-protecting behaviors. *Computers in Human Behavior*, 33, 153-162. <https://doi.org/10.1016/j.chb.2014.01.009>
- Finkelhor, D., Walsh, K., Jones, L., Mitchell, K., & Collier, A. (2021). Youth Internet safety education: Aligning programs with the evidence base. *Trauma Violence & Abuse*, 22(5), 1233-1247. <https://doi.org/10.1177/1524838020916257>
- Giannakas, F., Papasalouros, A., Kambourakis, G., & Gritzalis, S. (2019). A comprehensive cybersecurity learning platform for elementary education. *Information Security Journal: A Global Perspective*, 28(3), 81-106. <https://doi.org/10.1080/19393555.2019.1657527>
- Khalifa, A. L. (2000). *Intuition and creativity*. Gharib Publishing House.
- Lamond, M., Renaud, K., Wood, L., & Prior, S. (2022). SOK: Young children's cybersecurity knowledge, skills & practice: A systematic literature review. In *Proceedings of the 2022 European Symposium on Usable Security* (pp. 14-27). <https://doi.org/10.1145/3549015.3554207>
- Lastdrager, E., Gallardo, I.C., Hartel, P., & Junger, M. (2017). How effective is {anti-phishing} training for children? In *Proceedings of the 13<sup>th</sup> Symposium on Usable Privacy and Security* (pp. 229-239).
- Leyland, A. H., & Goldstein, H. (2001). *Multilevel modelling of health statistics*. John Wiley & Sons.
- Liao, T., & Lin, I. (2017). A survey of Blockchain Security Issues and Challenges. *International Journal of Network Security*, 19(5), 653-659.
- Lorenz, B., Kikkas, K., & Osula, K. (2018). Development of children's cyber security competencies in Estonia. In P. Zaphiris, & A. Ioannou (Eds.), *Learning and collaboration technologies. Learning and teaching* (pp. 473-482). Springer. [https://doi.org/10.1007/978-3-319-91152-6\\_36](https://doi.org/10.1007/978-3-319-91152-6_36)
- Mason, L. E., Krutka, D., & Stoddard, J. (2018). Media literacy, democracy, and the challenge of fake news. *Journal of Media Literacy Education*, 10(2), 1-10. <https://doi.org/10.23860/JMLE-2018-10-2-1>
- McGettrick, A. (2013). Toward effective cybersecurity education. *Security and Privacy Magazine*, 11(6), 66-68. <https://doi.org/10.1109/msp.2013.155>
- McKnight, K., O'Malley, K., & Bassett, K. (2016). Teaching in a digital age: How educators use technology to improve student learning. *Journal of Research on Technology in Education*, 48(3), 194-211. <https://doi.org/10.1080/15391523.2016.1175856>
- Mehta, K. (2022). *Should cybersecurity be made part of the school curriculum?* World Economic Forum.
- Mrah, I., & Tizaoui, H. (2018). The rise of misinformation in the digital age: Moroccan students' attitudes and perceptions of fake news online. *Journal of English Language Teaching and Linguistics*, 3(2), 117-135. <https://doi.org/10.21462/jeltl.v3i2.137>
- Page, B. (2019). 9 steps to successfully detect fake news. *Better Marketing*. <https://bettermarketing.pub/9-ways-to-detect-fake-news-an-insiders-guide-61aa425f5a6f>
- Patterson A., Ryckman L., & Guerra C. (2022). A systematic review of the education and awareness interventions to prevent online child sexual abuse. *Journal of Child & Adolescent Trauma*, 15, 857-867. <https://doi.org/10.1007/s40653-022-00440-x>
- Penncheva, D., Hallett, J., & Rashid, A. (2020). Bringing cyber to school: Integrating cybersecurity into secondary school education. *IEEE Security and Privacy Magazine*, 18(2), 68-74. <https://doi.org/10.1109/MSEC.2020.2969409>
- Qiu, X., Diego, O., Sherazi, A., Flammini, A., & Filippo M. (2017). Limited individual attention and online virality of low-quality information. *Human Nature*, 1(7), 1-7. <https://doi.org/10.1038/s41562-017-0132>

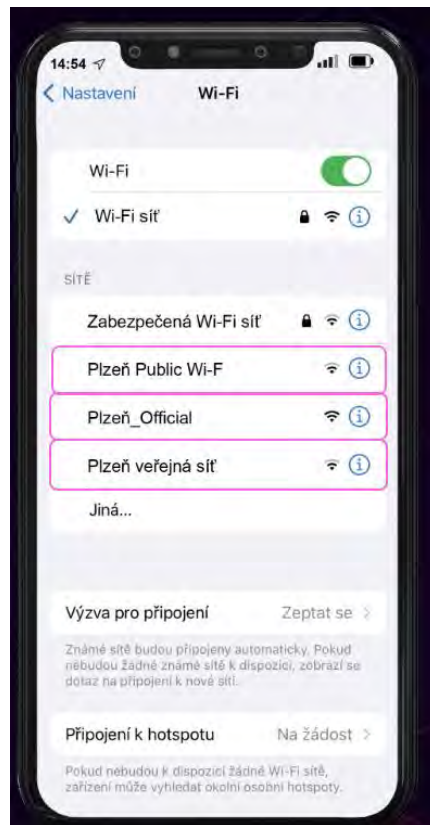
- Quayyum, F., Cruzes, D. S., & Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction*, 30, 100343. <https://doi.org/10.1016/j.ijcci.2021.100343>
- Shamsi, A. (2019). Effectiveness of cyber security awareness program for young children: A case study in UAE. *International Journal of Information Technology and Language Studies*, 3(2), 8-29. <https://doi.org/10.13140/RG.2.2.28488.14083>
- Shi, C., Wei, B., Wei, S., Wang, W., & Liu, H. (2021). A quantitative discriminant method of elbow point for the optimal number of clusters in clustering algorithm. *EURASIP Journal on Wireless Communications and Networking*, 31. <https://doi.org/10.1186/s13638-021-01910-w>
- Smalheiser, N. (2017). *Data literacy: How to make your experiments robust and reproducible*. Academic Press.
- Sullivan, G., & Feinn, R., (2012). Using effect size—or why the P value is not enough september. *Journal of Graduate Medical Education*, 4(3), 279-82. <https://doi.org/10.4300/JGME-D-12-00156.1>
- Taylor, J., McAlaney, J., Hodge, S., Thackray, H., & Richardson, C. (2017). Teaching psychological principles to cybersecurity students. In *Proceedings of the IEEE Global Engineering Education Conference* (pp. 1782-1789). IEEE. <https://doi.org/10.1109/EDUCON.2017.7943091>
- Tsirtsis, A., Tsapatsoulis, N., Stamatelatos, M., Papadamou, K., & Sirivianos, M. (2016). Cyber security risks for minors: A taxonomy and a software architecture. In *Proceedings of the 11<sup>th</sup> International Workshop on Semantic and Social Media Adaptation and Personalization* (pp. 93-99). <https://doi.org/10.1109/SMAP.2016.7753391>
- Vanderhoven, E., Willems, B., Van Hove, S., All, A. & Schellens, T. (2015). Wait and see? studying the teacher's role during in-class educational gaming. In *European Conference on Games Based Learning* (pp. 540-547).
- Venter, I. M., Blignaut, R. J., Renaud, K., & Venter, M. A. (2019). Cyber security education is as essential as “the three R's”. *Heliyon*, 5(12), ep02855. <https://doi.org/10.1016/j.heliyon.2019.e02855>
- Waldock, K. E., Miller, V., Li, S., & Franqueira, V. (2022). *A report on developing cyber skills amongst children and young people*. Institute of Cyber Security for Society, University of Kent.
- Winter, E., Costello, A., O'Brien, M., & Hickey, G. (2021). Teachers' use of technology and the impact of COVID-19. *Irish Educational Studies*, 40(2), 235-246. <https://doi.org/10.1080/03323315.2021.1916559>
- Zhang-Kennedy, L., Abdelaziz, Y., & Chiasson, S. (2017). Cyberheroes: The design and evaluation of an interactive ebook to educate children about online privacy. *International Journal of Child-Computer Interaction*, 13, 10-18. <https://doi.org/10.1016/j.ijcci.2017.05.001>
- Zhao, G. W., Dally, C., Slovak, P., Edbrooke-Childs, J., Van Kleek, M., & Shadbolt, N. (2019). 'I make up a silly name': Understanding children's perception of privacy risks online. In *Proceedings of the 2019 Conference on Human Factors in Computing Systems*, (pp. 1-13). ACM. <https://doi.org/10.1145/3290605.3300336>

APPENDIX A: SAMPLE TEST ASSIGNMENT

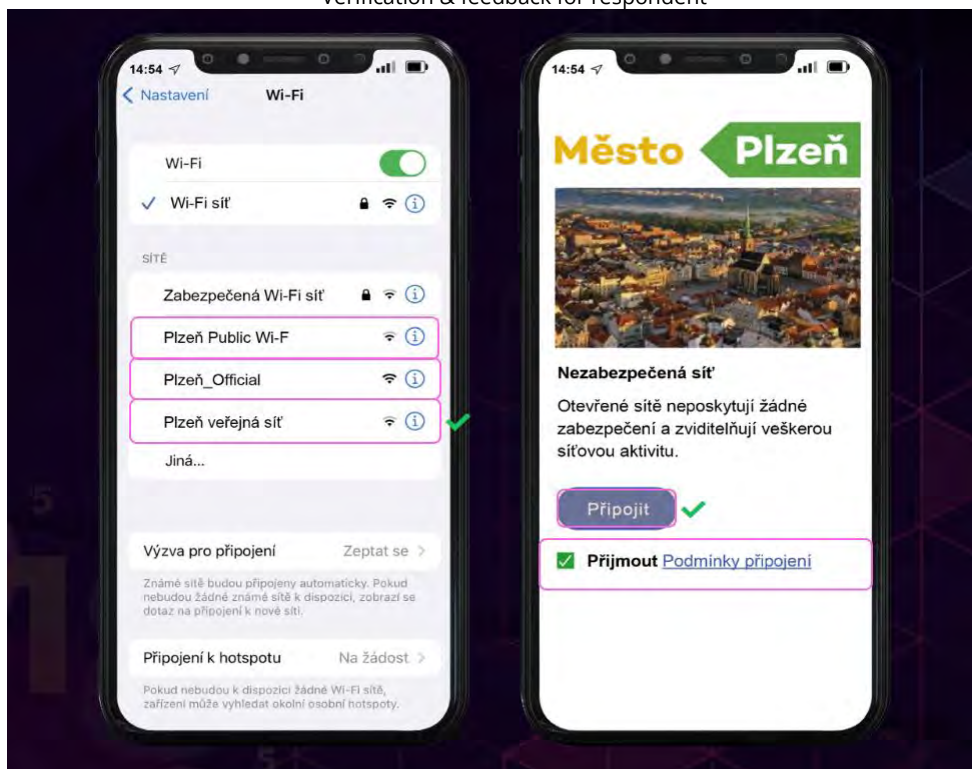
Identification of the participant:  
 Nickname  
 Telephone number  
 Address & bank account



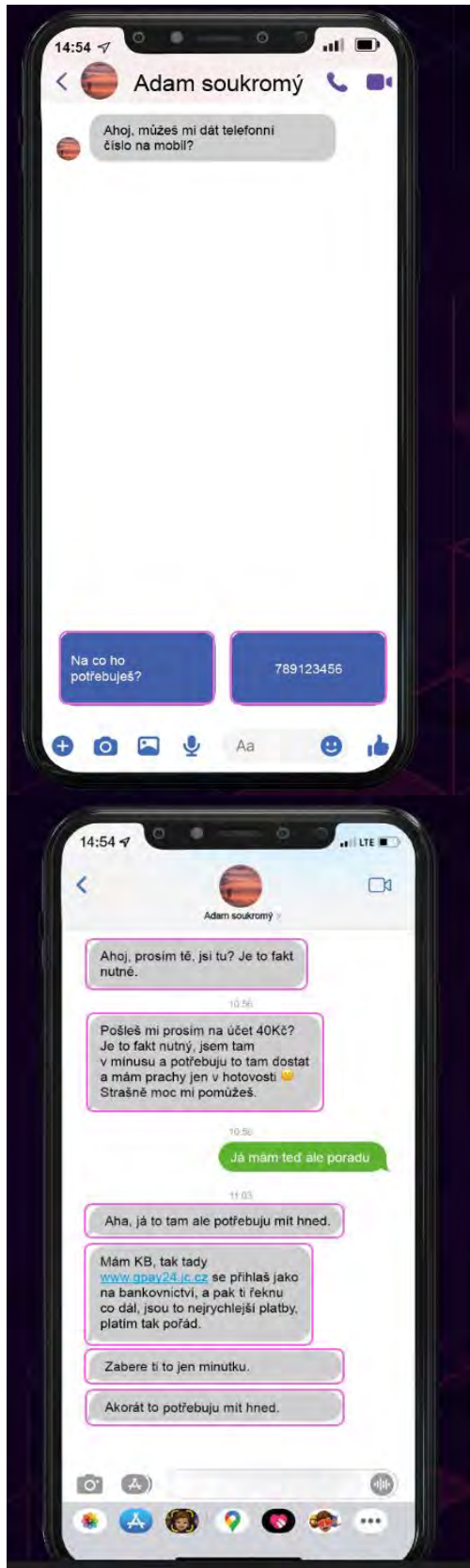
Sample of question asking to choose the safest public network to connect (feedback is received after having made choice)



Verification & feedback for respondent



Simulation of online communication



The participants are asked to choose the right answer with respect to security rules.

The question is: Hello, can you give me your personal telephone number?

Pupils can choose: Either:

Hey, what do you need it for?

Or: they write their number without asking the reason

Another type of conversation asking for personal data and insisting on fast response. The respondents are supposed to choose the appropriate answer.

