© University Press 2023
ISSN 2719-6550
ISSN 2719-7417 online

“Journal of Education, Technology and Computer Science”
No. 4(34)/2023
www.eti.ur.edu.pl

Received: 23.12.2022
Accepted for printing: 15.12.23
Published: 29.12.2023
License: CC BY-SA 4.0

DOI: 10.15584/jetacomps.2023.4.16

HELENA MIČKOVÁ[1], JANA MIKOVÁ[2], ZDENKA NOVÁKOVÁ[3], JAN ŠMIDA[4]

Pupils’ Risky Behavior in the Cyberspace During the Transition to Distance Education

[1] ORCID: 0000-0002-8235-9599, JUDr. Mgr. Helena Mičková, Palacký University Olomouc, Faculty of Education, The Institute of Education and Social Studies, Czech Republic.
[2] ORCID: 0000-0001-5322-1876, Mgr. Jana Miková, Palacký University Olomouc, Faculty of Education, The Institute of Education and Social Studies, Czech Republic.
[3] ORCID: 0000-0002-3867-8314, JUDr. Zdenka Nováková, Ph.D., Palacký University Olomouc, Faculty of Education, The Institute of Education and Social Studies, Czech Republic.
[4] ORCID: 0000-0002-1807-2884, Bc. Jan Šmída, Palacký University Olomouc, Faculty of Education, The Institute of Education and Social Studies, Czech Republic.

Abstract

In connection with the covid pandemic and the closing of schools as anti-covid emergency measures in many countries, face-to-face teaching has moved to an online environment.

The Ministry of Education, Youth and Sports of the Czech Republic has issued Methodological Recommendations for distance education realized online using software tools, the Internet, and digital technologies. The presented pilot study brought disturbing findings about online teaching, namely that respondents experienced threats during distance education, with some even being blackmailed. Three hundred fifteen respondents from elementary and secondary schools in the Czech Republic took part in the pilot study, which was realized via a questionnaire survey.

At the same time, the pilot study points to other risks of online learning when transitioning to a distance form of education, which also presents several other risks in cyberspace.

Keywords: distance learning, online learning, blackmail, threats, cyberspace risks

Research subject

Like many other European countries, the Czech Republic was forced to adopt anti-covid measures in connection with the education of primary and secondary school pupils when teaching moved to cyberspace. Primary and seconddary schools had to adapt to the current situation and, with the help of information and communication technologies (ICT), educate students at a distance. Until then, online or distance education had been used for lifelong adult education.

Piotrowski and Sliwa (2015) perceive today's world from a two-dimensional point of view, where real and cyber worlds are interconnected and interdependdent. This also characterizes the realization of the educational process, which was forced to move from the known real world to the unknown cyber world during the covid era.

Cyberspace can be characterized as a dynamically developing medium with many opportunities and threats that can attract various individuals aiming to exploit other people's vulnerability, unawareness, and trust. According to Kopecký and Krejčí (2010), the risks of virtual communication (communication in cyberspace) include, among others, cyberbullying, cyber grooming, stalking, and cyberstalking.

Distance education and online teaching, implemented through information and communication technologies in the cyberspace environment, represent possible risks and security threats during online teaching itself, which can interfere with the privacy of teachers and students. Over the past two years, primary and secondary school students and their teachers have been exposed to the digital environment many times more during the implementation of online teaching in connection with distance education.

With the increasing use of information and communication technologies in education, cybercrimes against children have also increased simultaneously (Prajapati, Kumar, 2022). Risky behavior not only in cyberspace is defined by Ostaszewski (2005) as behavior contrary to social norms and the legal order, which at the same time threatens human health and development. Online risky behavior can take many forms: making personal information available to others (Livingstone, Helsper, 2007, 2010), sharing visual material with the general public (Marcum, Ricketts, Higgins, 2010), engaging in online discussions with sexual overtones and vulgar comments (Ybarra, Mitchell, Finkelhor, Wolak, 2007), or establishing new friendships with unknown people (Livingstone, Helsper, 2007; Ybarra et al., 2007; Kopecký, Szotkowski, Krejčí, 2021). Adamski (2013) mentions anonymity, an unlimited range of users, and the universality of internet access as risky factors of behavior on the Internet with the possible development of cybercrime. Kopecký, Szotkowski and Krejčí (2021) consider, among other things, the use of fictitious identities, so-called equality of status, synchronous and asynchronous online communication, and social multiplicity in communication with an undetermined number of users to be risky.

Based on the initial questioning, threats, blackmail, and mockery during online teaching were found to be possible risky phenomena. We perceive those as possible threats during the implementation of online teaching.

Methodology

The introductory survey entitled “Selected risks of cyberspace during the transition of pupils to distance learning” focused on naming the possible risks of cyberspace that pupils of lower secondary schools, secondary schools, conservatories, and other schools of the Olomouc Region encountered during distance learning. As part of this research, we also found out what proportion of pupils encountered risky situations, such as blackmail or threats in cyberspace. The age range of the respondents varied between 13 and 19 years.

The initial questioning was implemented based on a ~~e~~quantitative research strategy. Data collection took place from 05/2022 to 07/2022 through a questionnaire survey, when online Google Forms questionnaires were used and shared among pupils of lower secondary and secondary schools. The obtained data were subsequently analyzed by statistical methods using MS Excel.

Research method:	Quantitative research method
Research tool:	Questionnaire survey
Research sample:	Lower secondary and secondary schools’ pupils
Data analysis:	Statistical data analysis

Research results analysis

It can be seen from the first graph that a large part (41.9%) of the pupils were not instructed in any way before or during online teaching about the risks that may exist in cyberspace. This can also be one of the factors behind the dangerous behavior of pupils on the Internet, as well as the high numbers in the field of cyberbullying, which the pupils themselves have experienced. If there was any instruction about safe behavior on the Internet, it was primarily provided by the school (32.1%), parents (22.9%), or the students’ teachers themselves (20.6%).

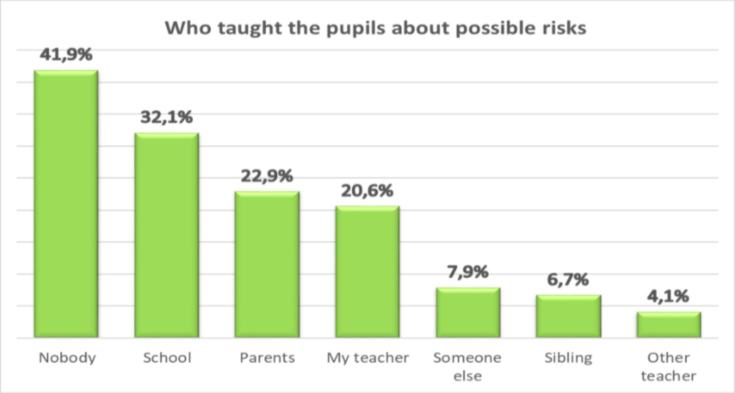

Figure 1

Source: our own research investigation.

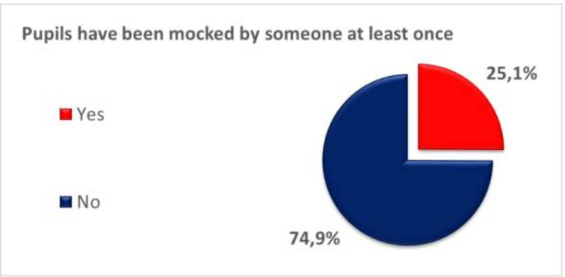

Figure 2

Source: our own research investigation.

Ridicule or mockery, which troubled pupils the most during distance learning, has long been the most widespread form of cyberbullying. This is also confirmed by Figure 2, which shows that up to 25.1% of pupils were mocked in some way during distance learning. That is, every fourth pupil.

However, risky behavior in cyberspace was not limited to ridicule. Figure 3 informs that during distance learning. Students also experienced hacking into their accounts (17.1%), misuse of their accounts (11.4%), or theft of personal data (8.6%). It is also quite alarming that 9.2% of pupils experienced threats during distance education, and even 9.5% were blackmailed. Of these, 3.8% of pupils experienced threats more than once, and 3.5% experienced blackmail more than once. Thus, almost every tenth student has become a victim of one or both forms of virtual attack. The question remains whether these percentages would be lower if the pupils were taught more, as described in Figure 1.

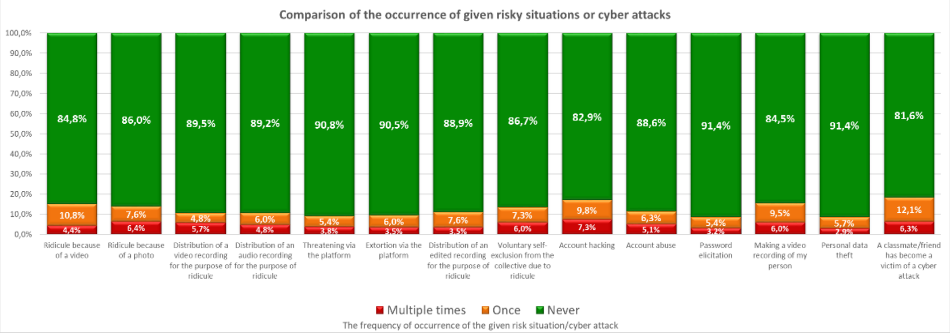

Figure 3

Source: our own research investigation.

Pupils were not only exposed to risky behavior but also behaved very risky themselves. This can be seen in chart No. 4. A relatively high percentage of pupils deliberately disrupted lessons in the online environment in various ways. For example, 17.8% of pupils (11.4% once, 6.4% multiple times) turned off their teacher's camera, and 16.2% (12.1% once, 4.1% multiple times) even disconnected the teacher himself from the lesson. If we focus on mockery, 8.9% of pupils (5.4% once, 3.5% more than once) admit to having shared mocking photos or videos of a teacher. Pupils are, therefore, the most frequent perpetrators of various cyberattacks or forms of cyberbullying.

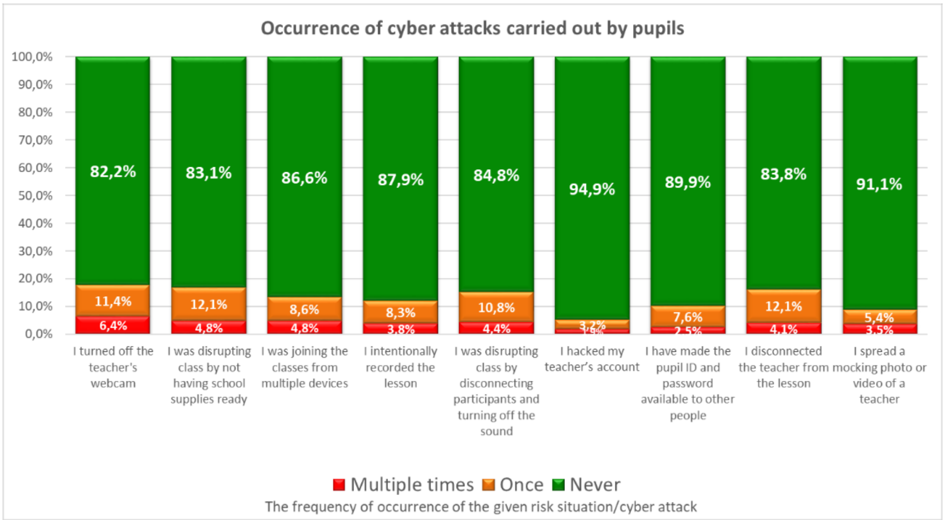

Figure 4

Source: our own research investigation.

Conclusions

The collected data represented by the charts clearly show that the pupils needed to be sufficiently instructed about safe behavior on the Internet, which could – and did – manifest itself in the frequency of various risky behaviors.

The following facts emerge from the data:

– 41.9% of pupils were not sufficiently trained in safe behavior on the Internet;

– 25.1% of pupils experienced ridicule or mockery at least once during distance education;

– 9.2% of pupils were threatened at least once, and 9.5% of pupils were even blackmailed online.

The preparation of pupils for online teaching should have been more sufficient. The low level of digital literacy and the ability to behave safely in cyberspace undoubtedly contributed to the intensity of various risky situations that students had to face during distance education, but also to how students dealt with non-standard situations.

From a long-term perspective and several contemporary pieces of research, it is evident that mockery is one of the most widespread forms of cyberbullying. This also follows from our research. However, special attention should also be paid to the other risks that cyberspace brings, such as the risk of blackmail or threats, as well as hackers breaking into someone's account and stealing personal and login data. According to research, the percentage of occurrences of risky behavior and risky situations among pupils is still very high, so it is necessary to constantly strengthen the digital competencies of pupils and teachers. The school and the parents, who allow their children to access various content on digital devices such as mobile phones or computers, should participate in this.

Security and especially prevention in cyberspace have been priorities of the 2030+ educational strategy in the Czech Republic (Fryč et al., 2020), in the context of digital literacy, digital competencies, and related educational goals. Thanks to technological trends, emphasis is simultaneously placed on improving quality, efficiency, and innovation in teaching. In contrast, a greater emphasis is placed on individualizing teaching and communicating with pupils through digital technologies.

Acknowledgements

The submitted article is part of the research project, internal grant IGA_PdF_2022_023 of the Palacký University in Olomouc, entitled: "Selected Risks of Cyberspace During the Transition of Pupils to Distance Education".

Reference

Adamski, A. (2003). Karnoprawna ochrona dziecka w sieci Internet. *Prokuratura i Prawo, 9,* 59–75.

Fryč, J., Katzová, P., Matušková, Z., Kovář, K., Beran, J., Valachová, I., Seifert, L., Běťáková, M., Hrdlička, F. (2020). *Education policy strategy of the Czech Republic until 2030+*. The Ministry of Education, Youth and Sports. Retrieved from: https://www.msmt.cz/uploads/Brozura_S2030_online_CZ.pdf (25.11.2023).

Kopecký, K., Krejčí, V. (2010). *Risks of virtual communication (a guide for teachers and parents)*. NET UNIVERSITY. Retrieved from: http://archiv.zsstipa.cz/informace/ke_stazeni/enebezpeci_a5_3.pdf (1.12.2023).

Kopecký, K., Szotkowski, R., Krejčí, V. (2021). *Risky communication and dating of Czech children in cyberspace*. Palacky University in Olomouc. Retrieved from: https://www.e-bezpeci.cz/index.php/ke-stazeni/odborne-studie/146-rizikova-komunikace-a-seznamovani-ceskych-deti--v-kyberprostoru-2021/file (1.12.2023).

Livingstone, S., Helsper, E.J. (2007). Taking risks when communicating on the internet: The role of offline social-psychological factors in young people's vulnerability to online risks. *Information, Communication and Society, 10*(5), 619–643. doi:10.1080/13691180701657998.

Livingstone, S., Helsper, E.J. (2010). Balancing opportunities and risks in teenagers' use of the internet: The role of online skills and internet self-efficacy. *New Media & Society, 12*(2), 309–329. doi:10.1177/1461444809342697.

Marcum, C.D., Higgins, G.E. Ricketts, M.L. (2010) Potential Factors of Online Victimization of Youth: An Examination of Adolescent Online Behaviors Utilizing Routine Activity Theory. *Deviant Behavior, 31*(5), 381–410. doi:10.1080/01639620903004903.

Ostaszewski, K. (2005). Podstawy teoretyczne profilaktyki zachowań problemowych. In: M. Deptuła (Ed.), *Diagnostyka, profilaktyka, socjoterapia w teorii i praktyce pedagogicznej* (pp. 111–137). Bydgoszcz: Wyd. Uniwersytetu Kazimierza Wielkiego.

Piotrowski, R., Sliwa, J. (2015). *Cyberspace Situational Awarness in National Security System* (2015 ed.). IEEE345 E 47TH ST, NEW YORK, NY 10017 USA.

Prajapati, K., Kumar, V. (2022). Digital Citizenship And Role of Teachers In Creating Responsible Digital Citizens. *International Journal of Early Childhood Special Education*, *14*(3), 1483–1488. doi:10.9756/INT-JECSE/VI413.172.

Ybarra, M.L., Mitchell, K.J., Finkelhor, D., Wolak, J. (2007). Internet Prevention Messages: Targeting the Right Online Behaviors. *Archives of Pediatrics and Adolescent Medicine, 161*(2), 138–145. doi: 10.1001/archpedi.161.2.138D.