Fostering Knowledge of Computer Viruses among Children

The Effects of a Lesson with a Cartoon Series

Katerina, Tsarava
katerina.tsarava@uni-tuebingen.de
Hector Research Institute for Education Sciences & Psychology, University of Tübingen
Tübingen, Germany

Manuel, Ninaus
manuel.ninaus@uibk.ac.at
Institute of Psychology, University of Innsbruck
Innsbruck, Austria

Tereza Hannemann
hannemann@ksvi.mff.cuni.cz
Faculty of Mathematics and Physics, Charles University
Prague, Czechia

Kristina, Volná
kristina.volna@czech-tv.cz
Czech Television
Prague, Czechia

Korbinian, Moeller
k.moeller@lboro.ac.uk
Centre for Mathematical Cognition
Loughborough University
Loughborough, UK

Cyril Brom
brom@ksvi.mff.cuni.cz
Faculty of Mathematics and Physics, Charles University
Prague, Czechia

ABSTRACT

Children increasingly use computing devices. However, it is unclear whether they have basic knowledge of security-related issues such as computer viruses and, in case they do not, what they can learn about them. It was found previously that Czech 8-year-olds have only limited knowledge of computer viruses, but neither naïve understanding of older children nor what they can learn has been researched. Here, we first examined preconceptions of computer viruses among Czech 5-6-graders (N = 14) and German 3-4-graders (N = 28) by means of a written test. Second, the German sample (experimental group), but not the Czech one (control group), received an intervention to learn about computer viruses, antiviruses, and software updates by means of a 45-min lesson combining a cartoon series on viruses, frontal instruction, and discussion. Both groups again completed the written test. A joint analysis of both samples indicated that Czech and German children already knew key points concerning computer viruses. These included, for instance, that viruses harm our computers (88% of the total sample). However, overall, their knowledge was patchy, and children also had misconceptions such as that viruses can only infect devices connected to the Internet (57%), and antiviruses can delete viruses from the Internet (40%). Due to the intervention, the experimental group improved from pre to posttest (d = 1.06), while this was not the case for the control group. A more in-depth analysis indicated that knowledge gains were mostly related to information repeatedly mentioned during the lesson, but it was less clear whether the lesson helped correct previously held misconceptions. Taken together, the results indicated that knowledge of computer viruses should and can be taught to primary school children, but attention must be paid to existing preconceptions.

Koli Calling '20, November 19–22, 2020, Koli, Finland

ACM ISBN 978-1-4503-8921-1/20/11…$15.00
https://doi.org/10.1145/3428029.3428033

CCS CONCEPTS

• **Social and professional topics → K-12 education**.

KEYWORDS

Primary computing education, Multimedia learning, Primary school children, Computer viruses, Conceptions

ACM Reference Format:
Katerina, Tsarava, Manuel, Ninaus, Tereza Hannemann, Kristina, Volná, Korbinian, Moeller, and Cyril Brom. 2020. Fostering Knowledge of Computer Viruses among Children: The Effects of a Lesson with a Cartoon Series. In *Koli Calling '20: Proceedings of the 20th Koli Calling International Conference on Computing Education Research (Koli Calling '20), November 19–22, 2020, Koli, Finland*. ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3428029.3428033

1 INTRODUCTION AND RELATED WORK

Children's use of computing devices is increasing [18, 25]. Hence, during primary school age (approx. 7 – 11 years), they should gradually understand security-related topics [1, 4], such as computer viruses and protective measures against them. This topic is particularly important because computer viruses can regularly attack smartphones, a common device children use [25]. A virus attack can have serious consequences on the device owner. The large European survey, EU Kids Online 2020, found that around 15% of surveyed children (aged 9 – 16 years) actually have had their devices infected by computer viruses during the last year [25].

Instructional materials concerning the topic of computer viruses, or malware more generally, have started to appear (e.g., [5, 13]). However, from an educational perspective, there are two issues. First, little is known about what children can learn about this topic at different ages. For instance, it is quite possible that 7-year-olds may hardly understand more than the basic idea that 'viruses harm computers'; whereas, 11-year-olds may acquire a detailed, mechanistic understanding of how various types of viruses function and what harm they can do to device owners. Second, it is unknown what preconceptions about this topic children bring to schools. Theories of cognitive constructivism, which are widely used in science education [7, 10–12, 19], indicate that to design proper instructional

environments and to understand the progress of learners, it is necessary to identify learners' preconceptions as the foundation for subsequent knowledge acquisition. Some preconceptions may be correct; others may be partly correct, others incorrect but amenable to change, still others may be incorrect and difficult to change.

Children's understanding of computing-related topics is generally outside the scope of large-scale international studies, such as ICILS [14] or PISA [24]. Also, these studies do not focus on primary school children. Several small-scale studies evaluated children's preconceptions about specific computing concepts, such as databases [2] or Internet ([8]; see [2, 9, 15, 17, 21–23], for other examples; see [16] for a mini-review). As far as we know, only three studies focused on the topic of computer viruses: all assessed preconceptions, and none examined learning about computer viruses. A recent study from 2019 indicated that Czech 8-year-olds had almost no knowledge about computer viruses, antiviruses, and software updates [16]. It is unclear whether the same also applies to older children. Another study [17] examined the understanding of computer viruses among 6-18-year-olds participants and concluded that "the large majority of online users have little understanding of a computer virus" (p. 528). However, the distribution of participants across age groups was unclear, so age differences could not be investigated. Moreover, the study was conducted already back in 2005 hence the patterns of acquiring preconceptions may well have changed since then (e.g., participants were familiar mostly with PCs only, back then). Finally, a study from 2012 in Germany [7] with "higher education learners and 10% of school students" (without specifying the participants' ages) concluded that there was "strong awareness of the risks, but relatively weak understanding of the working principles of viruses" (p. 171) among participants. Again, it is difficult to make precise statements about the understanding of participants from different age groups. It is apparent that research on the understanding of computer viruses and related topics among children is in its very early phases, and many open questions need to be addressed. Accordingly, the current study tried to build upon the existing studies and extend the current state-of-the-art by examining the following research questions:

- What is the level of children's prior understanding of computer viruses and protection against them? (RQ1)
- What incorrect conceptions about these topics do children have? (RQ2)
- How much can children learn from a 45-min long course on viruses with cartoon series? (RQ3)
- What new knowledge can be acquired by children (RQ4)?
- To what extent can previous misconceptions be corrected due to the course? (RQ5)
- Could the course introduce new misconceptions? (RQ6)

It is possible that quite a lot can be taught to children about viruses employing various experiential learning approaches. However, in the present study, we followed a more traditional approach, which is easy to implement in typical schools by typical, rather than exceptional, teachers. Namely, we pondered on what can be taught during a classical school lesson (i.e., 45 min) involving frontal instruction, group discussions, and an animated educational series showed to the students via a projector. This work extends a preliminary analysis [27].

2 METHOD

2.1 Design

This study was conducted jointly in the Czech Republic and Germany in 2 class subgroups and 3 after-school clubs, respectively. Participants in both countries were conveniently selected based on the teachers' willingness to participate in the study and integrate the experimental sessions in their teaching schedule. Students in Germany were assigned to the experimental group and received the 45-min long lesson on the topic of computer viruses that included two cartoon videos from a new animated series for children on how computers work. In contrast, Czech students were assigned to serve as the active control group that was instead offered an unplugged playful introduction to computational thinking concepts. The content of the activities selected for the active control group on purpose had no overlapping relation to the content of the intervention, but still remain relevant to computer science education topic. We followed a quasi-experimental control group pretest-posttest design where students in both groups (experimental and active control group) were tested before and after the intervention. The study was performed between October and December 2019.

2.2 Participants

In this study, 42 students participated in total (28 German and 14 Czech students). The students in Germany were second (n=1), third (n=8) and fourth (n=19) graders (7 girls and 21 boys; 8-10-year-olds) that attended a structured extracurricular program in two school sites, one in the city of Stuttgart and one in a smaller town southwest of Stuttgart. The students of the extracurricular program are recruited after being nominated for participation by their school teachers based on their performance and interest.

Students in the Czech Republic were fifth (n=13) and sixth (n=1) graders (7 girls, 5 boys, and 1 not indicated; 11-12-year-olds). They participated in the study as two separate subgroups, each from a different school: a public school at the suburb of Prague and a small private school in the city of Prague. Consequently, the sample in Germany, as well as Czech, included primarily well-situated middle class background participants. One additional participant was excluded from the study for not feeling well when testing was done.

For both groups, it is difficult to say precisely to what extent they have been exposed to computer science topics before. However, in Baden-Württemberg, Germany, there is officially no CS curriculum for primary school. Similarly, in the Czech Republic, the respective curriculum is generally oriented to digital literacy, but not explicitly to CS.

The groups in both countries were conveniently selected based on the research institutions that designed and ran this study.

In both countries, informed consent by students and their parents was required before the start of the study.

2.3 Materials

2.3.1 Educational Videos. In the experimental group, we used two animated videos: the 7th episode of the animated series Data Newtown on the topic of computer viruses and a supplementary "talk show" on the same topic. The videos have been created by Czech Television, the main public television service in the Czech Republic.

Figure 1: Screenshots from the series (two upper figures) and the talk show (two lower figures). (c) Czech Television.

Both videos are intended for children 7–12 years of age (see Figure 1). The key protagonists are James, who encounters a problem with a computing device in every episode, and Marwin, his older computer-savvy friend who helps him with the problem. The boys have a magical program: using this program, they can enter a world inside the computer (called Data Newtown). Unlike in popular media, this world is a functional model of the RAM content, depicted using a child-intelligible metaphor of a city (e.g., every building represents a running program, a character represents a program thread, etc.). In every episode, James's problem is solved in this computer world by exposing the underlying mechanism that causes the problem.

In the talk show, James invites key protagonists from episodes (i.e., program threads) to a television studio (see Figure 1). Therein, James assumes the role of a newsman and asks the protagonist questions that further elucidate the topic. This way, the viewer is frontally exposed to additional, verbally provided information. The talk show also features some expository graphics.

The series includes 10 episodes, and it was broadcasted in May 2020 (i.e., after we conducted this experiment). The supplementary talk shows are available only online since May 2020. All the videos are available at decko.cz/datovalhota in the Czech language. For the experiment, the videos were dubbed by a German professional actor.

The 7th episode: The episode is 4:40 min long. It starts when James enters school and schoolmates begin laughing at him because they have received a funny and embarrassing video showing James playing with a toy cucumber. At home, James enters Data Newtown and – together with Marwin – finds out that a computer virus has infected his computer because he switched off the antivirus and downloaded a virus-infected computer game from the Internet. The virus is a spyware: It used the webcam and recorded James doing various stuff in front of the computer (including playing with the toy cucumber). Also, the virus found the contact information of James schoolmates and sent all of them (via an intermediate server) James' cucumber video. By downloading the video, the schoolmates could also download the real virus. The story is self-contained (i.e., exposure to previous episodes is not needed).

From an educational standpoint, the episode elucidates the following concepts:

- computer viruses can harm computers and therefore, their users;
- an example of what the virus can do is spying on what one is doing on the computer;
- computer antiviruses can protect computers against viruses and can get rid of them (but they cannot undo the harm done by the viruses);
- it is crucial to keep antiviruses updated.

The talk show: The talk show is 4:50 min long. James' TV guest is the computer virus. During the dialog, information on the following topics is revealed:

- what other examples of computer viruses exist;
- how exactly the virus infected James notebook in the 7th episode (i.e., James switched the antivirus off and downloaded a virus-infected computer game);
- that computer viruses can also infect smartphones;
- that software updates are needed to keep computer programs, including antiviruses, updated.

2.3.2 Knowledge Test. To measure knowledge on computer viruses and protection against them, we devised our own test with 12 closed-form questions. These questions assessed the conceptual understanding of the topic. They were created based on our experience with teaching the topic of computer viruses in primary schools and based on prior research [16].

Czech and German versions of the test were created. The same test was administered as a pretest and posttest.

Each question had five possible answers, and 1-5 of them could be correct. Participants had to mark all correct answers. The test included questions of varying levels of difficulty. The 12 questions are as follows (the correct answers are underlined):

(1) What is a computer virus?
   I. Something our computer needs
   II. Something that helps our computer
   III. Something that harms our computer
   IV. A computer program
   V. Something accelerating a computer processor

(2) On what types of computing devices can a computer virus get into?
   I. Smartphones
   II. Only devices connected to the Internet
   III. Notebooks
   IV. Out of all mobile devices only the oldest ones
   V. Tablets

(3) How can a computer virus get into a computing device?
   I. By downloading it with a file from the Internet (e.g., a movie or a game)
   II. By clicking on a suspicious link from a message or an email
   III. By moving from a flash memory card
   IV. By moving from a power supply cable
   V. By answering a message from a stranger

(4) What can a computer virus do on our computing device?
   I. Delete or encrypt our files (e.g., videos, homework, pictures, etc.)
   II. Watching us through a webcam and record what we do
   III. Locate us
   IV. Fight harmful programs
   V. Find out contacts on our friends and misuse these contacts

(5) Where can a computer virus hide itself on our device?
   I. In a keyboard
   II. On a hard drive
   III. In the RAM
   IV. In another computer program
   V. In an email attachment

(6) What is an antivirus?
   I. A program looking for computer viruses on our computing device
   II. A program helping viruses
   III. A program that is dangerous
   IV. A program deleting viruses in our computing device
   V. A program looking for computer viruses on the Internet

(7) What can be done so that a computer virus NEVER appears on our computing device?
   I. Switch an antivirus on
   II. Switch an antivirus on a keep it updated
   III. Never go on the Internet
   IV. Never download email attachments
   V. Remove a battery from our computing device and never use it

(8) What is a software update?
   I. Deleting all antiviruses from a computing device
   II. Installing the newest versions of computer programs
   III. Finding out viruses on a computing device
   IV. Buying a new computing device in an e-shop
   V. Finding out new videogames or videos on the Internet

(9) Why do we need software updates?
   I. Improve "fighting abilities" of antiviruses
   II. Stop antiviruses
   III. Connect a computing device to the Internet even though no Wi-Fi is around
   IV. Improve the functioning of computer programs
   V. Increasing the storage capacity of a hard drive or a memory card

(10) How can we simplify access to our computing device for a virus?
   I. By switching software updates on
   II. By switching software updates off
   III. By opening all email and message attachments
   IV. By visiting web pages offered by online ads
   V. By telling everyone our phone number

(11) What can help antivirus to do its job better?
   I. A larger hard drive or memory card
   II. A large display
   III. Software updates being switched on
   IV. Better internet access
   V. Stronger passwords for our internet accounts

(12) What can an antivirus do?
   I. Delete viruses from the Internet
   II. Find out who made a computer virus
   III. Undo harm caused by a computer virus
   IV. Find out a forgotten password
   V. Update itself utilizing software updates

2.4 Procedure

Both the experimental and the active control group took part in a 90-minutes session. The structure of the sessions for both groups consisted of a pretest phase of approximately 20 minutes, an intervention phase of 45 minutes, and a posttest phase of approx. 20 minutes.

To make the intervention for the experimental group equal across the two schools (consisting of 3 after-school clubs in total) in Germany, the intervention followed a strictly timed schedule that consisted of:

- a warm-up discussion (2 min.)

- an episode of the animated series (introductory video, for details, see Section 2.3);
- debriefing of the episode (10 min.);
- another episode of the animated series (the talk show video, for details, see Section 2.3); and
- debriefing of the episode (15 min.).

After the posttest, students were also presented with a short bonus video to get a contextual understanding of the protagonists and their role in the animated series.

The warm-up phase started with the question, "Do you know what a computer virus is?" posed by the instructor. Students were motivated to brainstorm and respond freely. The discussion was driven by the instructor towards the core statement that a computer virus is a program that damages the computer.

The debriefing that followed the first video aimed at ensuring children's understanding of the storyline and further explaining what computer viruses, antivirus programs, and software updates are. This phase was structured on the following five questions:

- What did the viruses do to James?
- James was ashamed of the video. What kind of situations would you hate to be recorded in?
- How did James and Marwin solve the problem?
- What was James' mistake?
- What is the software update?

The discussion was driven towards the core statements that James' antivirus was turned off, and this allowed for the virus to activate the computer's camera, record a video, and send it. The instructor explained that cameras could be found on smartphones too, and thus viruses can also attack mobile devices like smartphones and notebooks. The role of an antivirus was emphasized by mentioning its ability to detect viruses, delete viruses, but not fully reverse the damages they may already have caused. Additionally, the role of software updates was mentioned regarding their influence on antiviruses' effectiveness.

The debriefing that followed the second video aimed at further explaining what viruses can cause and elaborate on what exactly the virus did with James' video. This phase was structured on three questions:

- What types of viruses were mentioned in this video?
- What did the spyware do to James?
- Do James' classmates have the virus on their computing devices?

The discussion was driven towards three core elements spyware, ransomware, and mining viruses. The instructor, in simple words, summarized what kind of information is attacked by these types of viruses, what is the mechanism of attack, and how one can protect one's device against them. Additionally, the instructor explained in detail how the virus presented in the episode could have affected the devices of the children that received the video of James. At that point, Trojan viruses were mentioned, and adult consultation was recommended in the case of suspicious malware on students' devices. The instructor of the intervention for all three after-school clubs of the experimental group was the same research assistant.

The active control group received an unplugged playful introduction to computational thinking concepts (like sequences, loops, simple conditionals, and others). Together with an instructor, students played the Treasure Hunt game of the board game series "Crabs and Turtles: A series of Computational adventures" [26]. This intervention was in no way related to the concept of computer viruses, antiviruses, and software updates. After the posttest phase, students were also shown the episode of the animated series as a bonus contextualizing the viruses knowledge test. The instructor of the activities for both school subgroups of the active control group was the same researcher.

Table 1: Descriptive statistics per group. The scale for correct answers is 0 - 27 (the larger the number, the better score). The scale for misconceptions is 0 - 33 (the larger the number, the worse the score).

Variable / Group	Czech		German		Cohen's
	M	SD	M	SD	*d*
Pre Correct	10.79	4.10	10.57	4.21	-0.05
Pre Misconceptions	5.36	1.08	5.82	2.80	0.22
Post Correct	11.79	3.89	15.43	5.16	0.80
Post Misconceptions	6.00	1.80	6.21	2.69	0.09
Post - Pre Correct	1.00	2.32	4.86	4.62	1.06
Post - Pre Misconceptions	0.64	1.50	0.39	2.77	-0.11

2.5 Data Analysis

As regards summative analysis, we analyzed separately correct answers and misconceptions in the knowledge test. With regards to correct answers, a point was given when the participant correctly checked a correct answer. In this way, participants could be awarded up to 27 points. Concerning misconceptions, a misconception point was given when participants incorrectly checked an answer that should not be checked. That is, with regards to the data analysis, we view misconception as a checked answer-option that is incorrect. Participants could be given up to 33 misconception points. Between-group comparison was conducted using t-tests in *jamovi* 1.0.7.0 (https://jamovi.org).

Aside from this summative analysis, we examined individual answers qualitatively for more detailed insight into participants' prior knowledge (both Czech and German groups) and what they learned and did not.

3 RESULTS

3.1 RQ1: Level of Understanding

Analyzing the frequency of correct responses in the knowledge pretest for the entire sample (control and experimental group; N = 42), we observed a rather moderate initial knowledge on the topic of computer viruses, antivirus protection, and software update (approx. ~40% of the maximum possible score for correct answers, yet only ~17% misconception points). Pre-intervention differences between Czech and German groups were negligible (see Table 1).

3.1.1 Understanding of Viruses. To the general questions about viruses, and particularly to question *Q1.*[1] *What is a computer virus?,*

[1]The question numbers refer to numbers used in the test, see Section 2.3.2 and https://osf.io/3wrdx/?view_only=4b6d52023f71416692751ba5c4004a65.

~88% of the students responded "something that harms our computers". To question *Q4. What can a computer virus do on our computing device?*, ~84% of the students responded, "delete or encrypt our files". To question *Q5. Where can a computer virus hide itself on our device?*, ~42% have given one or more of the following correct answers: "To a hard drive", "In the RAM", "In another computer program", "In an email attachment". The percentage of correct responses to these four questions indicates a good understanding of the adverse effects that viruses can have on our computers.

However, we also observed some initial misconceptions related to computer viruses. For example, to question *Q3. How can a computer virus get into a computing device?*, ~14% of the students replied: "by answering a message from a stranger". Similarly, to question *Q4. What can a computer virus do on our computing device?*, three students (~7%) replied, "fight harmful programs".

More specifically, measuring the average rate of correct responses for each question related to the virus, we found that to question *Q1. What is a computer virus?*, only ~10% of students gave the response "a computer program". To question *Q2. What types of computer devices can a computer virus get into?*, the correct responses smartphones (~43%), notebooks (~50%), and tablets (~40%) were given by almost half of the students. Similarly, to question *Q3. How can a computer virus get into a computing device?*, half of the students responded correctly (i.e., "By downloading it with a file from the internet, e.g., a movie or a game." [~55%]; "By clicking on a suspicious link from a message or an email." [~45%]). On the contrary, to the same question, only ~19% of the students correctly gave the response, "By moving from a flash memory card". To question *Q4. What a computer virus can do on our computing device?*, an average of ~43% of participants responded correctly, "Find out contacts on our friends and misuse these contacts.". However, only ~26% answered correctly, "Watching us through a webcam and record what we do.", and even less ~21% gave the response "Locate us".

3.1.2 Understanding of Antivirus Protection. To the broad question about antivirus protection, and particularly *Q6. What is an antivirus?*, ~29% of students responded that is "a program looking for computer viruses on our computing device". In comparison, ~57% responded that it is a "program deleting viruses in our computing device". The correct response rates to this question indicate a rather moderate understanding of the broader concept of an antivirus, but with specific misconceptions. For example, to the question Q6, there were some quite conflicting responses. For instance, 6 (~14%) students responded that it is "program helping viruses", 5 (~10%) students responded that it is "a program that is dangerous", and 4 (~9%) students replied that it is "a program looking for computer viruses on the Internet". Additionally, we noticed a number of misconceptions as regards to how antivirus software works. These are further detailed in Section 3.2.

3.1.3 The Understanding of Software Updates. To the general question *Q8. What is a software update?*, ~64% of students at pretest responded correctly that it is "installing the newest versions of computer programs". To question *Q9. Why do we need software updates?*, ~31% of the students replied, "improve "fighting abilities" of antiviruses", and 52% responded correctly "improve the functioning of computer programs". Furthermore, to question *Q11. What can help antivirus do its job better?*, ~43% of the students answered "software updates being switched on". Similarly, to question *Q10. How can we simplify access to our computing device for a virus?*, ~29% of the students replied "by switching software updates off", ~33% "by opening all email and message attachments", and ~24% "by visiting web pages offered by online ads". Correct response rates to these questions indicate a rather good general understanding of the concept of software updates, but with limitations as concerns detailed understanding.

Some misconceptions were observed, as well. For example, to question *Q8. What is a software update?*, 4 (~10%) students responded that a software update "is deleting all antiviruses from a computing device", 5 (~12%) students reported that it is "finding out viruses on a computing device", 3 (~7%) students answered that it is "buying a new computing device in an e-shop", and 4 (~10%) students responded that it is "finding out new videogames or videos on the internet". To *Q9. Why do we need software updates?*, 4 (~10%) students responded that software updates can "increase the storage capacity of a hard drive or a memory card".

In general, the level of children's prior understanding of viruses seems to differ considerably across students.

3.2 RQ2: Pre-existing Misconceptions

Altogether, children did not have many misconceptions (~5.7 out of 33; both groups combined). However, some misconceptions were recurring.

To question *Q2. On what types of computing devices can a computer virus get into?*, ~57% of students replied, "only devices connected to the internet". This rather large number of incorrect responses indicates a misconception on the functionality of viruses, which is only perceived as an internet-related possible threat.

To question *Q10. How can we simplify access to our computing device for a virus?*, ~29% of the students replied "by switching software updates on", and ~19% responded, "by telling everyone our phone number". As already discussed for Q2, both frequencies of false responses to this question indicate a misunderstanding of how viruses can gain access to computer devices.

To question *Q11. What can help antivirus to do its job better?*, ~21% of the students replied, "a larger hard drive or memory card", ~19% responded "better Internet access", and ~33% replied "stronger passwords for our internet accounts". To *Q12. What can an antivirus do?*, ~40% of students falsely replied, "delete viruses from the Internet ", and ~52% responded "undo harm caused by a computer virus". The frequency of incorrect answers to these questions indicates a misunderstanding of how antivirus protection works.

3.3 RQ3: Net Effects of the Intervention

How much can children learn from the 45-min long lesson? To investigate possible training effects due to the intervention, we ran independent samples t-tests (experimental vs. active control group) for pre-post gain in correct responses as well as pre-post difference in the number of misconceptions (i.e., the last two rows in Table 1).

In total, the improvement in performance from pre- to posttest was significantly larger for the experimental group as compared to the active control group [$t(40) = 2.93$, $p = .006$, $d = 1.06$]. However, there was no significant effect as regards a reduction of the number of misconceptions [$t(40) = -0.315$, $p = .755$, $d = -0.11$].

3.4 RQ4: New Knowledge

Children in the experimental group ($n = 28$) gained points for correct answers, mostly thanks to one of the following questions. Regarding question *Q1. What is a computer virus?*, they learned that "a virus is a computer program" (as indicated by an increase of correct answers from pretest to posttest from 1 to 10). Children knew this most likely from the teacher, as she directed their attention to the core statement that a computer virus is a program that damages the computer.

With respect to question *Q2. What types of computer devices can a computer virus get into?*, they learnt that a computer virus can get into smartphones (pre: 15, post: 24), notebooks (pre: 19, post: 24), and tablets (pre: 15, post: 26). We assume that this change may be due to the explicit reference to mobile devices during the cartoon episodes.

Regarding question *Q3. How can a computer virus get into a computing device?*, some children learned that a computer virus may get into a computing device by "downloading it with a file from the Internet" (pre: 12, post: 23) or by "clicking on a suspicious link from a message or an email" (pre: 11, post: 18). Interestingly, these were the central topics in the episode and the talk show, so one might expect that even more children would have learned these facts (the theoretical maximum equals to 28).

In fact, however, pre-post improvement was more pronounced for another central topic covered by *Q4. What can a computer virus do on our computing device?*. The majority of children improved on the question of whether viruses can watch us through a webcam and record what we do (pre: 5, post: 23).

A smaller improvement was noticed as concerns another part of Q4 and the videos' key topic: whether computer viruses can find out contacts on our friends and misuse these contacts (pre: 10, post: 18). It is unclear whether differences in magnitudes of these four improvements are caused by possible differences in these topics' complexity, the subtle differences in how they were incorporated in videos, or in initial knowledge of children. Also, we cannot exclude the possibility that these differences are spurious.

Some children also improved at question *Q6. What is an antivirus?*. Modest improvements were detected for answers "a program looking for computer viruses on our computing device" (pre: 6, post: 15) as well as "A program deleting viruses in our computing device" (pre: 15, post: 22). Antivirus threads looking for and deleting virus inside the computer was directly depicted in the episode; plus, this was also mentioned by the teacher. Finally, children learned from the episode that "software updates improve 'fighting abilities' of antiviruses" (pre: 8, post: 21).

3.5 RQ5: Reconstruction of Misconceptions

To what extent can previous misconceptions be corrected? Based on the students' responses at posttest among the experimental group, we observed four partially corrected conceptions after the intervention took place.

We noted that students from the pre- to posttest corrected their conception at question *Q2. On what types of computing devices can a computer virus get into?* by selecting multiple mobile devices as their response at posttest (see Section 3.4) and not "only devices connected to the Internet" (pre: 13, post: 6).

Additionally, regarding question *Q5. Where can a computer virus hide itself on our device?*, 3 out of the 4 students corrected their response from pre- to posttest by not including the "keyboard" in their answer. It is not clear to us how this conception was corrected as this was not covered explicitly in either the cartoon episodes or the discussions.

Furthermore, with respect to question *Q11. What can help antivirus to do its job better?*, 3 out of the 4 students corrected their response from pre- to posttest by not selecting "better internet access" to their response. One assumption for this correction of conception may be the explicit reference to software updates both in the cartoon episodes and the debriefing during the lecture.

Finally, regarding question *Q12. What can an antivirus do?*, 3 out of the 13 students corrected their response "undo harm caused by a computer virus" from pre- to posttest. We assume that the correction of this misconception is due to the reference during the debriefing that an antivirus can stop the virus from spreading the video, but cannot delete from all the recipient devices.

3.6 RQ6: Introduction of Misconceptions

Could the lecture introduce new misconceptions?: Observing the different patterns of responding to the same questions in pre- and posttest, we detected several unexpected results.

Regarding question *Q5. Where can a computer virus hide itself on our device?*, 12 students at pretest responded correctly that "a virus could hide in the RAM". However, at posttest, only 4 responded in the same way. It seems that after the intervention, most of them did not consider the RAM a possible place for a virus to hide.

Furthermore, to question *Q9. Why do we need software updates?*, fewer students responded correctly that "software updates improve the functioning of computer programs" at posttest as compared to pretest (pre: 15, post: 11). This contrasts with the robust gain on "software updates improve 'fighting abilities' of antiviruses" mentioned in Section 3.3.

Finally, regarding question *Q3. How can a computer virus get into a computing device?*, fewer students answered correctly at posttest that it can be moved from a flash memory card (pre: 6, post: 2). This, again, contrast with otherwise moderate improvements for other answers on Q3 (i.e., "downloading it with a file from the internet" and "clicking on a suspicious link from a message or an email"; Section 3.3).

One possible explanation of these puzzling findings is that students improved when information was directly stressed in the videos and somewhat worsened when they knew something beforehand, but this was not mentioned during the lesson. That is, we may speculate that some children reasoned that their preconception was incorrect when it was not explicitly confirmed by the videos. However, as it currently stands, this is just a working hypothesis. We would be cautious in generalizing this interpretation as our sample is rather small. However, we should consider looking in-depth into these concepts in future studies to gain a better understanding of children's perception.

4 DISCUSSION

The current study pursued two major goals. First, we examined the level of understanding of the topics of computer viruses, antiviruses,

and software updates among two convenience samples, i.e., 11-12-year-old Czechs and 8-10-year-old Germans, previously unexposed to these topics in schools. Second, in a quasi-experimental control group pretest-posttest design, we investigated whether children can acquire new knowledge about these topics during a 45-min long instructional program that combined an educational cartoon series, frontal teaching, and discussion. In the following text, we will discuss the results for these two aspects in turn.

4.1 Prior Knowledge and Misconceptions

Current results indicated that prior knowledge on computer viruses, antiviruses, and software updates was only moderate and differed considerably across children. However, compared to a younger sample of Czech 8-year-olds, who were assessed in a previous study [16], prior knowledge can be considered higher. Overall, children in the present study knew that viruses harm computers. General knowledge of antiviruses and software updates, however, was only moderate. This difference mirrors a similar difference found in the study by [16] because Czech 8-year-olds knew a bit about the existence of computer viruses, but almost nothing about antiviruses and software updates. Therefore, more direct instruction on measures against computer viruses seems necessary.

Even though we found evidence for moderate-to-high *prior knowledge* as regards general information on what computer viruses, antiviruses, and software updates are, we also identified substantial knowledge gaps as concerns specifics, such as the functioning of viruses. For example, when asked about what type of devices can be infected by viruses, most children mentioned at least one type but failed to mention another (out of notebooks, tablets, and smartphones). Half of them did not know that viruses can be downloaded with a file from the Internet. Only one-fourth of students knew, for example, that viruses can spy on us through a webcam; that antiviruses search for viruses inside our computing devices; and that visiting webpages suggested by online add-ons increases a risk of a virus attack.

In the current study we have also identified that children had pre-existing misconceptions. Most notably, half of them thought that only internet-connected devices can be infected by computer viruses; and antiviruses can undo harm done by viruses. Around one third of students reasoned that antiviruses can delete viruses from the Internet and a similar number thought that stronger passwords for our internet accounts can help antiviruses to do their jobs better. Certain incorrect answers were rare; such as that antiviruses help viruses and software updates find out new videogames on the Internet or increase the storage capacity of a device. It is unclear whether children really hold these rare, bizarre misconceptions, or their answers reflect random guessing. ' We have not observed differences in overall prior knowledge between Czech and German children. Descriptively, we have observed some differences in frequencies of correct responses for particular questions, but these differences can be spurious as our samples were relatively small.

Overall, we can conclude that the present study, considered together with the previous study [16] indicated that at the beginning of primary school level – about age 7-9 – children are not only able, in principle, to acquire some preconceptions about computer viruses and protection against them, but they indeed start acquiring them. However, they most likely do so outside schools – from parents, friends, and media exposure – and knowledge gained in this way is insufficient. Most prior knowledge was related to the general danger of computer viruses but to a lesser extent regarding preventive or active measures against them.

4.2 Acquisition of New Knowledge

The current study utilized a quasi-experimental control group pretest-posttest design to examine whether new knowledge about computer viruses, antiviruses, and software updates can be acquired by young children efficiently in schools. In particular, we used a 45-min long instructional program that combined an educational cartoon series, frontal teaching, and discussion to foster knowledge on the respective topics. It turned out that this short educational intervention, which should be easy to implement in schools, helped children to acquire additional knowledge on top of their preconceptions. Importantly, in the current study, Czech children served as a naïve active control group to the German sample, which received the educational intervention. Results indicated that new knowledge was gained among German children when respective information was focused on in one of the videos and/or stressed by the teacher. In other words, children learned when information was *directly* presented to them. Children not only learned new bits of information but also – to a limited extent – reconstructed some of their previously held misconceptions.

It is clear from the current data that, by far, children did not learn all new content that was presented to them. This unsurprising fact reiterates the importance of attention and motivation of children when teaching. Consequently, educational cartoon series or even games or experiential learning methods might be particularly helpful for engaging learners [3, 20]. Interestingly, we also noticed that some children appeared to "unlearn" correct information that children held at the beginning of the educational intervention but was not stressed during the lesson. Given our relatively small sample, this observation should be treated cautiously, and future research should examine whether it has a real substance or can be attributed to the noise in data.

4.3 Limitations

As far as we know, not many studies exist that investigate knowledge around the topic of computer viruses in young children. However, as children start to interact with digital applications quite young [25], acquiring knowledge on computer viruses and appropriate measures against them is crucial. While the current study provided new insights into this issue, it also comes with some limitations. The most obvious one is the rather small, convenience samples, with children probably above average regarding general skills and socio-economic background. This limitation is not uncommon in primary computing education research, but it makes generalization difficult. We think that our results speak of children of reasonably well-situated families. The results can be viewed as a demonstration that these children can acquire partly correct bits of knowledge on computer viruses and protection against them outside schools and improve this knowledge in schools in specific ages (8-10y). In the context of a Vygotskian perspective [6], we have shown that the respective topics are in these children's "zone

of proximal development". However, how detailed, or complex, knowledge about these topics children may acquire and how this complexity differs for different ages (e.g., 8y vs. 11y) remains to be clarified in the future.

Moreover, we need to note that the Czech sample was approx. two years older than the German sample. It is difficult to interpret why there was no difference in overall prior knowledge between these two samples: this might be because children of the German sample, may on average, be more gifted than the Czech sample children (because they were nominated by their teachers to participate because of their interest in the topic) or more exposed to the respective topics before the intervention. Future cross-cultural studies would be desirable to elucidate this issue.

5 CONCLUSION

Taken together, the present results indicate that, as of 2019, primary school children from Germany and the Czech Republic not necessarily acquire sufficient understanding of computer viruses and protection against them spontaneously without explicit or direct instruction. That is, information gained outside of schools, from parents, friends, and media exposure is not sufficient. At the same time, these children need this knowledge, as they are frequent users of computer devices, and they are thus vulnerable to computer virus attacks [25].

The present results also suggested that well-situated middle class German children 8-10 years of age can improve this knowledge thanks to a 45-min lesson that combines educational videos, frontal instruction, and discussions. Even though the samples of this study are not representative of the respective populations, the results advance the field by showing that primary school children can, and should, be taught about the topic of computer viruses, antiviruses, and software updates in schools at the primary level, not later than in Grades 3–4 (age 8 and above).

ACKNOWLEDGMENTS

CB and TH have been partly funded by the Charles University project, PRIMUS/HUM/03. Data Newtown project has been developed and funded by Czech Television (www.ceskatelevize.cz), CZ.NIC (www.nic.cz) and Charles University (mff.cuni.cz). We thank CZ schools that helped to conduct the experiment: primary school Vela (Hloubětín) and primary school of Dr. Edvard Beneš (Čakovice). Additionally, we would like to thank our research assistant Carla Schroepel, and the instructors Dominik Krauß and Hartmut Thamm for their valuable involvement in the study.

REFERENCES

[1] Computing at School Working Group (CAS). 2012. Computer Science: A curriculum for schools.
[2] Torsten Brinda and Thorsten Terjung. 2017. A Database is Like a Dresser With Lots of Sorted Drawers: Secondary School Learners' Conceptions of Relational Databases. In *Proceedings of the 12th Workshop on Primary and Secondary Computing Education*. 39–48.
[3] Cyril Brom, Vít Šisler, Michaela Slussareff, Tereza Selmbacherová, and Zdeněk Hlávka. 2016. You like it, you learn it: affectivity and learning in competitive social role play gaming. *International Journal of Computer-Supported Collaborative Learning* 11, 3 (2016), 313–348.
[4] Code.org. 2013. *Code.org*. http://code.org
[5] CZ.NIC. 2014. Computer security. Retrieved October 21, 2020 from https://www.jaknainternet.cz/page/1179/bezpecnost-pocitace/
[6] Pablo Del Rio and Amelia Alvarez. 2007. Inside and outside the zone of proximal development: An ecofunctional reading of Vygotsky. (2007).
[7] Ira Diethelm, Peter Hubwieser, and Robert Klaus. 2012. Students, teachers and phenomena: educational reconstruction for computer science education. In *Proceedings of the 12th Koli Calling International Conference on Computing Education Research*. 164–173.
[8] Ira Diethelm, Henning Wilken, and Stefan Zumbrägel. 2012. An investigation of secondary school students' conceptions on how the internet works. In *Proceedings of the 12th Koli Calling International Conference on Computing Education Research*. 67–73.
[9] Jérôme Dinet and Muneo Kitajima. 2011. " Draw me the Web" impact of mental model of the web on information search performance of young users. In *Proceedings of the 23rd Conference on l'Interaction Homme-Machine*. 1–7.
[10] Andrea A. diSessa. 2014. *A History of Conceptual Change Research* (2 ed.). Cambridge University Press, 88–108. https://doi.org/10.1017/CBO9781139519526.007
[11] Janice A Dole and Gale M Sinatra. 1998. Reconceptalizing change in the cognitive construction of knowledge. *Educational psychologist* 33, 2-3 (1998), 109–128.
[12] R Duit, H Gropengießer, U Kattmann, M Komorek, and I Parchmann. 2012. Science education research and practice in Europe. *Sense Publishers) The Model of Educational Reconstruction Framework for Improving Teaching and Learning Science* 1 (2012), 13–37.
[13] Internet-ABC e.V. 2001. *Internet-ABC*. https://www.internet-abc.de
[14] Julian Fraillon, John Ainley, Wolfram Schulz, Tim Friedman, and Eveline Gebhardt. 2014. *Preparing for life in a digital age: The IEA International Computer and Information Literacy Study international report*. Springer Nature.
[15] Shuchi Grover, Daisy Rutstein, and Eric Snow. 2016. " What Is A Computer" What do Secondary School Students Think?. In *Proceedings of the 47th acm technical symposium on computing science education*. 564–569.
[16] Tereza Hannemann, Tereza Stárková, Pavel Ježek, Kristina Volná, Kateřina Kačerovská, and Cyril Brom. 2019. Eight-Year-Olds' Conceptions of Computer Viruses: A Quantitative Study. In *Proceedings of the 14th Workshop in Primary and Secondary Computing Education*. 1–7.
[17] Yasmin B Kafai. 2008. Understanding virtual epidemics: children's folk conceptions of a computer virus. *Journal of Science Education and Technology* 17, 6 (2008), 523–529.
[18] Daniel Kardefelt-Winther. 2017. *How Does the Time Children Spend Using Digital Technology Impact Their Mental Well-being, Social Relationships and Physical Activity?: An Evidence-Focused Literature Review*. UNICEF Office of Research-Innocenti Florence, Italy.
[19] Richard E Mayer. 2002. Multimedia learning. In *Psychology of learning and motivation*. Vol. 41. Elsevier, 85–139.
[20] Manuel Ninaus, Simon Greipl, Kristian Kiili, Antero Lindstedt, Stefan Huber, Elise Klein, Hans-Otto Karnath, and Korbinian Moeller. 2019. Increased emotional engagement in game-based learning–A machine learning approach on facial emotion detection data. *Computers & Education* 142 (2019), 103641.
[21] Marina Papastergiou. 2005. Students' mental models of the Internet and their didactical exploitation in informatics education. *Education and Information Technologies* 10, 4 (2005), 341–360.
[22] Judy Robertson, Andrew Manches, and Helen Pain. 2017. "It's Like a Giant Brain With a Keyboard": Children's Understandings About How Computers Work. *Childhood Education* 93, 4 (2017), 338–345.
[23] Michael T Rücker and Niels Pinkwart. 2016. Review and discussion of children's conceptions of computers. *Journal of Science Education and Technology* 25, 2 (2016), 274–283.
[24] Andreas Schleicher. 2019. PISA 2018: Insights and Interpretations. *OECD Publishing* (2019).
[25] David Smahel, Hana MacHackova, Giovanna Mascheroni, Lenka Dedkova, Elisabeth Staksrud, Kjartan Olafsson, Sonia Livingstone, and Uwe Hasebrink. 2020. EU Kids Online 2020: Survey results from 19 countries.
[26] Katerina Tsarava, Korbinian Moeller, and Manuel Ninaus. 2018. Training computational thinking through board games: The case of Crabs & Turtles. *International Journal of Serious Games* 5, 2 (2018), 25–44.
[27] Katerina Tsarava, Manuel Ninaus, Tereza Hannemann, Kristina Volná, Korbinian Moeller, and Cyril Brom. 2020. Teaching primary school children about computer viruses: preliminary results of an intervention study. In *Proceedings of the 15th Workshop on Primary and Secondary Computing Education*. 1–2.