Journal of Information Technology Education: Innovations in Practice

An Official Publication of the Informing Science Institute
InformingScience.org

JITEiip.org

Volume 16, 2017

THE INFLUENCE OF TEACHING METHODS ON LEARNERS' PERCEPTION OF E-SAFETY

Václav Šimandl*	Faculty of Education, University of South Bohemia in České Budějovice, Czech Republic	simandl@pf.jcu.cz
Václav Dobiáš	Faculty of Education, University of South Bohemia in České Budějovice, Czech Republic	dobias@pf.jcu.cz
Michal Šerý	Faculty of Education, University of South Bohemia in České Budějovice, Czech Republic	kyklop@pf.jcu.cz

* Corresponding author

ABSTRACT

Aim/Purpose	The traditional method of teaching e-safety by lecturing is not very effective. Despite learners often being equipped with the right knowledge, they reject the need to act accordingly. There is a need to improve the way digital e-safety is taught.
Background	The study compares four different teaching styles, examining how each affected the way students perceive a range of e-safety keywords and consequently the way they approach this issue.
Methodology	The semantic differential technique was used to carry out the research. Students completed a semantic differential questionnaire before and after lessons. A total of 405 first year undergraduates took part in the study.
Contribution	The paper contributes to the debate on appropriate methods for teaching e-safety, with an aim to influence learners' attitudes.
Findings	Experience-based learning seems to be very effective, confronting students with an e-safety situation and providing them with a negative experience. This teaching method had the biggest influence on students who were deceived by the prepared e-safety risk situation.
Recommendations for Practitioners	E-safety instruction can be enhanced by ensuring that lessons provide students with a personal experience.
Recommendation for Researchers	The semantic differential technique can be used to measure changes in learners' attitudes during the teaching process.

Accepted by Editor Jo Coldwell-Neilson | Received: July 23, 2017 | Revised: October 15, 2017 | Accepted: October 16, 2017.

Cite as: Šimandl, V., Dobiáš, V., & Šerý, M. (2017). The influence of teaching methods on learners' perception of e-safety. *Journal of Information Technology Education: Innovations in Practice, 16,* 253-275. Retrieved from http://www.informingscience.org/Publications/3877

Impact on Society	Our findings may bring improvements to the way e-safety topics are taught, which could, in turn, evoke in learners a more positive e-safety attitude and a desire to improve their e-safety behavior.
Future Research	More research needs to be carried out to examine how the experiential learning method affects the attitudes of younger learners (primary, middle, and high school students).
Keywords	e-safety, teaching methods, experience-based learning, lecture, expert's talk, group learning, semantic differential

INTRODUCTION

E-safety concerns the protection of a user as well as information and communication technologies (ICT) he uses from the negative consequences of using ICT (Barrow & Heywood-Everett, 2006). This article focuses on a narrower area of e-safety called digital e-safety, which particularly relates to a user's interaction with digital technologies. Other possible users and relationships with them are perceived to be less significant than the technical side of the matter. Digital e-safety covers the issues of malware, computer breakdowns, passwords and identity theft, the negative consequences of email communication (spam, hoax, phishing), legislation (copyright, licenses, protection of personal data), and sharing personal data.

BACKGROUND

Students' e-safety knowledge and routines has been the subject of many research studies. A number of students do not use a complex password or change it on a regular basis (Symantec Corporation, 2010). They reuse the same password for multiple accounts (Lang et al., 2009) and perhaps even share their password with others (Organisation for Economic Co-operation and Development, 2011). Despite a large number of students expressing their fear of being vulnerable to malware (Eynon, 2009), some students have had malware downloaded into their computer or been victims of spyware (Child Exploitation and Online Protection, 2008; Symantec Corporation, 2010). Lower secondary students lack the critical evaluation skills to either be able to interpret incoming information or make appropriate judgements about how to behave online (Byron, 2008). Children and young people also need the help and support of the school to recognize and avoid e-safety risks and build their resilience (South West Grid for Learning, 2009).

One way to help students avoid the dangers related to using computers is by improving e-safety awareness and providing appropriate training (Aytes & Connolly, 2004). Considering the rather low level of knowledge and routines of some adult users, parents themselves cannot be relied on to educate their children about e-safety (Byron, 2008). According to the British Educational Communications and Technology Agency [Becta] (2006), education and training play an essential role in providing the basic support learners need to avoid e-safety risks. Many authors have claimed that school is the ideal place to teach children digital e-safety skills (Becta, 2005, 2007; Byron, 2008; Livingstone & Haddon, 2009; Papavasiliou, 2009; Vanderhoven, Schellens, Vanderlinde, & Valcke, 2016).

Despite such findings, there is very little literature providing support for teachers with e-safety methodology whose effectiveness has been evaluated (Livingstone & Bulger, 2013). However, there are some exceptions, such as a card game to support lessons on privacy (Barnard-Wills & Ashenden, 2015), a role play called Net Detectives, where children learn about e-safety through play (Wishart & Morris, 2007), or a set of activities intended for future IT professionals to support lessons on technical aspects of privacy (Peltsverger & Zheng, 2016).

Pupil learning can be looked at through various pedagogical theories. According to Piaget (1936/1965), pupils construct their own knowledge by acting on events in their environment. Such experiences may lead to assimilation, where a pupil incorporates a new event into preexisting cogni-

tive structures. If the new event is so different that the pupil is unable to incorporate it into the preexisting structure, accommodation will occur, where existing cognitive schemas will be modified or a completely new schema will be created (Piaget, 1936/1965).

Most Czech school children are familiar with traditional teacher-centred instruction (Maňák & Švec, 2003). This is based on pupils receiving new information in the form of a lecture delivered by the teacher from the front of the classroom. This form of teaching has been used for centuries and a methodological basis for it can be found in Herbart's work (1806).

The oral transfer of information is criticized by Kolb (1984), who insisted that learning is the process whereby knowledge is created through the transformation of experience. Dewey (1997) adopted a similar approach, claiming that education must be based upon experience – which is always the actual life-experience of some individual.

Pupils can acquire new information through the transformation of an experience gained either via observational learning (Bandura, 1977) or by listening to somebody else talking about their experience (Šimandl & Vaníček, in press). Social cognition is likely to play a significant role (Hayes, 1993), in this case the pupil's personal rating of the person trying to present his experience may be important.

In an age of digital media, information can be provided by anyone with inspiration from anywhere in the world. Connectivism sees learning as a process of connecting specialized nodes or information sources (Siemens, 2005). Learning can reside outside of ourselves and is focused on connecting specialized information sets (Siemens, 2005). Information can either come from technologies or people. According to Siemens (2005), learning and knowledge rests in diversity of opinions. Alongside connectivism, this principle is widely used in many discussion and group activities (Činčera & Caha, 2005; Royal, 2015).

MOTIVATION AND AIM OF THE RESEARCH

A number of learners become victims of cybercrime despite e-safety being taught in schools. This may be due to the fact that learners are often equipped with the right knowledge but they reject the need to act accordingly (Beránek, 2009; Šimandl, 2015). Therefore, the traditional method of teaching e-safety by lecturing seems to be rather ineffective. Improvement may be achieved by proposing and implementing appropriate strategies to deal with specific teaching methods aiming to influence learners' attitudes. Despite the unanimous opinion on the importance of e-safety education, there is still a lack of both resources and evaluations of the effectiveness of e-safety lessons. In order to contribute to the discussion on appropriate forms of e-safety lessons, we have decided to propose and test our own models for teaching this area. Hopefully, our findings will bring improvements to the way e-safety topics are taught, which could, in turn, evoke in learners a more positive e-safety attitude and a desire to improve their e-safety behavior.

The research problem was determined as: "How do various teaching methods used in digital e-safety lessons influence students' perception of this issue?" As implied by the research problem, the study does not focus on discovering how pupils' knowledge is influenced but addresses how pupils' attitudes are influenced. Having determined the research problem, the research aim was set. The aim of the research is to propose several models for teaching digital e-safety and to evaluate them in terms of their influence on learners' perception of e-safety.

Four models for teaching digital e-safety were proposed. The first approach, **Experience-based learning**, confronted students with a digital e-safety situation, providing them with a negative experience. The second approach, the **Expert's talk**, consisted of experts being invited to talk about the risks associated with digital e-safety using real life stories. The third approach, the **Lecture**, comprised the general idea of this teaching method, where the teacher delivered lesson content and students listened. The last approach, **Group learning**, was based on students' own active learning. Dur-

ing lessons, students worked in groups to create a presentation on a certain topic and to familiarize the other students with their work. These teaching methods are described in more detail below.

METHODOLOGY

ORGANIZATION OF THE RESEARCH

The research constituted a pair of semantic differential tests and the delivery of e-safety lessons. The first test – pre-test – was taken by students 1–2 weeks before the lessons. The second test – post-test – was taken by students 2 weeks after the lessons. Research was carried out at a certain college in South Bohemia. Sample size was determined by the number of students per year group at the college where the author was employed. The research questioned all of the college's full-time first year students who attended mandatory ICT lessons. This sample size was selected so that students could be divided into smaller groups whilst preserving sufficient group sizes for the chosen analytical methods.

Students were educated about digital e-safety within their subject study group. A total of 32 study groups participated in the research. In order to eliminate discrepancies due to different teachers, lessons were taught by the same teacher – apart from the Expert's talk. The topic was allocated a 90 minute lesson. Although a different teaching method was used for each study group, the same e-safety content was delivered in each study group. In order to gain an independent view of the lessons and ensure certain triangulation of the research, an impartial teacher was invited to monitor one teaching unit of each teaching method.

As claimed by Ferjenčík (2000), in order to ensure internal research validity, there should be a balance between the experimental groups and the control group. According to the Student Office at the college, students are randomly selected for seminar groups, so this requirement was implicitly met for our research.

For data analysis, members of experimental groups are considered to be those students who completed both the pre-test and post-test and attended lessons on the topic. Members of the control group are considered to be all students who either completed the pre-test or completed the post-test but did not attend lessons on the topic. This includes both students in the control seminar groups and students who were placed in a particular experimental seminar group but completed only part of the research (typically those who did not attend lessons). The number of participants per group for each type of lesson is given in Table 1.

Table 1: Number of participants per lesson type

Type of lesson	No. of participants pre-test	No. of participants post-test
Experience-based learning	58	58
Expert's talk	34	34
Lecture	21	21
Group learning	30	30
Control sample	262	142
Total	405	285

Alongside the above given disjunctive groups of participants, another extra group was formed. This group consisted of participants who had been involved in Experience-based learning and had been deceived into registering on a new website by the prepared e-safety risk scenario (see below). The

group consisted of 15 participants. This group was formed in order to gain a better understanding of how lessons had influenced those participants who had been deceived by the prepared e-safety threat (and are likely to be less cautious than those students who had attended the same type of lesson but had not succumbed to the threat).

Description of Teaching Methods

As implied by our previous research (Šimandl, 2015), a negative experience can significantly influence a person's perception of e-safety. This may develop directly from an authentic experience or be conveyed by telling stories of people affected by e-safety incidents which students can relate to. While an authentic experience was used by us for Experience-based learning, the Expert's talk was based on conveying e-safety incidents. Other lessons were delivered in the form of classic lecture and group learning.

Despite the different types of teaching techniques, each lesson had the same goal, the same teacher (apart from the Expert's talk) and the same content was taught every time. Lesson content was focused on individual areas of digital e-safety as covered by the European Computer Driving Licence concept (European Computer Driving Licence Foundation Ltd. 2007a, 2007b). Besides general risks associated with using ICT, specific risks concerning the use of mobile devices were also pinpointed.

Experience-based learning

Experience-based learning was used to provide students with a direct negative experience. This lesson type is described in depth in (Šimandl & Dobiáš, 2017); the following text provides a brief overview. During the preparation of this lesson type, Kolb's model of experiential learning (1984) was referred to for inspiration. Therefore, experience plays a central role in this lesson type.

Lessons consisted of a teacher-led talk and an experiential part, where students were provided with a certain negative experience. During the teacher-led talk, the teacher spoke on the topic and students listened to him. The lesson was enriched with graphic and audio-visual materials and the teacher asked students questions to encourage their participation. The experiential part was based on coping with a negative experience. Two e-safety risk scenarios were prepared by us and the students had to cope with them. If a student was unable to avoid these risk situations, it became a negative experience for him. As stated by Kolb (1984), the specific experience should be followed by hindsight and reflection. Hence, lessons included both provision of a negative experience and a follow-up analysis of the experienced situation and its actual and potential consequences.

Both e-safety risk scenarios were created to enable students to notice certain risk features and react to them, thus avoiding the threat. This is an important requirement not only from an ethical point of view but also for students to realise that they do have the choice and to acknowledge a certain amount of responsibility for not having foreseen the risk.

The first risk scenario was a phishing attack. To carry out this attack, a website was created to appear just like the school's information system. On entering the correct URL address of the school's information system during the lesson, students were redirected to this website. After logging onto the website, the student is offered a Christmas scholarship. In order to be eligible, he was asked to enter his National Insurance number. If the student did so, a successful completion announcement came up. A few seconds later, another of our webpages appeared automatically to warn of the fraudulent nature of the website.

The second risk scenario was registration on an unknown website. Several days before the planned lesson, students were sent an email from a fictitious student, informing them of a new website. The website offered materials to make their study easier (e.g., lesson notes or tests from previous years). To access the materials, the user was to register by entering his email address, choosing a password and agreeing with the website's Conditions of Use. The Conditions of Use stated that (the user) is aware that no further learning materials will be accessible after registering and that the information

provided at registration may be used for other purposes. Data given at registration was stored in a database – email address in legible form, password in hashed form.

Organization of the lesson. Students are told by the teacher to go onto the web resembling the school's information system (see first threat). If a student enters the requested details, a warning message appears and this should result in a negative experience – the student should feel that his personal data (National Insurance number) has been misused by hackers. The teacher turns this situation into a discussion on e-safety issues, following on with a teacher-led talk focusing on e-safety.

The teacher-led talk gets onto the issue of passwords, with the teacher showing students the Pirate-VŠTE website and displaying a list of all email addresses used during registration along with the hashed password. The students' negative experience should be connected with the students' feeling that they had been deceived and strangers now have access to data they entered. The teacher again goes back to the list of emails and passwords and points out that a number of students who had logged onto the online service must have agreed with the website conditions without having read them. The negative experience should be associated with the students' awareness of having consented to conditions of use that they don't agree with and that are to their disadvantage.

Ethics. While proposing lessons, the created solution has led us to deal with some ethical issues. Lessons cater for a debriefing with students, focused on an analysis of the two experienced situations simulating e-safety risks. Students are informed that they had faced simulations of real attacks and are reassured that none of the data they had entered was not, is not, and will not be misused. They are then given the opportunity to express their opinions or ask questions concerning what had gone on.

Both risk scenarios were prepared in such a way that users' private data was not put at risk during any of the procedures used to create the websites. Furthermore, efforts were made in both of the prepared scenarios to involve elements that would warn students of an attempted e-safety attack.

The Expert's talk

Our research on teachers' e-safety knowledge and routines has shown that teachers differentiate sources of information according to their trustworthiness and relevance (Šimandl, 2015). This led us to the decision to give lessons added value by inviting an external expert whose authority is likely to be more highly acknowledged by students. This Expert's talk took the form of teacher-led talk. The expert made every effort to convey negative experiences by talking about specific cases involving stories of people who the learner can relate to.

The lesson itself is taken by a teacher from another university who is introduced to students as an experienced expert. This raises his prestige in the eyes of the students. The expert aims to popularise the issue in his talk, focusing on the most serious risks and their typical features. He illustrates these with stories from his work experience, making efforts to convey negative experiences. The expert provides space for discussion and answers students' questions. In order to be more flexible, he does not use a digital presentation.

The Lecture

The Lecture provided students with information both on e-safety principles and ICT risks. E-safety principles were described, different types of risk were covered, and real-life examples of e-safety attacks were used. However, there was no emphasis on the negative experience of specific people who the students could relate to. The lecture is a widespread way of delivering lessons in the Czech Republic (Maňák & Švec, 2003; Podlahová, Vaněčková, Heřmánková, Klement, & Marešová, 2012; Skalková, 2007). As teachers and students are used to this method, it lacks the effect of being something new (unlike the other methods). Due to its frequent use, the lecture could be considered as the teaching method that controls the other teaching methods through comparison (Hays, 2005). The lecture provides quality information rapidly and may initiate deep feelings and experiences in students

(Maňák & Švec, 2003). On the other hand, it is difficult for students to remain attentive (Podlahová et al., 2012). It presents sorted facts which do not require further processing or immediate reactions (Maňák & Švec, 2003), which may result in students' lack of awareness of e-safety.

The Lecture applies the normal theoretical base of this teaching method. The teacher presents the topic and students listen to him. A number of graphic and audio-visual materials are used to enhance the Lecture. The teacher tries to make it more interesting by adding plenty of real-life examples. The teacher asks students questions to find out about their e-safety knowledge and routines and is open to discussion.

Group learning

The group learning method gives students the space to share their knowledge, skills, and experiences in a group, where students can mutually learn from each other (Maňák & Švec, 2003). This form of group learning contains elements of connectivism. If students learn mutually from each other, learning is indeed a process of connecting specialized nodes, that is, each of the students. Although learning does not a priori involve digital technologies, the learner creates a social network around himself, where active communication occurs. If the lesson focuses on events that are at least partially known to students, Siemens' stance (2005) that knowledge rests in diversity of opinions cannot be contradicted.

Our Group learning begins with the activisation method of brainstorming (Petty, 2009) terms relating to digital e-safety. Students are then divided into groups of three or four and each group is given one e-safety topic. Groups are to produce a short (5–10 minutes) oral presentation which they give in front of the other students. They are allocated around 45 minutes to do the task. Students are free to use the Internet, although they are encouraged to express their own experience and perspectives. The students themselves follow with their presentations and the teacher adds important information that a particular group forgets to mention.

The Semantic Differential

The semantic differential is designed to measure individual psychological meanings of certain keywords used by particular people by placing these keywords in a so-called semantic space (Chráska, 2007). Semantic differential questionnaires were used to measure these meanings. As the chosen research method is extensively discussed in Šimandl, Šerý, and Dobiáš (2017), only a brief description follows.

The questionnaires were made up of a total of twelve seven-point rating scales with outer points representing pairs of adjectives of opposite meaning (bipolar adjectives) chosen according to C. Osgood (Chráska, 2007). Participants made judgements about their perception of fifteen keywords and recorded them on the scales by choosing a particular point on these scales (Chráska, 2007). See the appendix for the semantic differential questionnaire. (The appendix does not include the page with instructions.)

In the questionnaire, the keywords to be judged are the focus of the research problem (Kerlinger, 1972). They are: Privacy, Email, Backup, Password, Ulož.to (the Czech equivalent of RapidShare.com; often used for the illegal distribution of works protected by copyright law), Facebook, Virus, and Loss. Keywords that are not directly connected to the issue of digital e-safety but characterise the participant himself were added to the semantic differential questionnaire in order to understand the connotative meaning of the above-mentioned keywords in a wider context (Šerý, 2013). The following keywords were chosen: Me, Fear, Knowledge, Life, Work, Money, and Teacher.

Analysing Data from the Semantic Differential Questionnaires

Data was analysed using our own software (Šerý, 2013). Data analysis was based on the method of global evaluation of keyword similarity, which allows us to judge the extent to which keywords can be

considered semantically similar or different, as claimed by Ferjenčík (2000). The Euclidean distance was used to calculate this so-called D-statistic (Kerlinger, 1972). The distance D_{ij} between keywords i and j was calculated according to this equation

$$D_{ij} = \sqrt{\sum_{k=1}^{12} \left(x_i(k) - x_j(k)\right)^2},$$

where $x_i(k)$ is the value of the k^{th} scale (i.e. the chosen value for the k^{th} pair of adjectives) for keyword *i* (see Kerlinger, 1972; Šerý, 2013). This means that the smaller the distance D_{ij}, the closer the given keywords *i* and *j* are in meaning and vice versa (Kerlinger, 1972). The calculated values of distance D were then recorded in a symmetrical D-matrix (Chráska, 2007). To calculate the global assessment of keywords by group of participants, the appropriate D-matrix was calculated for each participant separately, and then a final D-matrix with average distances was created (Šerý, 2013). The agglomerative clustering method was used during the analysis (Meloun & Militký, 2006), where each object at the beginning of this algorithm is regarded as a cluster. In each following step the two clusters nearest each other are joined into a single one. This process of gradual clustering gradually groups all objects into one big cluster (Meloun & Militký, 2006). Dendrograms were used to illustrate the arrangement graphically (Šerý, 2013).

The analysis of keyword data similarity was based on finding which of the other digital e-safety keywords it clustered with in the created dendrograms, given a certain number of clusters. To enable us to determine changes in perception of keyword, the pre-test dendrogram of a certain group of participants was compared with the post-test dendrogram of this group, observing any possible inter-cluster movement of a particular keyword. The following situations can be considered inter-cluster movement of keywords:

- Certain keywords in the pre-test dendrogram are in the same cluster, given a certain number of clusters, but in the post-test dendrogram they are in various clusters, given the same number of clusters. This movement is referred to below as being in the direction "*From one another*".
- Certain keywords in the pre-test dendrogram are in various clusters, given a certain number of clusters, but in the post-test dendrogram they are in one cluster, given the same number of clusters. This movement is referred to below as being in the direction "*To one another*".

Inter-cluster movement of keywords that was not a result of the lessons but a result of abnormalities in the experimental group was subsequently ruled out. Movement was ruled out where the initial inter-cluster pattern of observed keywords was different from that of the control group or the resulting inter-cluster pattern of observed keywords was the same as that of the control group.

As certain keywords moved closer to each other after lesson delivery in the direction "*To one another*", this movement is interpreted as participants beginning to perceive these keywords as being more similar to each other. As certain keywords moved away from each other after lesson delivery in the direction "*From one another*", this movement is interpreted as participants beginning to perceive them as less similar to each other.

RESULTS

The results are presented from a point of view of how a given type of lesson influenced participants' perception of selected digital e-safety keywords. The following information is given for each type of lesson:

- Dendrograms displaying the mutual similarity of selected keywords as perceived by a given group of participants before lessons (i.e., in the pre-test) and after lessons (i.e., in the post-test)

- A table listing the inter-cluster movement of keywords, having compared the pre-test and post-test dendrograms. The table only includes inter-cluster movement that was confirmed in a comparison with the control group (the pre-test and post-test dendrogram for the control group is shown in Figure 1). In rows of the table:
  - The direction "*To one another*" means that sets Keywords A and Keywords B created two differing clusters in the pre-test dendrogram, while creating one cluster in the post-test dendrogram. Note: This comparison was done given the splitting of the keyword set into a certain number of clusters which was the same for the pre-test dendrogram as for the post-test dendrogram. This number of clusters is specified in the column Number of clusters.
  - The direction "*From one another*" means that sets Keywords A and Keywords B created one cluster in the pre-test dendrogram, while creating two differing clusters in the post-test dendrogram.
- A discussion of the discovered inter-cluster movement of keywords

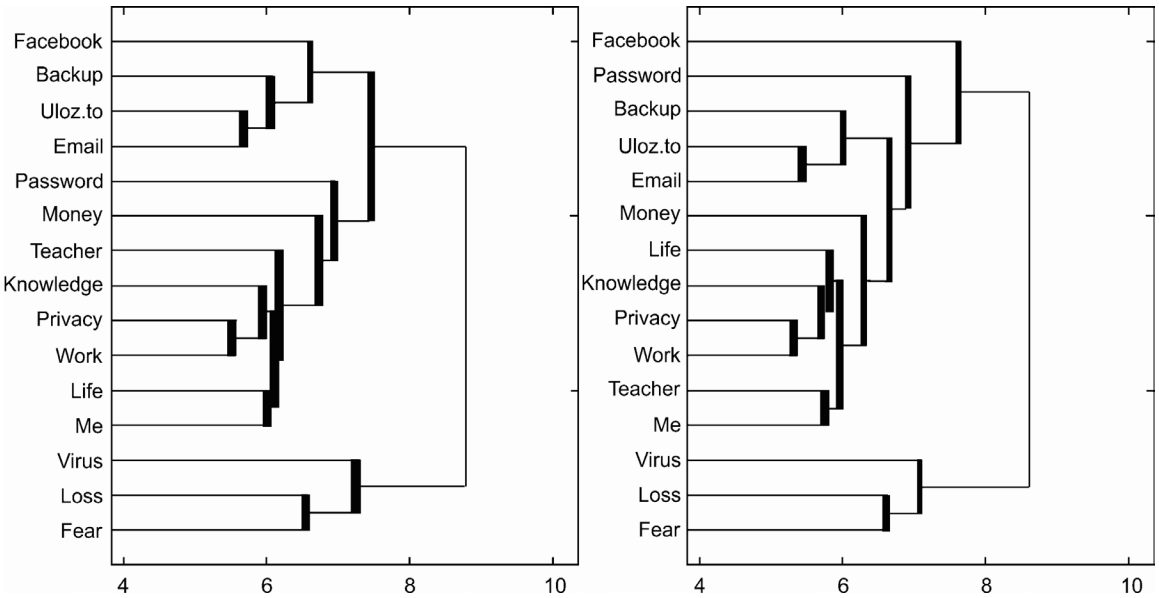


Figure 1. Pre-test dendrogram (on the left) and post-test dendrogram (on the right) for the control group

EXPERIENCE-BASED LEARNING

Table 2 shows inter-cluster movement of keywords found by analyzing the dendrograms in Figure 2 to be of significance for students having attended Experience-based learning.

Table 2. Inter-cluster movement of keywords for Experience-based learning – all students having attended this type of lesson

Keywords A	Keywords B	Direction	Number of clusters
Backup	Privacy, Money	To one another	7
Facebook	Ulož.to, E-mail	To one another	10

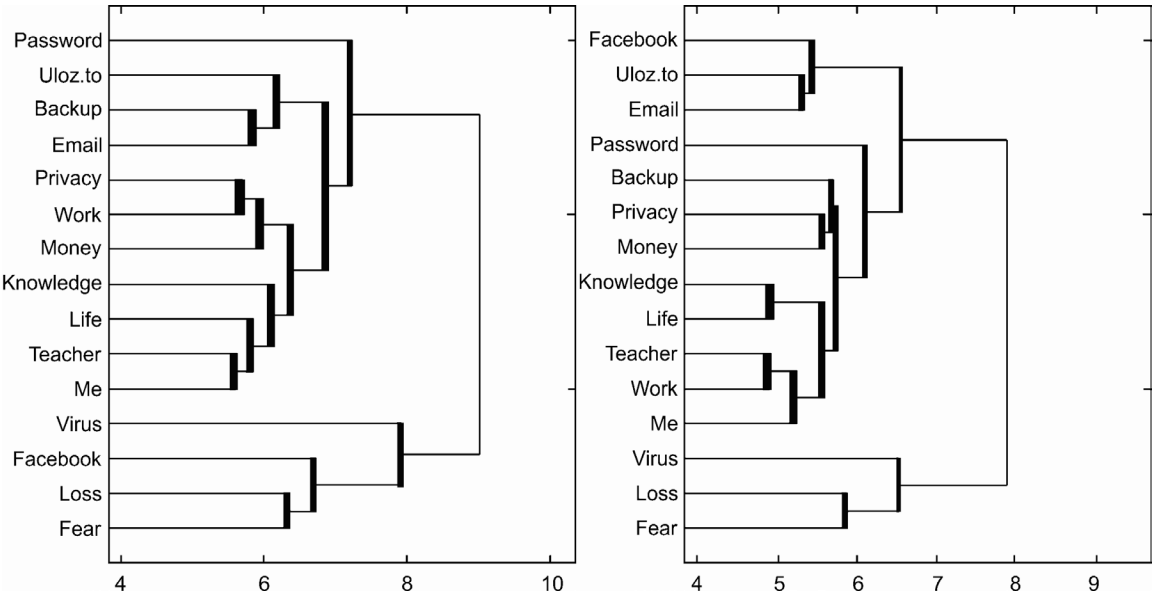


Figure 2. Pre-test dendrogram (on the left) and post-test dendrogram (on the right) for Experience-based learning – all students having attended this type of lesson

Following lessons, the keyword **Backup** moved closer to keywords **Privacy** and **Money.** This could mean that participants became more aware that backed up data is relatively valuable, just like money. Although this is unlikely to be associated with the negative experience that was provided as part of the Experience-based learning, it may be linked to the part of the lesson based on the teacher-led talk. The effectiveness of the lesson may have been increased by the experiential elements that had previously been incorporated in the lesson. The change is seen by us as positive. It gives hope that lessons have led to participants' greater awareness of the fact that backing up is a way of protecting their data (and that data backup needs to be taken more seriously than prior to lessons).

Following lessons, the keyword **Facebook** moved closer to the keywords **Ulož.to** and **Email**, which leads us to believe that participants became more aware of what various services had in common – the possibility for users to share information and data. Although this is not likely to be linked to the negative experience that was provided as part of the Experience-based learning, it may be associated to the part of the lesson based on the teacher-led talk. Nevertheless, as the lessons were not primarily focused on differentiating between various types of cloud services, this change is perceived by us as neutral.

Experience-based learning with registration on an unknown website

The scrutinized group was made up only of those students who had participated in the Experience-based learning and had registered themselves on an unknown website (see description of teaching methods). Table 3 shows inter-cluster movement of keywords found by analyzing the dendrograms in Figure 3 to be of significance for these students.

Table 3. Inter-cluster movement of keywords for Experience-based learning – students who had registered themselves on an unknown website

Keywords A	Keywords B	Direction	Number of clusters
Password	Me	To one another	5
Virus	Loss	To one another	4
Facebook	Ulož.to, E-mail	To one another	10

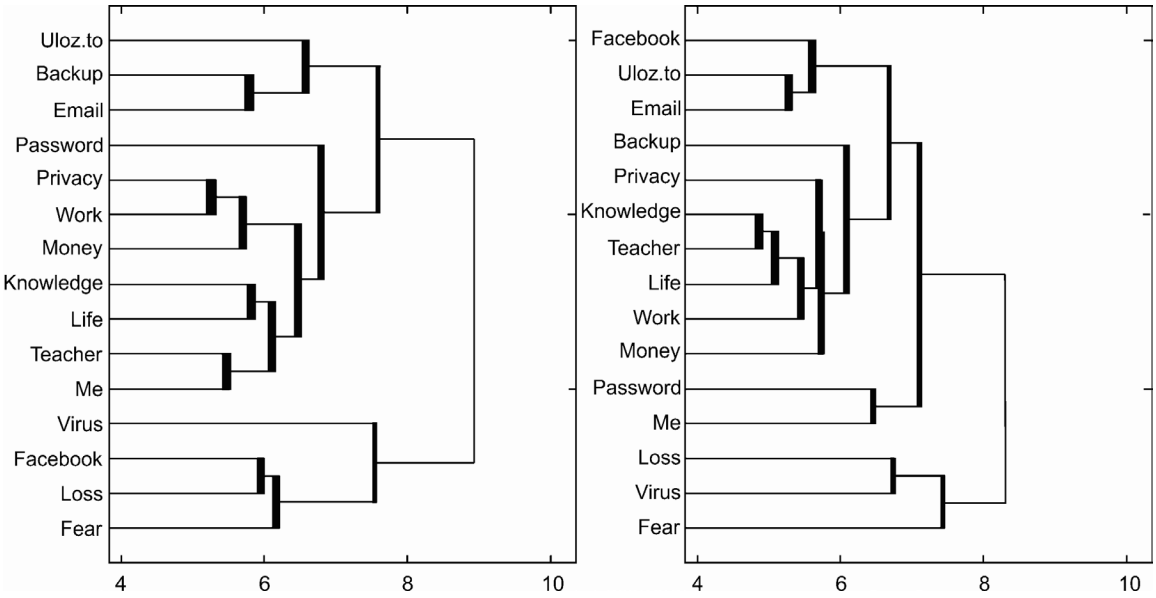


Figure 3. Pre-test dendrogram (on the left) and post-test dendrogram (on the right) for Experience-based learning – students who had registered themselves on an unknown website

The keyword **Password** moving closer to the keyword **Me** leads us to believe that participants have become more aware that passwords are the key to their person and data. Choosing an appropriate password and keeping it secure are vital to staying safe when using ICT. This move appears to be directly linked to the negative experience provided during the Experience-based learning lesson and directly experienced by participants. This change is perceived by us as positive. It gives hope that lessons have led to participants' greater awareness of the fact that their password is an element that keeps their person and data secure (and that they should adopt a more consistent approach to choice and use of password than prior to lessons).

The keyword **Virus** moving closer to the keyword **Loss** leads us to believe that participants became more aware that a virus brings the risk of a certain loss. Although this is unlikely to be linked to the negative experience provided during the Experience-based learning lesson, it may be associated with the part of the lesson based on the teacher-led talk. This change is perceived by us as positive. It gives hope that lessons have led to participants' greater awareness of the fact that a virus is a negative element resulting in a certain loss (and that they need to take antivirus protection more seriously than prior to lessons).

The keyword **Facebook** moving closer to the keywords **Ulož.to** and **Email** coincides with the results of the whole Experience-based learning group, as stated above. This change is perceived by us as neutral.

The Expert's talk

Table 4 shows inter-cluster movement of keywords found by analyzing the dendrograms in Figure 4 to be of significance for students who had attended The Expert's talk.

Table 4. Inter-cluster movement of keywords for The Expert's talk

Keywords A	Keywords B	Direction	Number of clusters
Virus	Loss	To one another	4
Facebook	Loss, Virus	To one another	2

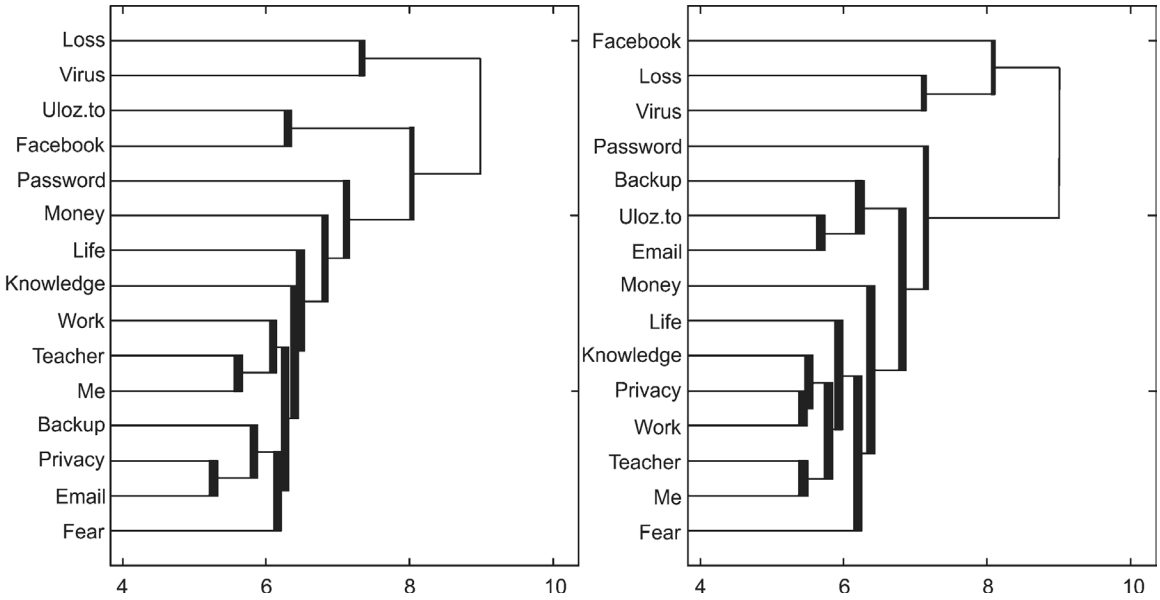


Figure 4. Pre-test dendrogram (on the left) and post-test dendrogram (on the right) for The Expert's talk

After lesson delivery, the keyword **Virus** moved closer to the keyword **Loss**, which could mean that participants became more aware that a virus brings the risk of a certain loss (e.g., loss of data, loss of privacy, or financial loss). This change in perception of the keywords in question gives hope that lessons have led to participants' greater awareness of the fact that viruses are a negative element that could result in a certain loss (and that they need to do more to protect themselves from viruses than prior to the lessons). For that reason, we find this a positive change.

Following lessons, the keyword **Facebook** moved closer to the keywords **Loss** and **Virus.** This leads us to believe that participants became more aware that using Facebook brings the risk of a certain loss (e.g., loss of privacy, loss of control over one's data). This is comparable to the effects of a computer virus, which brings the risk of a similar loss. This change gives hope that lessons have led to participants becoming more aware of the risk of privacy loss or loss of control over one's data resulting from the use of Facebook (and becoming more careful when using Facebook than prior to lessons). For that reason, we find this change positive.

THE LECTURE

Table 5 shows inter-cluster movement of keywords, found by analyzing the dendrograms in Figure 5 to be of significance for students who had attended the Lecture.

Table 5. Inter-cluster movement of keywords for the Lecture

Keywords A	Keywords B	Direction	Number of clusters
Virus	Loss	From one another	3
Ulož.to	Backup, E-mail	From one another	6
Ulož.to	Facebook	To one another	8

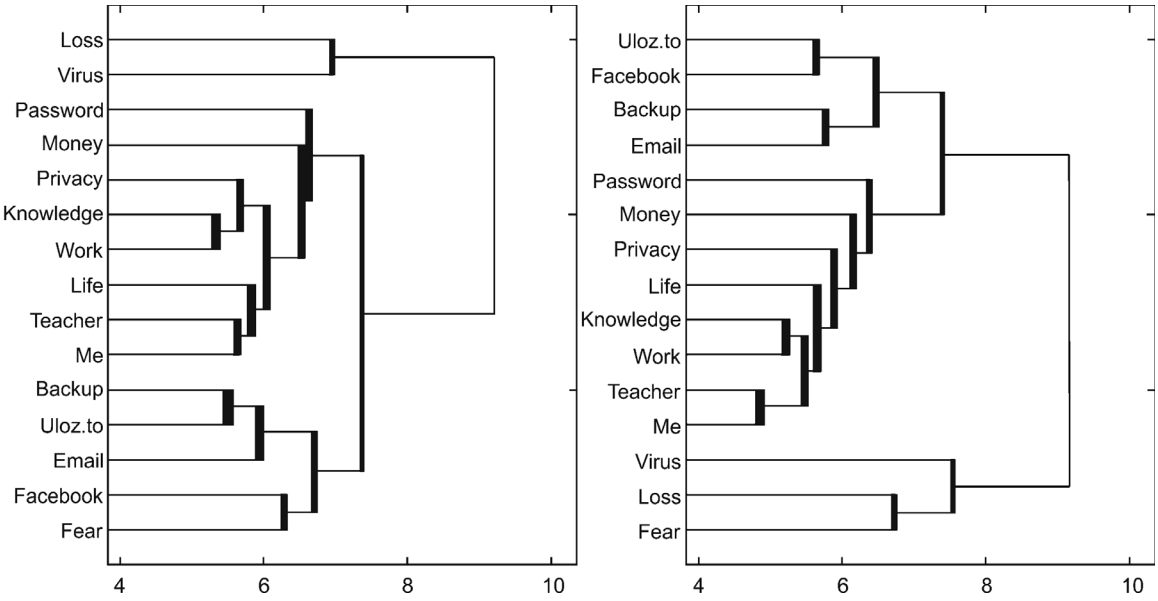


Figure 5. Pre-test dendrogram (on the left) and post-test dendrogram (on the right) for the Lecture

After lesson delivery, keywords **Virus** and **Loss** moved away from each other. This could mean that participants have become less aware that a virus carries the risk of a certain loss (e.g., loss of data, loss of privacy, or financial loss). This move could be evidence of a certain contra-productivity of the Lecture, which might have distorted a participant's original conceptions of computer viruses without creating a new perception of this keyword in terms of its consequences. Hence, this change is perceived by us as negative.

After lesson delivery, the keyword **Ulož.to** moved away from keywords **Backup** and **Email.** Participants seem to have become more aware that ulož.to is a public file-hosting service enabling users to share data but is unsuitable for storing personal data and backup whereas an email box is a private area that other users should have no access to. Therefore, personal data can be stored in the email box or kept there as a certain type of backup. This change is perceived by us as positive. It gives hope that lessons have facilitated participants' ability to differentiate between various cloud services (increasing their awareness of where to store what data and how to use a certain service).

The keyword **Ulož.to** moved closer to the keyword **Facebook.** Participants seem to have become more aware of the similarity of these services. Both involve one user publishing data and its occasional consumption by another user. This move may be related to the above-mentioned move of Ulož.to away from Email, resulting in the keyword Ulož.to moving closer to another keyword representing an online service. For that reason, it is perceived by us as neutral.

Group Learning

Table 6 shows inter-cluster movement of keywords found by analyzing the dendrograms in Figure 6 to be of significance for students who had attended Group learning.

Table 6. Inter-cluster movement of keywords for Group learning

Keywords A	Keywords B	Direction	Number of clusters
Backup	Knowledge	To one another	9
Knowledge	Me, Privacy, Work, Life, Money	From one another	9

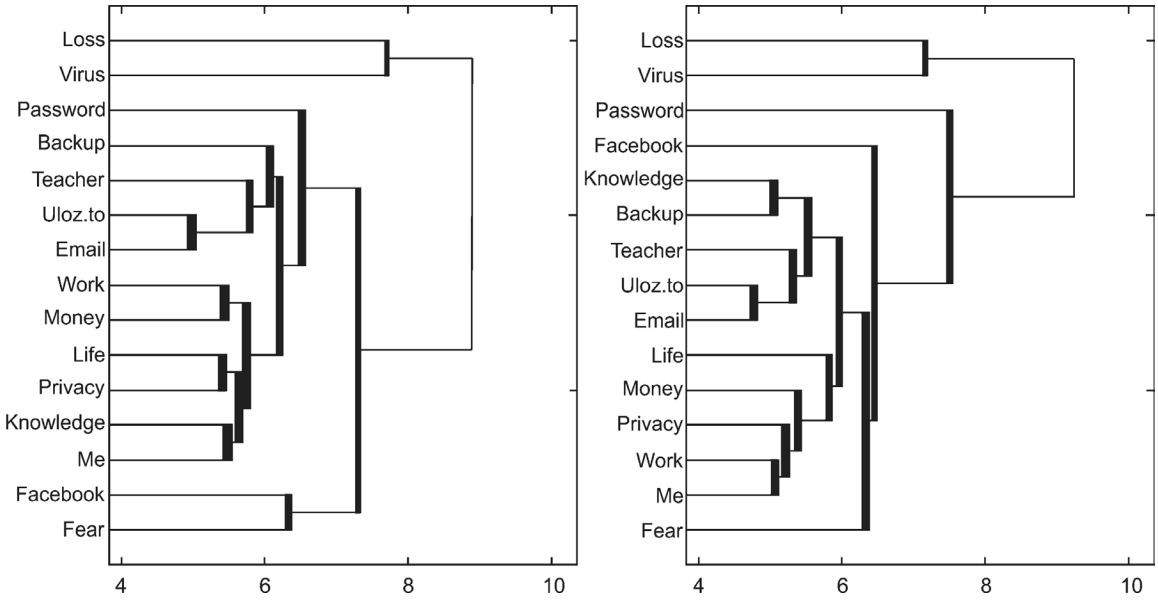


Figure 6. Pre-test dendrogram (on the left) and post-test dendrogram (on the right) for Group learning

Following lessons, the keyword **Backup** moved closer to the keyword **Knowledge**. This leads us to believe that participants became more aware of backing up as a deliberate and purposeful activity that requires certain knowledge (e.g., how to make a backup and what media to use). The above-mentioned change in perception of keywords Backup and Knowledge is further emphasized by the keyword Knowledge moving away from the cluster of keywords Me, Privacy, Work, Life, Money. The change in perception of the keywords in question is considered positive by us. It gives hope that lessons lead to participants' increased awareness of backing up as a deliberate and purposeful activity (and to more careful planning of data backup than prior to lessons).

DISCUSSION

From a holistic point of view (i.e., focusing on all students attending this type of lesson), Experience-based learning seems to be relatively effective. However, its effectiveness seems more likely to be rooted in the part of the lesson based on the teacher-led talk than in the part where students were confronted with a particular negative experience. Our research has not revealed any changes in the way students perceive the areas of e-safety in which they had been given the chance to experience the risks. For that reason, the prepared e-safety risk scenarios must be considered merely as activisation elements, particularly for those students who were not deceived by them. However, a different situation occurred when focusing on those learners who had been deceived by the prepared e-safety risk scenario. They developed a more favorable perception of e-safety, noticeable in the areas of digital e-safety that the prepared scenarios focused on. This gives us reason to assume that the lessons demonstrated the need for those students to improve their e-safety strategies. This was the impulse for them to change their perception of e-safety. According to Piaget (1936/1965), that means noticeable accommodation occurred in the students. Considering the nature of the lessons, it could be classed as a successful example of experiential learning (Kolb, 1984).

Lessons based on the Expert's talk seem to be relatively effective. Students who had attended it became more aware of digital e-safety issues that the lessons had focused on. However, the effectiveness of lessons may have been distorted by this new teaching method and by students' expectations of a prestigious expert lecturer who will explain the topic better than the average teacher. Cognitive bias or, more precisely, the social status effect (Bednář, Drahoňovský, Hlušička, & Těšitelová, 2013)

may have occurred here. This may have led students to be more open to hearing an expert conveying his experience. The expert lecturer's personality may have also played its part, being different from the personality of the teacher in the other types of lessons. Such differences in personality and knowledge of their profession are natural, this being the reason for inviting an expert into the classroom.

The Lecture seems to be effective in certain respects. But it does run the risk of being counterproductive. During lessons, students' initial perceptions of an issue (which needn't necessarily be completely wrong) may be distorted. However, they will not be sufficiently replaced by a new complex view of the given area (e.g., due to the vast number of facts). In terms of Piaget's theory (1936/1965), lessons caused disequilibrium in the students and the formation of new schema. However, some of the schema may have been formed by misinterpretation of transferred information. As claimed by Nichols (2000), in the formation of the schema, this situation has a negative exponential effect on the completion of the correct schema, as one piece of information is crucial for each component that follows. The effectiveness of the Lecture might have been distorted because the students and teacher are accustomed to this method in routine lesson delivery. Due to this, students are not preoccupied with a new method of teaching but both they and the teacher are able to work very effectively with it.

In accordance with the created scenario, Group learning seems to be effective in certain respects. Despite this, its effect is smaller than that of the other styles of teaching. However, the effectiveness of this method may have been negatively influenced by the fact that students are not used to working in this particular way, lacking the ability to mutually share their knowledge. This gives us reason to assume that many students had trouble understanding the issue in a broader context and presenting relevant facts in an appropriate way. Moreover, students were unable to find coherence among pieces of information and to create a holistic picture. However, according to Siemens' principles of connectivism (2005), the ability to see connections between fields, ideas, and concepts is a core skill.

Lessons based on the Expert's talk have been found to improve e-safety knowledge and routines. Such lessons have led to a more significant improvement than Lecture-type lessons. Experience-based learning has benefited those students who were deceived by the prepared risk scenario. It can therefore be assumed that the negative experience had a positive influence on the perception of e-safety of those learners who were directly affected by it. However, it is yet to be determined whether this will result in such an effect every time. The fact that it may depend on other circumstances cannot be ruled out (e.g., whether or not the student accepts his share of the blame for not having foreseen the risk).

CONCLUSION

Our study has aimed to discover the way various teaching methods influence students' perception of the issue of digital e-safety. One of the techniques used for instruction was to simulate an e-safety threat, which provided students with a direct negative experience. Another method was to have a negative experience conveyed through an expert's talk, which illustrated particular risks by talking about specific cases involving stories of people who the learner can relate to. Other lessons were delivered in the form of classic lecture and group learning.

The results of the experiment indicate that prepared e-safety risk scenarios have a positive influence on the perception of e-safety of those learners who were deceived by them and therefore subjected to a negative experience. However, there was no effect on those students who had not been fooled by it. Hence, the technique used for instruction can be compared to the treatment of disease, which only affects the individual who requires a particular type of intervention. Students' perception of digital e-safety was positively influenced by lessons based on the expert's talk, which had a more significant impact than lessons delivered in the form of classic lecture. Group learning had a smaller impact than the other three teaching techniques.

This research indicates that e-safety instruction can be enhanced by ensuring that lessons provide students with a personal experience. Moreover, our research has revealed the possibility to create tools to support digital e-safety lessons. Learners would be provided a negative experience and its usefulness and effectiveness would be verified in lessons using appropriate methods. However, it would be necessary to consider not only technical issues but also ethical issues, making this type of intervention relatively challenging to implement.

There are certain limitations to the research related to problems with the research setup. The Expert's talk involved a university teacher with a long track record in the field of e-safety acting as the expert. If a real IT expert (e.g., from a company dealing with computer safety and security) had been invited, the question remains as to whether this expert would have been able to communicate with students in an appropriate way (i.e., without overloading them with technical details that they would not understand). Another limitation of the research is that the course of Experience-based learning was dependent on whether certain students were deceived by prepared e-safety risk scenarios. If none of the students had been deceived, the teacher would not have been able to use the e-safety risks in the intended pedagogical scenario. A solution would be to prepare an alternative pedagogical scenario. This would involve the teacher acting as a user confronted with a risk which leads him to becoming deceived. This would at least allow the students to experience a demonstrated negative experience, aware that they could have been the victim of deception.

Future research should focus on examining how the experiential learning method affects the attitudes of younger learners (primary, middle, and high school students). It would presumably be more difficult to propose appropriate teaching styles for such research. The college students researched for our study are usually aware of e-safety rules, and there is only a need to push them to follow the rules. On the other hand, younger learners will have to be initially educated about cyber threats. This will involve placing an emphasis on the reality of threats as well as the chances of rationally overcoming them. If this does not occur, learners could develop an unfounded fear of the risks inherent in ICT. Moreover, future research could be focused on investigating whether the use of e-safety risk scenarios in lessons really does have a positive influence on the perception of e-safety of those learners who were deceived by them. Perhaps it could focus on revealing the determinants that strengthen the effect of such lessons or, conversely, subdue it.

REFERENCES

Aytes, K., & Connolly, T. (2004). Computer security and risky computing practices: A rational choice perspective. *Journal of Organizational and End User Computing*, *16*(3), 22–40. https://doi.org/10.4018/joeuc.2004070102

Bandura, A. (1977). *Social learning theory* (2nd ed.). Englewood Cliffs, N.J: Prentice Hall.

Barnard-Wills, D., & Ashenden, D. (2015). Playing with privacy: Games for education and communication in the politics of online privacy. *Political Studies*, *63*(1), 142–160. https://doi.org/10.1111/1467-9248.12049

Barrow, C., & Heywood-Everett, G. (2006). *E-safety: The experience in English educational establishments*. Coventry: British Educational Communications and Technology Agency. Retrieved from http://dera.ioe.ac.uk/1619/1/becta_2005_esafetyaudit_report.pdf

Bednář, V., Drahoňovský, J., Hlušička, P., & Těšitelová, H. (2013*). Sociální vztahy v organizaci a jejich management* [Social relationships in the organization and their management]. Praha: Grada.

Beránek, L. (2009). Information systems security education for future teacher at secondary and primary schools. *Journal of Technology and Information Education*, *1*(2), 89–93. https://doi.org/10.5507/jtie.2009.043

British Educational Communications and Technology Agency. (2005). *E-safety: Developing whole-school policies to support effective practice*. Coventry: British Educational Communications and Technology Agency. Retrieved from http://www.wisekids.org.uk/BECTA%20Publications/esafety.pdf

British Educational Communications and Technology Agency. (2006). *Safeguarding children in a digital world: Developing a strategic approach to e-safety*. Coventry: British Educational Communications and Technology Agency. Retrieved from http://webarchive.nationalarchives.gov.uk/20101102103654/http://publications.becta.org.uk/download.cfm?resID=25933

British Educational Communications and Technology Agency. (2007). *Signposts to safety: Teaching e-safety at Key Stages 3 and 4*. Coventry: British Educational Communications and Technology Agency. Retrieved from https://www.education.gov.uk/publications/eOrderingDownload/signposts_safety_ks3and4.pdf

Byron, T. (2008). *Safer children in a digital world: The report of the Byron review*. Department for Children, Schools and Families. Retrieved from http://webarchive.nationalarchives.gov.uk/20130401151715/http://www.education.gov.uk/publications/eOrderingDownload/DCSF-00334-2008.pdf

Chráska, M. (2007). *Metody pedagogického výzkumu: základy kvantitativního výzkumu* [Methods of pedagogical research: The basics of quantitative research]. Praha: Grada.

Child Exploitation and Online Protection. (2008). *IYAC children and young persons' global online charter: Supplementary document*. London: Child Exploitation and Online Protection. Retrieved from http://webarchive.nationalarchives.gov.uk/20101225011254/http://www.ceop.police.uk/Documents/iyac_charter_supp.pdf

Činčera, J., & Caha, M. (2005). *Výchova a budoucnost: Hry a techniky o životním prostředí a společnosti* [Education and the future: Games and techniques about the environment and society]. Brno: Paido.

Dewey, J. (1997). *Experience and education* (1st Touchstone ed.). New York, NY: Simon and Schuster.

European Computer Driving Licence Foundation Ltd. (2007a). *European Computer Driving Licence / International Computer Driving Licence – Concepts ICT sylabus 5.0 (M1)*. Retrieved from http://www.ecdl.cz/data/Sylabus-ECDL-CZ-M1-5.0.pdf

European Computer Driving Licence Foundation Ltd. (2007b). *European Computer Driving Licence / International Computer Driving Licence – Concepts ICT sylabus 5.0 (M7)*. Retrieved from http://www.ecdl.cz/data/Sylabus-ECDL-CZ-M7-5.0.pdf

Eynon, R. (2009). *Harnessing technology: The learner and their context: Mapping young people's uses of technology in their own contexts – A nationally representative survey*. Coventry: British Educational Communications and Technology Agency. Retrieved from http://archive.teachfind.com/becta/research.becta.org.uk/uploaddir/downloads/page_documents/research/reports/ht_learner_context_survey.doc

Ferjenčík, J. (2000). *Úvod do metodologie psychologického výzkumu: Jak zkoumat lidskou duši* [Introduction to the methodology of psychological research: How to explore the human psyche]. Praha: Portál.

Hayes, N. (1993). *Principles of social psychology*. Abingdon, Oxon: Routledge.

Hays, R. T. (2005). *The effectiveness of instructional games: A literature review and discussion*. Orlando: Naval Air Warfare Center Training Systems Division. https://doi.org/10.21236/ADA441935

Herbart, J. F. (1806). *Allgemeine Pädagogik: Aus dem Zweck der Erziehung abgeleitet* [General pedagogy: Derived from the purpose of education]. Göttingen: JF Röwer.

Kerlinger, F. N. (1972). *Základy výzkumu chování: Pedagogický a psychologický výzkum* [The basics of behavioral research: Pedagogical and psychological research]. Praha: Academia.

Kolb, D. A. (1984). *Experiential learning: Experience as the source of learning and development*. Englewood Cliffs, NJ: Prentice Hall.

Lang, M., Devitt, J., Kelly, S., Kinneen, A., O Malley, J., & Prunty, D. (2009). Social networking and personal data security: A study of attitudes and public awareness in Ireland. *2009 International Conference on Management of e-Commerce and e-Government*, 486–490. https://doi.org/10.1109/ICMeCG.2009.105

Livingstone, S., & Bulger, M. (2013). *A global agenda for children's rights in the digital age*. Florence: UNICEF Office of Research. Retrieved from http://www.unicef-irc.org/publications/pdf/lse%20olol%20final3.pdf

Livingstone, S., & Haddon, L. (2009). *EU Kids Online: Final report*. London: EU Kids Online. Retrieved from http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20I%20%282006-9%29/EU%20Kids%20Online%20I%20Reports/EUKidsOnlineFinalReport.pdf

Maňák, J., & Švec, V. (2003). *Výukové metody* [Teaching methods]. Brno: Paido.

Meloun, M., & Militký, J. (2006). *Kompendium statistického zpracování dat: Metody a řešené úlohy* [Compendium of statistical data processing: Methods and solved tasks]. Praha: Academia.

Nichols, J. D. (2000). *Schema theory: A new twist using duplo models*. Annual Meeting of the American Educational Research Association. Retrieved from https://ia600208.us.archive.org/35/items/ERIC_ED440961/ERIC_ED440961.pdf

Organisation for Economic Co-operation and Development. (2011). The protection of children online: Risks faced by children online and policies to protect them. *OECD Digital Economy Papers*, No. 179. Paris: Organisation for Economic Co-operation and Development. https://doi.org/10.1787/5kgcjf71pl28-en

Papavasiliou, S. (2009). *Survey: Promotion of internet safety into the school curriculum*. SaferInternet.gr. Retrieved from http://www.saferinternet.org/c/document_library/get_file?p_l_id=10526&folderId=19099&name=DLFE-416.doc

Peltsverger, S., & Zheng, G. (2016). Enhancing privacy education with a technical emphasis in IT curriculum. *Journal of Information Technology Education: Innovations in Practice*, *15*, 1–17. Retrieved from https://www.informingscience.org/Publications/2330

Petty, G. (2009). *Teaching today: A practical guide* (4th ed.). Cheltenham: Nelson Thornes.

Piaget, J. (1965). *The origins of intelligence in children* (3rd ed.). (M. Cook, Trans.). New York: International Universities Press. (Original work published in 1936.)

Podlahová, L., Vaněčková, M., Heřmánková, P., Klement, M., & Marešová, J. (2012). *Didaktika pro vysokoškolské učitele* [Pedagogy for university teachers]. Praha: Grada.

Royal, B. (2015). *The little blue reasoning book: 50 powerful principles for clear and effective thinking* (Rev. ed.). Calgary: Maven Publishing.

Siemens, G. (2005). Connectivism: A learning theory for the digital age. *International Journal of Instructional Technology & Distance Learning*, *2*(1). Retrieved from http://www.itdl.org/journal/jan_05/article01.htm

Skalková, J. (2007). *Obecná didaktika: Vyučovací proces, učivo a jeho výběr, metody, organizační formy vyučování* [General pedagogy: Teaching process, curriculum and its selection, methods, organizational forms of teaching]. Praha: Grada.

South West Grid for Learning. (2009). *School online safety template policy*. Exeter: South West Grid for Learning. Retrieved from http://swgfl.org.uk/products-services/esafety/resources/creating-an-esafety-policy/Content/ESP_template-School-Template-Policy.aspx

Symantec Corporation. (2010). *Norton online family report: Global insights into family life online*. Mountain View: Symantec Corporation. Retrieved from http://us.norton.com/content/en/us/home_homeoffice/media/pdf/nofr/Norton_Family-Report-USA_June9.pdf

Šerý, M. (2013). *Použití sémantického diferenciálu při hodnocení výuky na ZŠ* [Using of semantic differential for education assessment at basic school]. (Doctoral dissertation, Jihočeská univerzita v Českých Budějovicích). Retrieved from http://theses.cz/id/m7rifg/Disertacni_prace_2013_v_28.pdf

Šimandl, V. (2015). ICT teachers and technical e-safety: Knowledge and routines. *International Journal of Information and Communication Technologies in Education*, *4*(2), 50–65. https://doi.org/10.1515/ijicte-2015-0009

Šimandl, V., & Dobiáš, V. (2017). Využití zkušenostního učení při výuce e-bezpečnosti [The use of experiential learning in e-safety lessons]. In D. Horváthová, J. Jacková, A. Michalíková, & J. Škrinárová (Eds.), *DidInfo&DidactIG 2017* (pp.147–152). Banská Bystrica: Univerzita Mateja Bela.

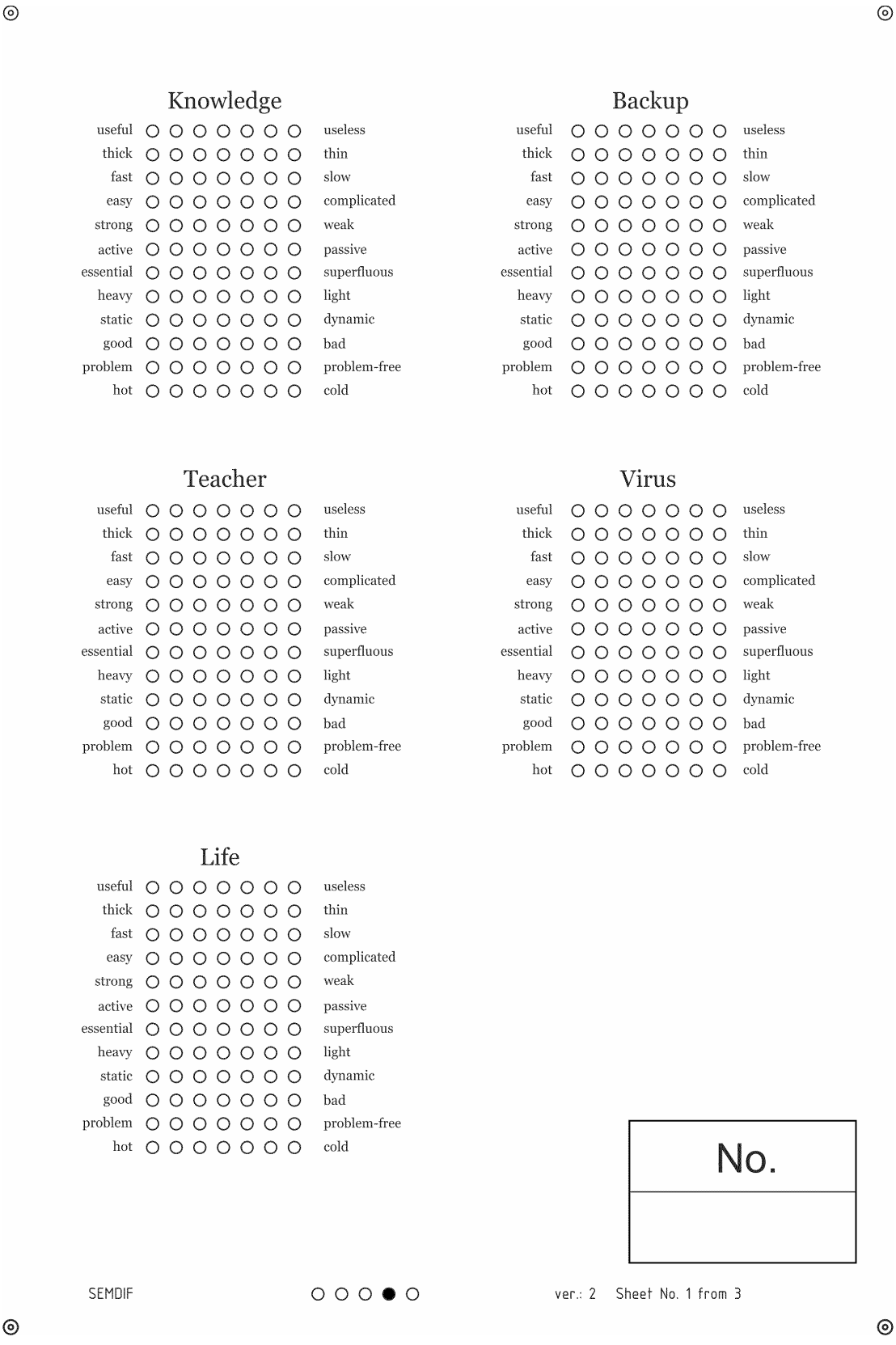
Šimandl, V., Šerý, M., & Dobiáš, V. (2017). Using semantic differential for measuring changes in understanding selected concepts by respondents. *16th Conference on Applied Mathematics APLIMAT 2017. Proceedings,* 1398–1408.

Šimandl, V., & Vaníček, J. (in press). Influences on ICT teachers knowledge and routines in a technical e-safety context. *Telematics and Informatics*. https://doi.org/10.1016/j.tele.2017.06.012

Vanderhoven, E., Schellens, T., Vanderlinde, R., & Valcke, M. (2016). Developing educational materials about risks on social network sites: a design based research approach. *Educational Technology Research and Development*, *64*(3), 459–480. https://doi.org/10.1007/s11423-015-9415-4

Wishart, J. M., & Morris, M. (2007). Using online role play to teach internet safety awareness. *Computers & Education*, *48*(3), 460–473. https://doi.org/10.1016/j.compedu.2005.03.003

APPENDIX



Knowledge

useful	○ ○ ○ ○ ○ ○ ○	useless
thick	○ ○ ○ ○ ○ ○ ○	thin
fast	○ ○ ○ ○ ○ ○ ○	slow
easy	○ ○ ○ ○ ○ ○ ○	complicated
strong	○ ○ ○ ○ ○ ○ ○	weak
active	○ ○ ○ ○ ○ ○ ○	passive
essential	○ ○ ○ ○ ○ ○ ○	superfluous
heavy	○ ○ ○ ○ ○ ○ ○	light
static	○ ○ ○ ○ ○ ○ ○	dynamic
good	○ ○ ○ ○ ○ ○ ○	bad
problem	○ ○ ○ ○ ○ ○ ○	problem-free
hot	○ ○ ○ ○ ○ ○ ○	cold

Backup

useful	○ ○ ○ ○ ○ ○ ○	useless
thick	○ ○ ○ ○ ○ ○ ○	thin
fast	○ ○ ○ ○ ○ ○ ○	slow
easy	○ ○ ○ ○ ○ ○ ○	complicated
strong	○ ○ ○ ○ ○ ○ ○	weak
active	○ ○ ○ ○ ○ ○ ○	passive
essential	○ ○ ○ ○ ○ ○ ○	superfluous
heavy	○ ○ ○ ○ ○ ○ ○	light
static	○ ○ ○ ○ ○ ○ ○	dynamic
good	○ ○ ○ ○ ○ ○ ○	bad
problem	○ ○ ○ ○ ○ ○ ○	problem-free
hot	○ ○ ○ ○ ○ ○ ○	cold

Teacher

useful	○ ○ ○ ○ ○ ○ ○	useless
thick	○ ○ ○ ○ ○ ○ ○	thin
fast	○ ○ ○ ○ ○ ○ ○	slow
easy	○ ○ ○ ○ ○ ○ ○	complicated
strong	○ ○ ○ ○ ○ ○ ○	weak
active	○ ○ ○ ○ ○ ○ ○	passive
essential	○ ○ ○ ○ ○ ○ ○	superfluous
heavy	○ ○ ○ ○ ○ ○ ○	light
static	○ ○ ○ ○ ○ ○ ○	dynamic
good	○ ○ ○ ○ ○ ○ ○	bad
problem	○ ○ ○ ○ ○ ○ ○	problem-free
hot	○ ○ ○ ○ ○ ○ ○	cold

Virus

useful	○ ○ ○ ○ ○ ○ ○	useless
thick	○ ○ ○ ○ ○ ○ ○	thin
fast	○ ○ ○ ○ ○ ○ ○	slow
easy	○ ○ ○ ○ ○ ○ ○	complicated
strong	○ ○ ○ ○ ○ ○ ○	weak
active	○ ○ ○ ○ ○ ○ ○	passive
essential	○ ○ ○ ○ ○ ○ ○	superfluous
heavy	○ ○ ○ ○ ○ ○ ○	light
static	○ ○ ○ ○ ○ ○ ○	dynamic
good	○ ○ ○ ○ ○ ○ ○	bad
problem	○ ○ ○ ○ ○ ○ ○	problem-free
hot	○ ○ ○ ○ ○ ○ ○	cold

Life

useful	○ ○ ○ ○ ○ ○ ○	useless
thick	○ ○ ○ ○ ○ ○ ○	thin
fast	○ ○ ○ ○ ○ ○ ○	slow
easy	○ ○ ○ ○ ○ ○ ○	complicated
strong	○ ○ ○ ○ ○ ○ ○	weak
active	○ ○ ○ ○ ○ ○ ○	passive
essential	○ ○ ○ ○ ○ ○ ○	superfluous
heavy	○ ○ ○ ○ ○ ○ ○	light
static	○ ○ ○ ○ ○ ○ ○	dynamic
good	○ ○ ○ ○ ○ ○ ○	bad
problem	○ ○ ○ ○ ○ ○ ○	problem-free
hot	○ ○ ○ ○ ○ ○ ○	cold

No.

SEMDIF ○ ○ ○ ● ○ ver.: 2 Sheet No. 1 from 3

Loss

useful	○ ○ ○ ○ ○ ○ ○	useless
thick	○ ○ ○ ○ ○ ○ ○	thin
fast	○ ○ ○ ○ ○ ○ ○	slow
easy	○ ○ ○ ○ ○ ○ ○	complicated
strong	○ ○ ○ ○ ○ ○ ○	weak
active	○ ○ ○ ○ ○ ○ ○	passive
essential	○ ○ ○ ○ ○ ○ ○	superfluous
heavy	○ ○ ○ ○ ○ ○ ○	light
static	○ ○ ○ ○ ○ ○ ○	dynamic
good	○ ○ ○ ○ ○ ○ ○	bad
problem	○ ○ ○ ○ ○ ○ ○	problem-free
hot	○ ○ ○ ○ ○ ○ ○	cold

Password

useful	○ ○ ○ ○ ○ ○ ○	useless
thick	○ ○ ○ ○ ○ ○ ○	thin
fast	○ ○ ○ ○ ○ ○ ○	slow
easy	○ ○ ○ ○ ○ ○ ○	complicated
strong	○ ○ ○ ○ ○ ○ ○	weak
active	○ ○ ○ ○ ○ ○ ○	passive
essential	○ ○ ○ ○ ○ ○ ○	superfluous
heavy	○ ○ ○ ○ ○ ○ ○	light
static	○ ○ ○ ○ ○ ○ ○	dynamic
good	○ ○ ○ ○ ○ ○ ○	bad
problem	○ ○ ○ ○ ○ ○ ○	problem-free
hot	○ ○ ○ ○ ○ ○ ○	cold

Facebook

useful	○ ○ ○ ○ ○ ○ ○	useless
thick	○ ○ ○ ○ ○ ○ ○	thin
fast	○ ○ ○ ○ ○ ○ ○	slow
easy	○ ○ ○ ○ ○ ○ ○	complicated
strong	○ ○ ○ ○ ○ ○ ○	weak
active	○ ○ ○ ○ ○ ○ ○	passive
essential	○ ○ ○ ○ ○ ○ ○	superfluous
heavy	○ ○ ○ ○ ○ ○ ○	light
static	○ ○ ○ ○ ○ ○ ○	dynamic
good	○ ○ ○ ○ ○ ○ ○	bad
problem	○ ○ ○ ○ ○ ○ ○	problem-free
hot	○ ○ ○ ○ ○ ○ ○	cold

Uloz.to

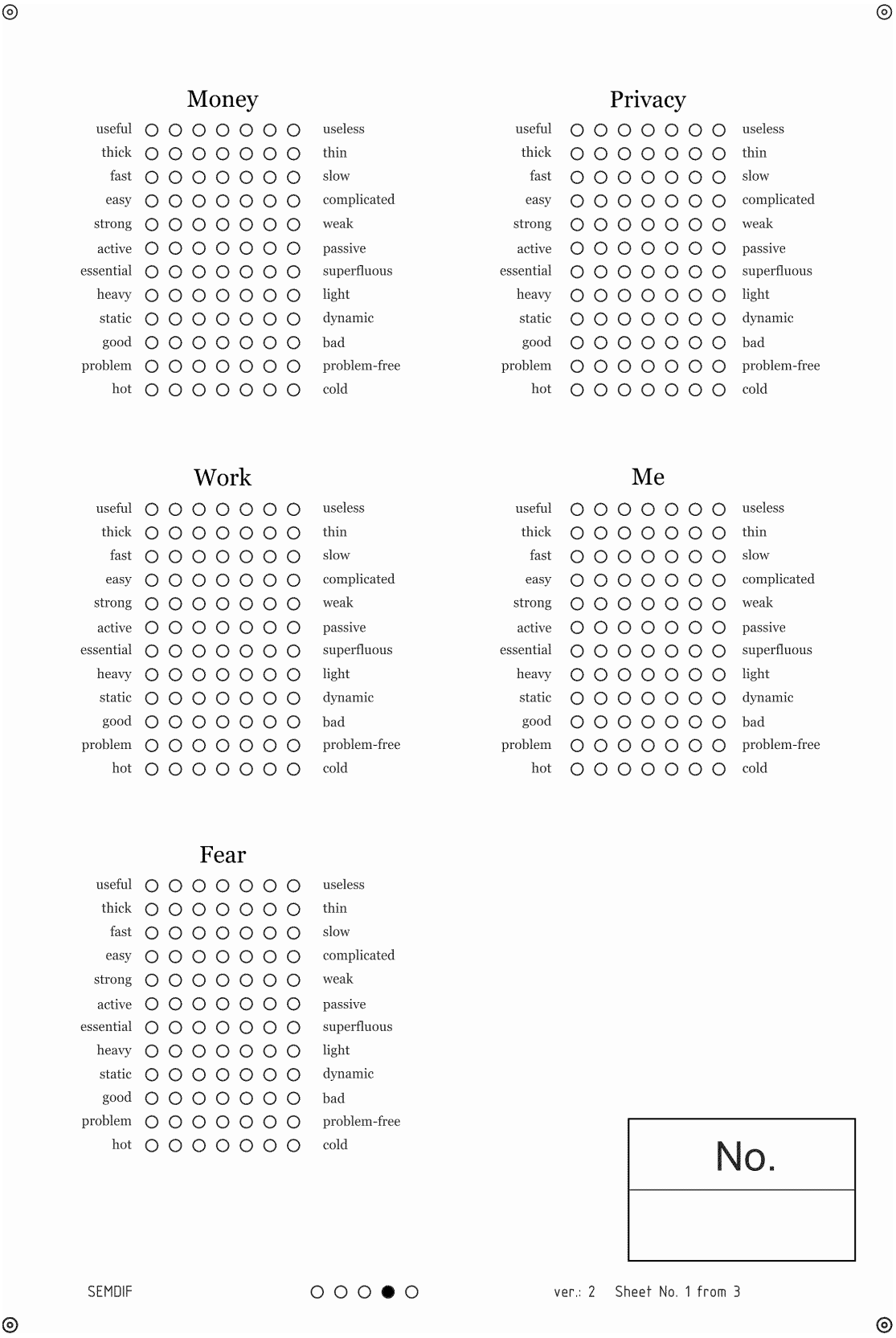
useful	○ ○ ○ ○ ○ ○ ○	useless
thick	○ ○ ○ ○ ○ ○ ○	thin
fast	○ ○ ○ ○ ○ ○ ○	slow
easy	○ ○ ○ ○ ○ ○ ○	complicated
strong	○ ○ ○ ○ ○ ○ ○	weak
active	○ ○ ○ ○ ○ ○ ○	passive
essential	○ ○ ○ ○ ○ ○ ○	superfluous
heavy	○ ○ ○ ○ ○ ○ ○	light
static	○ ○ ○ ○ ○ ○ ○	dynamic
good	○ ○ ○ ○ ○ ○ ○	bad
problem	○ ○ ○ ○ ○ ○ ○	problem-free
hot	○ ○ ○ ○ ○ ○ ○	cold

Email

useful	○ ○ ○ ○ ○ ○ ○	useless
thick	○ ○ ○ ○ ○ ○ ○	thin
fast	○ ○ ○ ○ ○ ○ ○	slow
easy	○ ○ ○ ○ ○ ○ ○	complicated
strong	○ ○ ○ ○ ○ ○ ○	weak
active	○ ○ ○ ○ ○ ○ ○	passive
essential	○ ○ ○ ○ ○ ○ ○	superfluous
heavy	○ ○ ○ ○ ○ ○ ○	light
static	○ ○ ○ ○ ○ ○ ○	dynamic
good	○ ○ ○ ○ ○ ○ ○	bad
problem	○ ○ ○ ○ ○ ○ ○	problem-free
hot	○ ○ ○ ○ ○ ○ ○	cold

No.

SEMDIF ○ ○ ○ ● ○ ver.: 2 Sheet No. 1 from 3



Money

useful	○ ○ ○ ○ ○ ○ ○	useless
thick	○ ○ ○ ○ ○ ○ ○	thin
fast	○ ○ ○ ○ ○ ○ ○	slow
easy	○ ○ ○ ○ ○ ○ ○	complicated
strong	○ ○ ○ ○ ○ ○ ○	weak
active	○ ○ ○ ○ ○ ○ ○	passive
essential	○ ○ ○ ○ ○ ○ ○	superfluous
heavy	○ ○ ○ ○ ○ ○ ○	light
static	○ ○ ○ ○ ○ ○ ○	dynamic
good	○ ○ ○ ○ ○ ○ ○	bad
problem	○ ○ ○ ○ ○ ○ ○	problem-free
hot	○ ○ ○ ○ ○ ○ ○	cold

Privacy

useful	○ ○ ○ ○ ○ ○ ○	useless
thick	○ ○ ○ ○ ○ ○ ○	thin
fast	○ ○ ○ ○ ○ ○ ○	slow
easy	○ ○ ○ ○ ○ ○ ○	complicated
strong	○ ○ ○ ○ ○ ○ ○	weak
active	○ ○ ○ ○ ○ ○ ○	passive
essential	○ ○ ○ ○ ○ ○ ○	superfluous
heavy	○ ○ ○ ○ ○ ○ ○	light
static	○ ○ ○ ○ ○ ○ ○	dynamic
good	○ ○ ○ ○ ○ ○ ○	bad
problem	○ ○ ○ ○ ○ ○ ○	problem-free
hot	○ ○ ○ ○ ○ ○ ○	cold

Work

useful	○ ○ ○ ○ ○ ○ ○	useless
thick	○ ○ ○ ○ ○ ○ ○	thin
fast	○ ○ ○ ○ ○ ○ ○	slow
easy	○ ○ ○ ○ ○ ○ ○	complicated
strong	○ ○ ○ ○ ○ ○ ○	weak
active	○ ○ ○ ○ ○ ○ ○	passive
essential	○ ○ ○ ○ ○ ○ ○	superfluous
heavy	○ ○ ○ ○ ○ ○ ○	light
static	○ ○ ○ ○ ○ ○ ○	dynamic
good	○ ○ ○ ○ ○ ○ ○	bad
problem	○ ○ ○ ○ ○ ○ ○	problem-free
hot	○ ○ ○ ○ ○ ○ ○	cold

Me

useful	○ ○ ○ ○ ○ ○ ○	useless
thick	○ ○ ○ ○ ○ ○ ○	thin
fast	○ ○ ○ ○ ○ ○ ○	slow
easy	○ ○ ○ ○ ○ ○ ○	complicated
strong	○ ○ ○ ○ ○ ○ ○	weak
active	○ ○ ○ ○ ○ ○ ○	passive
essential	○ ○ ○ ○ ○ ○ ○	superfluous
heavy	○ ○ ○ ○ ○ ○ ○	light
static	○ ○ ○ ○ ○ ○ ○	dynamic
good	○ ○ ○ ○ ○ ○ ○	bad
problem	○ ○ ○ ○ ○ ○ ○	problem-free
hot	○ ○ ○ ○ ○ ○ ○	cold

Fear

useful	○ ○ ○ ○ ○ ○ ○	useless
thick	○ ○ ○ ○ ○ ○ ○	thin
fast	○ ○ ○ ○ ○ ○ ○	slow
easy	○ ○ ○ ○ ○ ○ ○	complicated
strong	○ ○ ○ ○ ○ ○ ○	weak
active	○ ○ ○ ○ ○ ○ ○	passive
essential	○ ○ ○ ○ ○ ○ ○	superfluous
heavy	○ ○ ○ ○ ○ ○ ○	light
static	○ ○ ○ ○ ○ ○ ○	dynamic
good	○ ○ ○ ○ ○ ○ ○	bad
problem	○ ○ ○ ○ ○ ○ ○	problem-free
hot	○ ○ ○ ○ ○ ○ ○	cold

No.

SEMDIF ○ ○ ○ ● ○ ver.: 2 Sheet No. 1 from 3

BIOGRAPHIES

Václav Šimandl is an Assistant Professor at the Faculty of Education, University of South Bohemia in České Budějovice. His research activities focus on the area of teacher and pupil e-safety knowledge and routines and the delivery of e-safety lessons in ICT subjects.

Václav Dobiáš is a Ph. D. student at the Faculty of Education, University of South Bohemia in České Budějovice. His research activities concern the field of qualitative research of second level digital divide and strategies for solving computer problems.

Michal Šerý graduated in the Czech Technical University in Prague, Faculty of Electrical engineering, specialization Cybernetics and Robotics. His research interests lay in application of programming and control system in physics, biology and psychology.