International Journal of Management, Knowledge and Learning | ISSN 2232-5697

Peer Instruction as a Teaching Method in Cybersecurity and Data Privacy

Bettina Schneider
University of Applied Sciences and Arts Northwestern Switzerland FHNW
bettina.schneider@fhnw.ch

Petra M. Asprion
University of Applied Sciences and Arts Northwestern Switzerland FHNW
petra.asprion@fhnw.ch

Purpose/background: Cybersecurity and data privacy are important fields today. Basic education in these two interconnected areas should already be offered in schools, as practically everyone today can encounter the dangers and risks of the Internet regarding data theft, data manipulation or the like. However, cybersecurity and data privacy are generally abstract, and many people are not interested in such technical topics.

Study design/methodology/approach: To arouse interest and provide a certain basic education, we used 'peer instruction' combined with storytelling as a promising method to teach cybersecurity and data privacy. Within the framework of an EU project called GEIGER and with the support of students who have learned data privacy using the presented method, our specific peer instruction approach has been further developed, applied, tested, reflected, and iteratively improved.

Findings: The study shows that peer instruction in combination with storytelling is useful as teaching method in cybersecurity and data privacy. Especially the concept test questions encourage learners to engage with specific real-world situations. The study however revealed limitations of peer instruction in transforming facts into experiences.

Originality/value: In summary, the results presented are useful for cybersecurity and data privacy teaching, but the recommendations must be considered concerning careful preparation and testing.

Introduction

In today's world, and since the coronavirus pandemic has reached almost every country, digitisation is advancing rapidly. To remain competitive as a country, a digitally literate society is a key factor. The concept of 'digital literacy' – basic digital education − was defined by the European Commission years ago and extended with a low-threshold learning offer − a digital driver's license (European Commission, 2019).

Following current developments, cybersecurity is one of the predominant societal challenges. The annual Global Risk Report confirms that cyberwar and cybercrime are regarded as severe threats (World Economic Forum, 2021). Furthermore, cybersecurity is an important building block to ensure data privacy. The requirements for safeguarding digital privacy on the part of data-processing organisations have become significantly stricter in recent years. The European General Data Protection Regulation (EU GDPR), which unfolds extraterritorial effects, holds data controllers and processors accountable and imposes the burden of enormous fines in the event of violations (European Parliament, 2016).

Expanding on basic digital education, foundational knowledge of cybersecurity and data privacy should be among the educational goals of schools and universities. However, it is a challenging goal. Most concepts of cybersecurity and data privacy are somewhat abstract. For example, a cyberattack or data leak is not an imminently visible incident from an end user's viewpoint. Therefore, to teach the basics of cybersecurity or data privacy, the content must be

made experienceable (how it can be made tangible for end users?), and on the other hand, it must be made clear how the individual is affected (what has it got to do with me?).

Traditional teaching concepts alone are not sufficient in this context. One essential question has not yet been sufficiently answered: what new teaching approaches make the abstract concepts of cybersecurity and data privacy experienceable and simultaneously immersive so that one's own affectedness becomes clear?

Several future-oriented teaching/learning approaches exist, such as 'eduScrum' or 'flipped classroom'. In this study, the concept of 'peer instruction' is introduced and analysed in more detail. The objective is to investigate the applicability of peer instruction in the context of cybersecurity and data privacy. Furthermore, the authors aim to analyse the extent to which this learning approach supports the experiencability of data privacy concepts and fosters the learners' personal affectedness.

As a methodological approach, design science research (DSR) was followed (Hevner & Chatterjee, 2010). DSR draws upon existing knowledge from the knowledge base, such as the theoretical background of the peer instruction method. Another important pillar of DSR is the needs of the environment, the clear forum for the addressed stakeholders. For example, in this research context, data privacy and cybersecurity learners. As a core step, DSR leads to developing an artefact – in our case, an adapted learning approach – validated in the environment. The findings from the validation led to an improved research result.

The remainder of this paper is structured as follows. In the subsequent chapter, relevant basics of peer instruction are discussed. Next, the adapted learning approach, in combination with its application in practice, is shown. Reference is made to a current EU project called GEIGER[1]. This project is developing an educational ecosystem to protect European micro-enterprises from cyberattacks and help them comply with applicable data protection laws. The Horizon 2020 project is coordinated by the University of Applied Sciences and Arts Northwestern Switzerland FHNW. As a result of evaluating the learning artefact, it is analysed to what extent the peer instruction concept fulfils the following two criteria: a) enabling an experience and b) causing personal affectedness. Finally, a conclusion is drawn.

Peer Instruction

Foundations

The teaching/learning method of peer instruction is well described in Mazur (2017). This section refers to this source. Peer instruction aims to teach a topic area's basic concepts while emphasising practical exercises. Thus, the method is designed to lay and reinforce conceptual foundations. The approach builds on learning materials being worked through before educational lectures. During the classes, the time is used to introduce the core concepts and point out possible difficulties briefly. The learning material is enriched with the help of examples and tasks.

The focus lies on the so-called 'concept test question' (CTQ), intended to stimulate the active participation of the learners. It is a multiple choice (MC) question, which is worked on directly after a core concept has been theoretically discussed. Each learner is provided with a timeframe to think about the correct answer. This is followed by the essential phase of peer instruction: the discussion among learners. The interactive team discussions help to achieve the desired deepening of the learning material because each person is engaged to formulate and justify their understanding. After the discussion, the teacher collects answers, feedback, and conclusions

[1] https://project.cyber-geiger.eu

from the learners' interactions. For example, the following core concept can be introduced if the teacher concludes that the topic was understood correctly. If the overall level of understanding is insufficient, further explanations and a second CTQ follow. Table 1 shows a sample structure for incorporating the QTQs into the lessons (as suggested by Mazur, 2017).

Table 1: Scheme for the use of concept test questions (CTQs) adapted from Mazur (2017)

Description	Allocated Time
1. Introduction of the question	1 minute
2. Time for students to reflect	1 minute
3. Noting the individual answer (optional)	
4. Convince-your-neighbour discussion (peer instruction)	1-2 minutes
5. Noting the - possibly - revised second answer (optional)	
6. Feedback on the answers to the teacher and documentation	
7. Explanations of the correct answer	2+ minutes

The quality of questions is an important success factor of the peer instruction method. Therefore, it is recommended to follow Bauer (2018), who has developed an iterative procedure for creating CTQs.

Application of the Peer Instruction Method

One of the research results of the EU project GEIGER is a low-threshold learning offer for non-experts to build up basic data privacy knowledge. In particular, the project aims to help owners and employees of micro-enterprises to understand the EU GDPR better so that they can implement or comply with the regulatory requirements. To make the learning offer attractive for the target group, it should take little time and contain playful elements to help learners understand the 'unattractive' context in a playful way.

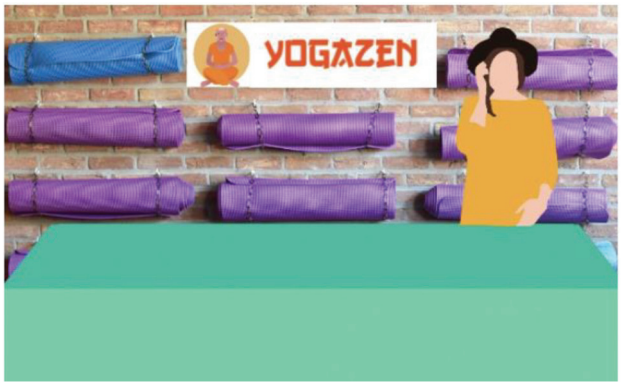
Before concrete learning content could be created, it was necessary to analyse which theoretical concepts should be part of a basic data protection education for micro-enterprises. In the GEIGER context, the following core concepts were chosen: 1.) personal data, 2.) applicability of the GDPR, and 3.) data subject rights (Schneider et al., 2020).

In the first version, an MC-question quiz has been developed and implemented in the Moodle open-source learning platform. In addition, storytelling has been applied to ensure that the quiz questions had the necessary relevance for the players. Storytelling can be defined as the ability to tell stories in a way that is relevant to the audience by describing a flow of events that takes place in time and space. The purpose of telling a story is to engage and emotionally captivate the audience (Lugmayr et al., 2017).

For the GEIGER project, the stories have been transferred to the context of micro-enterprises, for example, a small yoga studio or a hairdresser's shop. Three sequential stories were developed for each of the core concepts. Figure 1 shows an example of Mary, an entrepreneur, and her client Frederick. The story revolves around the first core concept – the definition of personal data.

A few weeks later, Friedrich returns to the store to buy a new set of yoga mats. When it is time to pay, Mary remembers that he did not yet complete the form and asks again if he could finish. Friedrich responds that he does not like spam and prefers not to. Then, Mary explains that she will only send out birthday promotion emails. Friedrich likes this idea and fills out all fields: name, date of birth, e-mail, car licence plate number & background on physical limitations.

What "categories" of personal data did Friedrich reveal?



- a. Data concerning health
- b. Biometrics
- c. Identifier
- d. Genetic data

Check

Art. 4
Name, date of birth, e-mail: 'normal' personal data; Lincence plate number: This is an identifier;Background on physical limitations: This is 'data concerning health' and hence regarded as 'special category of personal data'

The correct answers are:
Identifier,
Data concerning health

Figure 1: Sample story (top part) with possible answers and solution explanation (bottom part) enhanced from Schneider et al. (2020)

The stories have been evaluated as part of a master's lecture with business informatics students (around 40 students). The learners suited the target group of the GEIGER project – non-experts from small enterprises – as the master program is a part-time study program. Moreover, as 99% of the companies in Switzerland are small or medium-sized (Federal Statistics Office, 2019), many working students show experience in these environments.

Following the peer instruction method, a short input on data privacy and basic concepts was given. After that, the quiz started. The questions were not read aloud; instead, the learners could read the stories on Moodle at their own pace (top part in figure 1), think about them, and choose the answer options of the corresponding MC question (bottom left in figure 1). Deviating from the theory of the CTQ (see table 1), it was not intended that a peer instruction round takes place after each question. Instead, groups of questions were clustered. The learning system Moodle was configured in such a way that after submitting the answers, an evaluation and feedback on the correct solution were displayed to the learners (bottom right in figure 1). On completion of the quiz, a plenary reflection round took place.

The peer instruction method resulted in mixed feedback during the first test phase. The stories and the interactive quiz were evaluated positively and led to a lively discussion. However, there were some points of improvement. First, the time available was estimated too optimistically. A discussion (in the team) and reflection (in the plenum) could not be realised within 1-2 minutes each. In addition, students progressed at very different paces. While some were bored, others had to be interrupted in their thinking process.

Furthermore, three stories were provided for each of the three selected theoretical concepts. Based on the Moodle evaluation, it became clear that some participants experienced this too long and did not fully utilise the learning offer. On average, the participants spent 8 minutes on the quiz, whereas one-fifth of the learner dropped out after 3 minutes of playing time (rounded).

Analysis

In this chapter, the peer instruction concept is assessed concerning the criteria of personal affectedness and experientiality. This analysis − in addition to the experience gained from a practical application − is intended to enable an assessment of the extent to which peer instruction is suitable for teaching cybersecurity and data privacy concepts.

Personal Affectedness

It is not immediately apparent to what extent the topic affects the individual in cybersecurity and data privacy. This may seem illogical, as reports of cyberattacks and their consequences dominate the media. However, among the target group of micro-enterprises, there is a persistent misconception that they are too irrelevant for anyone to care about their own data. Therefore, people believe or hope they will not be affected themselves (Schneider, 2018).

The concept of peer instruction, particularly the CTQ, encourages learners to engage with specific questions and possible answers. While the CTQ does not need to elicit personal involvement, the link to the storytelling approach is promising. The stories introduce data privacy problems at companies with comparable conditions. Ideally, learners can put themselves in the situation and relate the use case to their own company. This way, an understanding of how they are affected is built up. The interactive exchange in the team and the plenum opens the space to exchange viewpoints − matching the story.

Experiencability

A capacity for abstraction is necessary to grasp the digital world (Allmann & Blank, 2021). Therefore, it is important to develop teaching methods to make invisible effects tangible to a dedicated target group.

The peer instruction method has limitations when transforming facts into experiences. For example, the CTQ, in combination with storytelling, makes it possible to talk about third-party experiences in the context of a short story. This can be quite immersive but does not generate a ‘first-hand’ experience. One possibility would be to link the CTQ with an experiment or a small work instruction so that own actions are enforced. Such an extension would be conceivable under good guidance, provided sufficient time is allotted.

Another option might be to incorporate the CTQ into a larger context. Instead of referring to an individual, separate stories, a game world could be provided. As a concrete example, within the framework of the GEIGER project, a virtual ‘cybersecurity escape room’ was developed. In the escape room, participants are supposed to track down a hacker. This escape room could be played in class and supplemented with CTQ. However, there are arguments against it: first, the learning scenario and the classroom setting are becoming increasingly complex; this could lead to overload for teachers and learners. Second, the strength of a virtual game is that learners are immersed in the game world. Continuous interruption by peer instruction would potentially disrupt the flow of the game. Third, a fundamental principle of escape rooms is that a task must be solved quickly. The CTQ would hence either dissolve this principle or lead to a conflict. An intensive discussion in the team would counter the chance of winning, namely finishing the game in the shortest possible time.

Conclusion

Even though the conducted analysis does not allow a final assessment of the peer instruction concept, valuable conclusions could be drawn. It has been shown that − especially in combination with storytelling − a personal affectedness can be created. The relevance of basic concepts can be brought closer to the learners. Direct experience is not made possible by the method or the CTQ per se. Based on the stories, the experiences of third parties are presented. However, an extension of the peer instruction method would be possible under certain conditions.

In conclusion, by applying the method in a master course, the following lessons could be learned: peer instruction needs sufficient time and preparation. The theoretical concepts must be well chosen in advance, and the short lectures and the questions must be thoroughly prepared and tested in advance in a feedback-capable context. The dosage of the peer instruction method is considered necessary, i.e., a few selected concepts and questions can provide added value. For example, three concepts with nine questions in four hours of instruction were regarded as too extensive − attention decreased over time. On the other hand, the implementation of MC questions via the learning platform Moodle was considered very positive. It is easy to use, allows automated feedback, and provides transparency to the teacher about progress.

Overall, applying the peer instruction method for data privacy training in small enterprises could be recommended. Care should be given to selecting the stories, which need to be clearly aligned to the properties and needs of the respective organisation. As a desire for further development, the company name, related location information and related branding should be customisable to create stories representing the learner's situation in their small business as closely as possible. This measure is expected to increase immersion, which would need to be evaluated in a future educational research project.

Acknowledgements

This work was made possible with funding from the European Union's Horizon 2020 research and innovation programme under a grant agreement No. 883588 (GEIGER). However, the opinions expressed, and arguments employed herein do not necessarily reflect the official views of the funding body.

References

Allmann, K., & Blank, G. (2021). Rethinking digital skills in the era of compulsory computing: methods, measurement, policy and theory. Information, Communication & Society, 24(5), 633-648.

Bauer, T. (2018). Design von Aufgaben für Peer Instruction zum Einsatz in Übungsgruppen zur Analysis. In Hanse-Kolloquium zur Hochschuldidaktik, 63-74.

European Commission (2019). The Digital Competence Framework 2.0. https://ec.europa.eu/jrc/en/digcomp/digital-competence-framework

European Parliament (2016). Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung). https://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1554130655357&uri=CELEX:32016R0679

Federal Statistics Office (2019). Kleine und mittlere Unternehmen. https://www.bfs.admin.ch/bfs/de/home/statistiken/industrie-dienstleistungen/unternehmen-beschaeftigte/wirtschaftsstruktur-unternehmen/kmu.html

Hevner, A., & Chatterjee, S. (2010). Design science research in information systems. In Design research in information systems (pp. 9-22). Springer, Boston, MA.

Lugmayr, A., Sutinen, E., Suhonen, J., Sedano, C. I., Hlavacs, H., & Montero, C. S. (2017). Serious storytelling–a first definition and review. Multimedia tools and applications, 76(14), 15707-15733.

Mazur, E. (2017). Peer instruction. In Peer instruction. Springer Spektrum, Berlin, Heidelberg, 9-19.

Schneider, B. (2018, June): Nobody is interested in my data anyway – the impact of GDPR on industry 4.0. Presentation at a trinational Conference 'Fundamentals, Current Trends, Future Industry 4.0', Villingen-Schwenningen, Germany.

Schneider, B., Bontempo, N., Asprion, P.M. & Habbabeh A. (2020): Storytelling and Gamification in E-Learning – An Empirical Study to Educate Swiss Microenterprises in Data Protection. In: Dermol, V. (Ed.): Expanding Horizons: Business, Management and Technology for Better Society. Proceedings of the MakeLearn and TIIM International Conference 20–22 May 2020, Virtual. Bankok, Celje, Lublin: ToKnowPress, 319-328. http://www.toknowpress.net/ISBN/978-961-6914-26-0.pdf

World Economic Forum (2021). The Global Risks Report 2021. https://www.weforum.org/reports/the-global-risks-report-2021