10-9-2023

Decide wisely: Interactive videos as appealing educational element to attract students to information security

Martin Brehmer
Faculty of Business and Economics, University of Augsburg, Germany, martin.brehmer@uni-a.de

Decide wisely: Interactive videos as appealing educational element to attract students to information security

Research Paper

Martin Brehmer[1]

[1]University of Augsburg, Faculty of Business and Economics, Augsburg, Germany
martin.brehmer@uni-a.de

Abstract. Educational videos play an important role in university education. However, they are often not designed to foster active learning and the learning process is not immersive. Interactive digital storytelling is a promising game design element but requires a rigorous evaluation to avoid negative side effects. Therefore, we adopt a design science research approach to design and evaluate an interactive video that includes interactive storytelling and real-world recordings. The proposed artifact aims to raise information security awareness among bachelor students at a German university for malicious USB sticks and the reporting of incidents. In our evaluation, we focus on learning progress before and after using the video as well as qualitative feedback about the experience with the learning object. Our results show that videos that are based on interactive choice-based storytelling can foster an active and immersive process, and significant learning outcomes.

Keywords: interactive video, interactive digital storytelling, information security, awareness, university

1 Introduction and problem motivation

Although videos are hardly indispensable in today's university education, designing effective educational videos is still a major challenge because inappropriate video designs can decrease students' motivation to watch and lead to comprehension problems, or students perceive videos as stressors, monotonous and thus, not engaging and boring (Beheshti et al., 2018; Chouhan, 2021; Croasdell et al., 2018; Wang, 2022). Hence, it is crucial that the design of the video supports active learning, e.g., by using game design elements, such as a narrative and including interaction opportunities (Beheshti et al., 2018; Chouhan, 2021; Wang, 2022). Thereby, appropriate gamification fosters motivating, interactive, and immersive learning environments and the achievement of learning goals (Deterding et al., 2011; Hamari et al., 2014). Conversely, inappropriate gamification can imply negative effects, such as not reaching the learning goals or fostering feelings of aversion and boredom (Almeida et al., 2021). Thus, current research calls for rigorous evaluations of gamified approaches, such as an interactive video that relies on interactive digital storytelling. In particular, the evaluation should include whether learning outcomes are reached and, in addition, discuss motivational aspects regarding the learners‘ engagement with the system. (Chen et al., 2018; Hamari et al., 2014; Melcer et al., 2020) This article aims to address this gap by evaluating a novel instance of an interactive educational video that aims to build information security awareness (ISA) among university students. Therefore, we answer the following research questions in the following chapters by applying a mixed-method approach:

> ***RQ1:*** *To what extent does the level of information security awareness change after using an educational video which includes interactive digital storytelling?*
>
> ***RQ2:*** *What are crucial design factors of the learning object that should be improved or remain within future design cycles?*

We focus on students' ISA because they represent a great share of IT users at universities where, security awareness is often low (Ulven and Wangen, 2021). Furthermore, security education is still ineffective, often perceived as burdensome, and demotivating (D'Arcy et al., 2014; Hu et al., 2021). Universities also face a high number of severe cyberattacks that, e.g., threaten human life, put down IT infrastructure, and lead to leaks of confidential data (Knop, 2023; Martin, 2023; Ralston, 2021). Thus, we strive to design an interactive educational video that suits user preferences in security education (Abawajy, 2014), overcomes some limitations of non-interactive videos, and is based on a scalable delivery method (Croasdell et al., 2018; Rajadell and Garriga-Garzón, 2017). Furthermore, our research aims to contribute to current research streams as a complement for realistic security education interventions by leveraging the effects of interactive storytelling and immersive user experience (Fertig et al., 2022; Ulsamer et al., 2021). We chose 'reporting of security incidents' in combination with 'malicious USB sticks', named bad USB sticks, as a learning subject because they are an often-neglected tremendous threat to universities' information security. For instance, many end user are not aware how to report security incidents at universities (Ulven and Wangen, 2021). Tischer et al. (2016) further reveal that deployed and prepared USB sticks have been merely reported but picked up and plugged in by finders in up to 98%. Recently, the FBI also warned that bad USB sticks are now being used to spread ransomware (Tung, 2022). Thus, there is a need for educating and raising ISA for bad USB sticks and the reporting of incidents effectively for universities. This article is part of a larger design science research project that follows the Design Science Research Methodology (Peffers et al., 2007). The overarching goal is to develop innovative and effective educational approaches using information systems, e.g., a learning management system (LMS) as well as game design elements, to increase the level of ISA. Thereby, this article represents an additional design cycle that builds on our previous research in improving security education (Brehmer et al., 2021), in particular analyzing the effect of gamification on learning outcomes, e.g., by implementing a narrative (Brehmer and Reinelt, 2023). Thus, we apply a within-subjects design to overcome our previous limitations whether a gamified learning object (LO) is able to foster learning progress. We focus on developing and evaluating another novel artifact, which is an interactive video with real-world scenarios and an underlying choice-based narrative. We outline the problem motivation for this article in this chapter. Within the next chapter, we depict the theoretical knowledge base that influenced our design decisions. The contribution of this artifact will be evaluated in chapter 4 by following Venable et al. (2012), proving its utility and purpose, identifying weaknesses and areas of improvement, but also outlining negative side effects. With this, we contribute to existing design science research by following the suggestion of Nguyen and Pham (2020) to contribute to research by a) extending the pedagogical body of knowledge for security education in regard to building ISA, and b) sharing insights about an empirically proven effective artifact.

2 Knowledge base and related work

Linking interactions with information systems and storytelling is known as ***interactive digital storytelling***. Thereby, a player is able to influence a storyline (Murray, 2018) by making meaningful choices through interactions with an information system (Melcer et al., 2020). Furthermore, Murray (2018) depicts interactive digital storytelling as a rapid evolving field of both, research (e.g., see the annual *'International Conference on Interactive Digital Storytelling'*) and university education that includes several decades of research knowledge to date and multiple facets of representations, e.g., **interactive videos**, games, simulations and augmented reality approaches. Within the context of interactive educational videos, digital storytelling offers several pedagogical advantages (Baldwin and Ching, 2017; Shelton et al., 2016): E.g., it promotes learning by conveying complex topics through rich information streams. But it also connects students emotionally with the learning content or enables them to check their understanding while navigating through the story of the video. This supports students in active learning as it increases, e.g., curiosity and flow within the learning process. Thus, interactive storytelling is discussed among many educational fields, e.g. history, STEM and ethics (Grasse, Kreminski et al., 2022). Current literature connect educational interactive storytelling to the ***self-determination theory*** of Ryan and Deci (2000) and highlight that intrinsic motivation is a crucial factor for achieving learning outcomes, that should be addressed by fostering the feeling of autonomy and competence within the learning process, but also immersion and relatedness, e.g., by implementing real-world scenarios (Grasse, Kreminski et al., 2022; Grasse, Melcer et al., 2022). In turn, role play and narratives are game design elements that support the feeling of relatedness: They address intrinsic as well as extrinsic motivational preferences by creating a state of flow, which is a 'highly focused psychological state of mind, where an individual experiences high enjoyment and is intrinsically motivated while executing any specific and even difficult task at hand', according to the ***theory of flow*** (Brehmer and Reinelt, 2023; Csikszentmihalyi, 1990; Deci and Ryan, 2000; Grasse, Kreminski et al., 2022). Thus, within the context of effective ISA trainings, branching narratives that include role play, e.g., based on "choose your own adventure" approaches are promising, as they combine the concept of interactivity with storytelling as a game design element (Dincelli and Chengalur-Smith, 2020). Nevertheless, the literature review that we have conducted using the term *"(security-education OR information-security-awareness-training OR cyber-security-awareness-training OR "SETA") AND (storytelling OR narrative OR choose-your-own-adventure OR video) AND (interactiv* OR immersive)"* (data fields: Abstract, Title; excluded articles contain full video games and lacked a narrative) in the databases of AISeL, IEEE Xplore, and WebOfScience only provided two articles. These articles show that educational videos can support to change attitudes and behavior related to individual ISA through realistic immersive scenarios (Dincelli and Chengalur-Smith, 2020; Ulsamer et al., 2021). Thus, interactive choice-based storytelling within videos further addresses known ***success factors for security education and training awareness programs*** to a great extent namely, e.g.: a) applying gamification and using rich media, b) providing immersive learning content which supports autonomy in the learning process for a specific target group, c) provide feedback through the opportunity of choices and their consequences (Alyami et al., 2022; Brehmer et al., 2021; Hu et al., 2021; Kirova and Baumöl, 2018; Yoo et al., 2018). From the perspective of educational practice, gamification is already reported to work well with students (Hamari et al., 2014). In conclusion, interactive digital storytelling is promising as it enables the experience of realistic training through game play, e.g., including simulated real-world decision situations.

However, as previously mentioned, meaningful learning content is crucial. Thus, we utilize the ***Human Aspects of Information Security Questionnaire (HAIS-Q)*** from Parsons et al. (2017) as a guideline for content details. This questionnaire is well accepted and validated (McCormac et al., 2016). It is also consistent with standards, e.g., NIST SP 800-50 (Wilson and Hash, 2003). The questionnaire is furthermore a useful tool to measure the level of individual ***information security awareness (ISA)*** among varying contexts (Parsons et al., 2014; Wahyudiwan et al., 2017) as well as assessing ISA among students (Salem et al., 2021). Here, ISA is a representation of someone's knowledge about security procedures (dos and don´ts) for specific focus areas, e.g., 'incident reporting', but also the attitude towards following common standards or compliance guidelines, and in addition, the actual behavior of the person (Parsons et al., 2017). Aligning the educational video according to the HAIS-Q facilitates a rigorous evaluation of specific learning outcomes, which also addresses current calls for research (see chapter 1). Thus, the HAIS-Q serves as prescriptive theoretical design knowledge for our approach as well as evaluation methodology. However, the HAIS-Q lacks the opportunity for important qualitative feedback regarding the design of the LO itself, such as user experience and perceived usefulness for learning. The interactive video presented in the following section can be considered as a LO that will be qualitatively evaluated (see chapter 4). In this context, a learning object is an "interactive web-based tool[s] that support[s] the learning of specific concepts" (Kay and Knaack, 2009).

3 Designing the artifact – an interactive choice-based video

The overall theme of our interactive video is – how to deal with USB sticks which are found on the university campus and how to report threats and incidents. We used items of the HAIS-Q (Parsons et al., 2017) as the theoretical basis for developing the learning content, included focus areas are 'Incident Reporting' and 'Information Handling' (only subarea inserting removable media). In order to ensure scalability in terms of sharing the video with other faculties or universities, we used the H5P-software framework and created an 'interactive video' (see https://h5p.org/interactive-video), because H5P-modules can be integrated into some LMS, such as Moodle or to some extent in

Stud.IP-based systems. We uploaded only one video that contains jump labels, to head from decisions to the next video scene. The video was recorded on the university campus and to make the video as realistic looking and immersive as possible we recorded video material in a first-person perspective. One full-time employee and 3 part-time employees were necessary to play the roles and create the video. The storyline and decision options have been documented using a process diagram to ensure transferability for later projects and independence from technology. The narrative starts with, that the student (protagonist, first-person view) is receiving an e-mail with instructions to go to university and once there, he is finding a USB stick (labeled with "contracts") and having to decide within multiple decision situations how to deal with the stick and upcoming situations. Afterward, the student has to deal with the decision, of whether or not to report that he plugged in the stick, or in case he makes a different decision beforehand (represents another decision path), whether or not to report that fellow students found USB sticks but did not report them. In the end, the decisions lead to the scenario that the university gets hacked (try again) or the cyberattack can be averted. Further design details can be found in the following table (or see Brehmer (2023)).

Table 1. characteristics of the developed interactive video

Shortest / longest possible walk-through / video material in total:	10:12 min** / 18:09 min** / 28:08 min (**w/o time for decision-making)
Possible decision situations and options:	
- minimum 5, maximum 9 decision situations (unnecessary repetitions excluded)	
- minimum 11 decision options in total (without repetitions – shortest walk-through) up to 18 decision options (longest walkthrough due to forced repetitions as result of bad decisions (unnecessary repetitions excluded))	
Basic design considerations:	
1. repetitions are possible to support learning, 2. wrong decisions lead to learning scenarios, 3. use humor and reward good behavior, 4. use Memes and realistic scenarios to attract the target group, covering possible real-world circumstances (closed IT-Department)	

4 Evaluation of the artifact

4.1 Evaluation procedure and sample description

The sample for the quantitative evaluation consists of **n=60** completed surveys from **13 female and 47 male bachelor students** at a university in Germany (invalid surveys are excluded, e.g., incomplete datasets). The majors of these students vary. Most participants are business information systems engineering students (n=29), followed by students of industrial engineering (n=25), students of business administration (n=5), and 1 student of computer science. Since the purpose of the LO is to be reused in different courses, we analyze all fields of study as one group. The structure of the survey is depicted in Table 2 and will be described in the following. In order to ensure that our results are meaningful for educators who want to address different target groups, such as freshman students as well as students in advanced semesters, we collected data

Table 2. structure of the surveys

	Description	No. of items (w/o demographic items)
1st survey:	HAIS-Q quant. pretest (n=60)	9
2nd survey:	HAIS-Q quant. posttest (n=60)	9
	LOES-S – qual. questions (n=60)	2
	Control Measure (n=60)	4

within a first-semester lecture and a seminar which is suggested for students of the fifth semester. The student's recent semester of study is described by the following distribution: 1st-, 2nd-, and 3rd-semester students (n=38), 5th- and 6th-semester students (n=15), 7th-semester students and above (n=7). All data has been collected in one week to reduce the risk of bias. **The sample size for the qualitative evaluation** is consistent with the pretest (n=60). We introduced our survey as part of our research namely an "evaluation of a digital educational element for teaching at universities". Participation in the study was voluntary. To ensure that the results of the pre- and posttest can be linked, students were asked to create a unique but anonymous code (based on assembled letters) which is only used for this purpose.

Assessing the extent to which an educational design element is successful is essential and desirable design knowledge for educators and researchers, which we aim to derive by answering RQ1. Thus, we evaluate the learning goal of this educational approach which is to raise ISA for the handling of unknown and potentially harmful USB sticks and reporting security incidents by students. We applied the HAIS-Q of Parsons et al. (2017) as a quantitative measure to determine the level of ISA (see chapter 2) and whether the interactive video affects learning outcomes. For reproducibility and transparency, we point out that we use five points of the Likert scale, following the initial HAIS-Q developers (e.g., Parsons et al. (2017) and McCormac et al. (2016)), instead of applying a four points of Likert scale (e.g., like Cindana and Ruldeviyani (2018)).

Beyond measuring learning outcomes, it is essential to know the design factors that influenced these learning outcomes. Thus, in order to answer RQ2, we evaluate the feedback of students. With this in mind, we include the two qualitative questions of the "Learning Object Evaluation Scale for Students"-questionnaire (LOES-S) of Kay and Knaack (2009) in our survey because these questions offer the opportunity for students to give qualitative feedback for a specific LO and provide design knowledge for further improvements - the applied questions are: *1. What, if anything, did you LIKE about the learning object? 2. What, if anything, did you NOT LIKE about the learning object?* To analyze all answers for our LO, we use the 3 applicable categories ('Learning', 'Engagement', 'Quality') of the coding schema provided by Kay and Knaack (2009) with the slight adaption of the subcategories to align it to the format of an interactive video. The applied subcategories are presented and discussed with regard to the results in chapter 4.4. In addition to the two LOES-S items, we ask the students as a control measure of our qualitative feedback, if they "would recommend this information security training to [their] fellow students" using a 10-point scale and further, if they "would participate again in an information security training that uses interactive video formats like this training". Both questions include an input field for explanations. The purpose of the control measure is further outlined in the following chapter.

4.2 Methodology for evaluating learning outcomes and qualitative feedback

Table 3. Reliability testing using Cronbach's' Alpha (9 items)

Sample	HAIS-Q constructs(Parsons et al., 2017)	Cronbach's α
HAIS-Q pretest (n=60)	Focus area: incident reporting (9 items)	.801 (satisfying)
HAIS-Q posttest (n=60)	Focus area: incident reporting (9 items)	.712 (satisfying)
HAIS-Q pretest (n=60)	Focus area: information handling → sub-area: inserting removable media (3 items)	.299 (insufficient, excluded*)
HAIS-Q posttest (n=60)	Focus area: information handling → sub-area: inserting removable media (3 items)	.488 (insufficient, excluded*)

* because alpha is substantially lower than acceptable values such as α = <.7 (Taber, 2018)

Our dataset includes a **pre- and posttest**, which is essential to determine whether the interactive video fulfills its purpose in reaching the learning goal (an increased level of ISA). To assess this and **answer RQ1,** we compare these tests and use the t-test for dependent samples. Initially, we assess the reliability of our measured HAIS-Q constructs, this means we calculate Cronbach's Alpha for the HAIS-Q focus area 'incident reporting' and one subarea from the focus area 'information handling', which is 'inserting removable media'. The internal consistency of the focus area 'incident reporting' is reliable for both, the pretest with **α=.801** and the posttest with **α=.712**. However, Cronbach's alpha for the subarea 'inserting removable media' is insufficient. In consequence, we exclude this subarea from the analysis. To compare the pre- and posttest we apply the t-test of dependent samples and calculated the effect size using the method of Cohen's d (see next chapter). Given the robustness of the t-test for n>30, we do not check for normal distribution. We checked the dataset for outliers but found none. Furthermore, we analyzed the pretest data, in particular the mean values of the constructs to see if there were differences in students' prior knowledge between lower (1-3) and higher (5-7) semester groups, but these differences were not significant.

The learning content was designed according to the HAIS-Q focus area 'incident reporting' and one subarea from the focus area 'information handling'. Therefore, we also use the corresponding HAIS-Q items of the focus area 'incident reporting' to measure learning outcomes, but without the items of 'information handling' (see Table 3). 'Incident reporting' consists out of 3 subareas with 3 items each (one item per dimension: knowledge, attitude, behavior). In conclusion, we used 9 items in total with a 5-point Likert scale ranging from '1 – strongly disagree' to '5 – strongly agree' and recoded reversely scored items. The level of ISA is a result of mean values and to measure this, we 1.) calculate the mean value of each subarea by summing up the mean values of each subarea item score (minimum 3 – maximum 15 points), then, 2.) we calculate the mean value for the (overall) subarea score (minimum 1 – maximum 5 points) to perform the t-test and 3.) discuss the scores from 1) and 2) as a measured representation of the level of ISA in chapter 4.4. We are aware of literature that suggests applying weightings to the dimensions (knowledge, attitude, behavior) of the HAIS-Q focus areas (e.g., Cindana and Ruldeviyani (2018) or Firsty Arisya et al. (2020)). However, in order to increase transferability, we decided to weight all dimensions equally, which is also common practice (e.g., see Wahyudiwan et al. (2017) or Salem et al. (2021)). To determine whether the ISA score of an HAIS-Q subarea or HAIS-Q focus area is sufficient, average, or alarming and requires action (here: further educational interventions), we follow the current literature, e.g. Wahyudiwan et al. (2017) or Firsty Arisya et al. (2020), and use the following categorization (but without weighting): good awareness (80-100% of all possible points per subarea (=12-15 points)), average awareness (60-79% of all points), poor awareness (<60% of all points). In order to evaluate the **qualitative user feedback on the LO** and to derive **design factors to answer RQ 2**, we analyze first, all provided qualitative statements for the LOES-S items, but also second, the control measure items. More details about the evaluation procedure are outlined in the previous chapter 4.1. Here, we refer to this procedure and add information about how we derive findings. First, the posttest data set (n=60), including the two qualitative LOES-S items, provide statements about positive and negative design factors that are categorized by applying our adopted coding framework from Kay and Knaack (2009). This means that statements are assigned to the framework (sub-)categories and numbered in cases where the meanings of provided statements are similar. Second, the same dataset contains students' responses to the four further items of the control measure, these are 2 quantitative items and 2 qualitative items. It is known that collecting qualitative data is likely to be influenced by interfering factors like social desirability (Crowne and Marlowe, 1960). Thus, the quantitative items and qualitative items of the control measure are included as an indicator for social desirability and thus, provide indications regarding the reliability and validity of the findings (Crowne and Marlowe, 1960) that are based on the LOES-S items. In other words, we assume that not every student would recommend our educational approach without restrictions. Thus, we would further assume a high likeliness that our findings are influenced by social desirability if the statements of respondents are contradictory or almost every student would fully "recommend this information security training to fellow students" and in case almost every student "would participate again in an information security training that uses interactive video formats like this training". In other words, our findings would be questionable if our approach is evaluated as "perfect". In consequence, we review the dataset for contradictory statements and outliers.

4.3 Results

The result of our t-test for dependent samples is calculated by the mean values of each subarea before and after treatment and indicates that our interactive video (see Table 4) **significantly** increases the level of ISA for the subarea 'Reporting suspicious behavior (RSB)' t(59)=-2.616, p=.011*, d=.81. In addition, the video **significantly** increases the level of ISA for the subarea 'Ignoring poor security behavior by col. (IPSBC)' t(59)=-3.096, p=.003**, d=.99, furthermore, it **significantly** increases the level of ISA for the subarea 'Reporting all incidents (RAI)' t(59)=-2.109, p=.039*, d=.98. Based on this data we can interpret, that the interactive video has a significant effect on increasing the level of ISA for all three subareas of the HAIS-Q focus area 'incident reporting' if used in a university lecture for bachelor students. After screening all qualitative statements, we found 59 statements (n=60; one blank answer excluded) that refer to what

Table 4. results of comparing the HAIS-Q pre- and posttest (dependent t-test, Cohen's d)

Subareas of focus area: incident reporting	**Level of ISA (mean values; n=60)**		**t-test (df=59; *p < .05; **p < .01)**	
	pre- vs. posttest	**SD/Dif.**	**t; p*/p****	**Cohen's d**
Reporting suspicious behavior (RSB)	4,2778 (pretest)	.80603/ -.27222	-2.616; **.011***	**.81**
	4,5500 (posttest)			
Ignoring poor security behavior by col. (IPSBC)	3,8667 (pretest)	.98671/ -.39444	-3.096; **.003****	**.99**
	4,2611 (posttest)			
Reporting all incidents (RAI)	4,1778 (pretest)	.97964/ -.26667	-2.109; **.039***	**.98**
	4,444 (posttest)			

they LIKE about the LO and 34 comments on what they did NOT LIKE. Here, it is noteworthy, that 6 students gave further positive feedback answering the "NOT LIKE" question and thus, these parts of the statements are reframed as "LIKE" statements. For instance, one student answered the "NOT LIKE" question by stating "Even the option to replay was good to find different outcomes of the Story" and thus, the statement is obviously positive instead of negative. Within the further analysis, we excluded individual indifferent and inaccurate answers like "all good", "nothing", "everything was perfect" or "not everything was good" as they cannot be categorized and are questionable regarding their information value.

To analyze the qualitative feedback statements we use the coding schema of Kay and Knaack (2009) including the three main categories "Learning", "Engagement" but also "Quality". However, we discarded the sub-category "help" because there is no statement which refers to it directly. In addition, the following categories offered no statements for the "NOT LIKE" item: 'Learning: beneficial visual feature'; 'Learning: occurred learning/teaching issue'; 'Engagement: using the artifact is fun/enjoyable/engaging/ interesting'; 'Engagement: comparison to other methods of teaching'. The rigorous analysis revealed that there are statements that only show slight differences, e.g., "Learning content was not challenging/obvious solutions" sets a focus on challenging learning content in general, and "Learning content was too obvious to students with prior knowledge" adds information that this might only concern students with prior knowledge. With that in mind, we outline and discuss the key findings and declare the number of statements referred to it within the text or by the number within parentheses at the end of a finding, e.g., "statement 1 (4)".

First, we analyze the statements related to the ***"Learning category"***. For the sub-category *"challenging learning content"* 1 student liked the vivid and understandable learning content, 1 student liked that they learned something new (e.g., the location of the computer department) and 1 more student noted that the content is applicable and even 'beneficial' for students of other bachelor programs. Contrary, a considerable number of students stated that the learning content was not challenging or included obvious solutions (8) and thus, that it might be too obvious to students with prior knowledge (1). The next sub-category is *"beneficial visual feature"*. Students mentioned positively that real-world video pictures support tangible awareness of real threats (2), decision paths support positive learning experiences and 'look and feel' (2), they also liked the integration of learning scenarios, that are explained by the educator (2), and further, that decision screens enabled the reflection of own behavior (1). The last sub-category *"occurred learning/teaching issue"* provided only one statement, namely "no issues".

Second, we proceed to analyze the statements related to the ***"Engagement category"***. Regarding the sub-category *"using the artifact is fun/enjoyable/engaging/interesting"*, a considerably high number of students provided positive feedback, namely that the video is entertaining, interesting, and engaging, so it supports active learning (10), generally the video is enjoyable and exciting (2) and one student would like to watch more videos like this, further, students mentioned that the included decision paths increase curiosity (2) and makes the learning content engaging (2) in a way, that it motivates even "not attractive learning content" (1). In addition, statements related to the sub-category *"comparison to other methods of teaching"* revealed that the method is perceived as something new or refreshing (6), that fosters a better focus on learning content (e.g., compared to non-interactive videos) (3), furthermore, the first-person perspective makes it immersive (2), and the interactive method activates learning better than passive methods (1). However, related to the sub-category *"occurred issues with technology"*, a minor number of students report problems with technology: The visual representation within the LMS (1) is not sufficient, the video stops in some cases after wrong decisions (1) and that decision options disappeared (1).

Third, we identify a high number of statements that refer to the **"Quality category"**. For instance, regarding the sub-category *"interactive parts"*: A high number of students liked the interactivity in general (12) and that different decisions within a story support immersive interactions (7) or that a variety of options are available, not just the right or wrong (3). Thus, some report that this supports learning the key statements (3). Positive feedback related to the sub-category *"animation"* includes the following: Realistic scenario recordings in general (4), first person-perspective (4), using time laps of real-world recordings (1), and real persons' actions made it look real (1). Nevertheless, students report negative aspects as well, such that the e-mail on the recorded screen was hardly readable (2), the time laps scene was a bit too long (1) and the video quality (resolution) should be improved (1). For the sub-category *"control while using the learning object"* four positive feedback statements are identified, to be specific, students liked to control the path of the story within the video through their own decisions, but one student criticizes that decision paths are not predictable before taking any action. Regarding the sub-category *"ease of use"*, 2 students mentioned positively that the decision paths are traceable and realistic making them easy to understand, contrary, 2 students state a problem regarding the understanding of the decision path and option wording, and 1 student criticizes the pace of the storytelling in the video. Only three statements are related to the sub-category *"theme"*: 3 statements emphasized the importance of the topic, 1 student liked the "useful content", remaining 1 student who stated the theme was not complex enough. Statements that relate to the sub-category of "organization of the learning object" are: Students liked the creativity regarding the whole video (3), the gameful experience (2) real person actors within the video (2), using humor (2), appropriate design (1), that content is designed to reflect the known real-world environment of the target group (1), the storyline (1), and the option to replay (1). However, 5 statements include that the story was predictable to some degree, non-professional actors show limited emotions and acting skills but also dialog quality looks staged (4), options that are obvious to the user are not presented, which interrupts the immersive gameplay (1), and that the video needs too much time (2). Statements related to the sub-category *"audio"* only include critique, namely the voice of the actors seem a bit robotic (1), the audio quality should be improved (1) and one student reports the ringtone of the smartphone used in the video as a negative aspect.

The results of analyzing the control measure items show that 28 students would recommend this ISA training to other students (9-10 points), and 12 students scored 8 points. Further, 34 students would participate again in an ISA training which is using interactive videos (9-10 points), and 10 students rated 8 points. Explanation of students that rated lower than 9 points are mostly similar, which means that decision options and solutions are too obvious, they do not recommend lectures in general, or feel very confident regarding their level of ISA. This indicates that a high number of students rate our approach positively, but some students with limitations. Thereby, the differentiated explanations confirm both the quantitative scoring and our findings to be consistent and so we assume our qualitative findings to be valid and reliable.

4.4 Discussion

In order to determine the level of ISA on basis of the results of the t-test, we calculate the ISA score by the summed-up mean values of the subareas, but also of the focus area, and assign them to the categorical levels of ISA (good, average, poor). Here, it is noteworthy that the ISA average level was 'good' before treatment for the *whole* focus area (summed up mean value of points: 12,23 points = >82%). However, as 2 out of 3 subareas reached a level of 80%, the score of the sub-category 'Ignoring poor security behavior by colleagues' revealed a need for action as it was only average (11,6 points =<78%). The ISA level *after treatment* increased to a considerably high level for the whole focus area (summed up mean value of points: 13,26 points =>88%) and also for the previously lower rated subarea 'Ignoring poor security behavior by colleagues' (12,79 points=>85%). So RQ1 can be answered with regard to the level of ISA and in combination with the significant results of the t-test. Both results indicate evidence that the interactive video strongly increased the level of ISA of students and thus, supports positive learning outcomes to a significant extent. In addition, RQ2 can be answered by outlining the qualitative findings. These indicate that an interactive narrative can be an important design factor for successful educational approaches since it supports active learning and engagement with the learning content, e.g., by fostering curiosity using choice-based interactions and the reflection of own decisions. Further, the statements indicate that for cybersecurity education, videos recorded in first-person perspective for a specific target group, and real-world recordings in general, foster immersive and credible learning content but also convey the importance of the topic realistically. Nevertheless, a high number of students reported that the approach is "refreshing/something new" and although this seems positive at first sight, it may also indicate that learning effects are also related to the novelty of interactive videos themselves and may differ if interactive videos would become ubiquitous. The results also contain criticisms that are important for further design iterations, e.g., that the learning content and solutions for decisions might be too limited and obvious (but can also be considered a low-barrier training format for students without prior knowledge). Hence, more complex but traceable decision options should be integrated. Thus, we consider differentiation for different key-user groups in the future. Additionally, the results indicate that the video should be further streamlined, including fastening the pace of the storytelling and shortening the video length. Although only mentioned in three statements, technical problems must be solved in the future to provide a positive learning experience for all students, e.g., the visual representation within the LMS or bugs while interacting within the decision process should be reviewed.

In summary, the quantitative and qualitative results strongly indicate that the interactive video achieved its aim, namely educating students and training ISA. Furthermore, the video improves the level of ISA and was enjoyable even for students with prior knowledge and this indicates that it can be applied as a refreshing measure.

5 Conclusion: implications and limitations

The design and the evaluation of our artifact provides meaningful design knowledge for practitioners and researchers. In response to RQ1, we state that our interactive educational video has a **strong significant effect on building ISA** for the reporting of security incidents. Furthermore, by analyzing the qualitative students' feedback and answering RQ2, we provide important novel design knowledge for effective security education in general and the development of design principles in future design cycles, for effective interactive videos that rely on choice-based storytelling. Thus, for better transferability toward future design principles, we formulate the following recommendations for information security educators in accordance to Gregor et al. (2020) but note that for mature design principles, further evidence is needed: Educators should implement a wide variety of meaningful decision options including different levels of challenge to support active learning and engagement with the content. In addition, learning videos should be designed using real-world recordings and varying storylines to foster curiosity, relatedness and interest, so that it creates value for the students. Further, using humor and implementing an interactive design in general is crucial for educational videos in the field of security education because students perceive such an approach to be refreshing, enjoyable but also engaging. Pitfalls that educators should avoid are, technical issues with accessing the content, including too few decision options within the video and providing too much video content in length. Future research should focus on determining a range for an appropriate number of decision options and length of video content. However, there are limitations: a) We evaluated only one focus area of the HAIS-Q and thus, other areas should be included in future design iterations. Further, b) using a within-subject design without a control group only reveals the effectiveness of the interactive video but provides no direct evidence whether it performs better than other ways of delivery. However, some qualitative statements indicate a better performance and therefore, we state this as further promising point for future research.

References

Abawajy, J. (2014) 'User preference of cyber security awareness delivery methods', *Behaviour & Information Technology*, vol. 33, no. 3, pp. 237–248.

Almeida, C., Kalinowski, M. and Feijo, B. (2021) 'A Systematic Mapping of Negative Effects of Gamification in Education/Learning Systems', *2021 47th Euromicro Conference on Software Engineering and Advanced Applications (SEAA).* Palermo, Italy, 01.-03.09.2021, IEEE, pp. 17–24.

Alyami, A., Sammon, D., Neville, K. and Mahony, C. (2022) 'The Critical Success Factors for Security Education, Training and Awareness (SETA) Programmes', *2022 Cyber Research Conference - Ireland (Cyber-RCI).* Galway, Ireland, 25.04.2022, IEEE, pp. 1–12.

Baldwin, S. and Ching, Y.-H. (2017) 'Interactive Storytelling: Opportunities for Online Course Design', *TechTrends*, vol. 61, no. 2, pp. 179–186.

Beheshti, M., Taspolat, A., Kaya, O. S. and Sapanca, H. F. (2018) 'Characteristics of Instructional Videos', *World Journal on Educational Technology: Current Issues*, vol. 10, no. 1, pp. 61–69 [Online]. Available at https://eric.ed.gov/?id=ej1170366.

Brehmer, M. (2023) *Interaktives Lernvideo zur Bildung von Informationssicherheitsbewusstsein: ein zielgruppenspezifisches Training für Studierende* [Online], University of Augsburg. Available at https://www.digillab.uni-augsburg.de/kursarchiv/interaktives-lernvideo-zur-bildung-fuer-informationssicherheitsbewusstsein-ein-zielgruppenspezifisches-training-fuer-studierende/.

Brehmer, M., Abbas, E. A. and Vaidyanathan, N. (2021) 'Towards Designing A Method To Create Sticky Information Security Training For SMEs: Identifying Design Factors', *29th European Conference on Information Systems,* 14.-16.06.2021, (ECIS).

Brehmer, M. and Reinelt, R. (2023) 'Gamifying a Learning Management System: Narrative and Team Leaderboard in the Context of Effective Information Security Education', *Proceedings of the 56th Annual Hawaii International Conference on System Sciences,* 03.01-06.01.2023.

Chen, C.-C., Huang, ChingChih, Gribbins, M. and Swan Karen (2018) 'Gamify Online Courses with Tools Built into Your Learning Management System (LMS) to Enhance Self-Determined and Active Learning', *Online Learning*, vol. 22, no. 3.

Chouhan, R. (2021) 'Effective interactive video assignments and rewatch analytics for online flipped classrooms', *2021 IEEE 1st International Conference on Advanced Learning Technologies on Education & Research (ICALTER).* Lima, Peru, 16.-18.12.2021, IEEE, pp. 1–4.

Cindana, A. and Ruldeviyani, Y. (2018) 'Measuring Information Security Awareness on Employee Using HAIS-Q: Case Study at XYZ Firm', *2018 International Conference on Advanced Computer Science and Information Systems (ICACSIS).* Yogyakarta, Indonesia, 27.-28.10.2018, IEEE, pp. 289–294.

Croasdell, D., Elste, J. and Hill, A. (2018) ‘Cyber Clinics: Re-imagining Cyber Security Awareness’, *Hawaii International Conference on System Sciences 2018 (HICSS-51)* [Online]. Available at https://aisel.aisnet.org/hicss-51/ks/ks_security/8.

Crowne, D. P. and Marlowe, D. (1960) ‘A new scale of social desirability independent of psychopathology’, *Journal of consulting psychology*, vol. 24, pp. 349–354.

Csikszentmihalyi, M. (1990) *Flow: The psychology of optimal experience*, New York, Harper & Row.

D'Arcy, J., Herath, T. and Shoss, M. K. (2014) ‘Understanding Employee Responses to Stressful Information Security Requirements A Coping Perspective’, *Journal of Management Information Systems*, vol. 31, no. 2, pp. 285–318.

Deci, E. L. and Ryan, R. M. (2000) ‘The „What“ and „Why“ of Goal Pursuits: Human Needs and the Self-Determination of Behavior’, *Psychological Inquiry*, vol. 11, pp. 227–268.

Deterding, S., Dixon, D., Khaled, R. and Nacke, L. (2011) ‘From game design elements to gamefulness’, *Proceedings of the 15th International Academic MindTrek Conference on Envisioning Future Media Environments.* Tampere, Finland, 28.09.2011 - 30.09.2011. New York, USA, p. 9.

Dincelli, E. and Chengalur-Smith, I. (2020) ‘Choose your own training adventure: designing a gamified SETA artefact for improving information security and privacy through interactive storytelling’, *European Journal of Information Systems*, vol. 29, no. 6, pp. 669–687.

Fertig, T., Henkelmann, D. and Schütz, A. (2022) ‘360 Degrees of Security: Can VR Increase the Sustainability of ISA Trainings?’, *Proceedings of the 55th Hawaii International Conference on System Sciences,* (HICSS).

Firsty Arisya, K., Ruldeviyani, Y., Prakoso, R. and Lailatul Fadhilah, A. (2020) ‘Measurement of Information Security Awareness Level: A Case Study of Mobile Banking (M-Banking) Users’, *2020 Fifth International Conference on Informatics and Computing (ICIC).* Gorontalo, Indonesia, 03.-04.11.2020, IEEE, pp. 1–5.

Grasse, K. M., Kreminski, M., Wardrip-Fruin, N., Mateas, M. and Melcer, E. F. (2022) ‘Using Self-Determination Theory to Explore Enjoyment of Educational Interactive Narrative Games: A Case Study of Academical’, *Frontiers in Virtual Reality*, vol. 3.

Grasse, K. M., Melcer, E. F., Kreminski, M., Junius, N., Ryan, J. and Wardrip-Fruin, N. (2022) ‘Academical: A Choice-Based Interactive Storytelling Game for Enhancing Moral Reasoning, Knowledge, and Attitudes in Responsible Conduct of Research’, in *Games and Narrative: Theory and Practice,* Springer, Cham, pp. 173–189.

Gregor, S., Kruse, L. and Seidel, S. (2020) ‘Research Perspectives: The Anatomy of a Design Principle’, *Journal of the Association for Information Systems*, vol. 21, pp. 1622–1652.

Hamari, J., Koivisto, J. and Sarsa, H. (2014) ‘Does Gamification Work? -- A Literature Review of Empirical Studies on Gamification’, *2014 47th Hawaii International Conference on System Sciences.* Waikoloa, HI, 06.-09.01.2014, IEEE, pp. 3025–3034.

Hu, S., Hsu, C. and Zhou, Z. (2021) 'Security Education, Training, and Awareness Programs: Literature Review', *Journal of Computer Information Systems*, pp. 1–13.

Kay, R. H. and Knaack, L. (2009) 'Assessing learning, quality and engagement in learning objects: the Learning Object Evaluation Scale for Students (LOES-S)', *Educational Technology Research and Development*, vol. 57, no. 2, pp. 147–168.

Kirova, D. and Baumöl, U. (2018) 'Factors that Affect the Success of Security Education, Training, and Awareness Programs: A Literature Review', *Journal of Information Technology Theory and Application (JITTA)*, vol. 19, no. 4 [Online]. Available at https://aisel.aisnet.org/jitta/vol19/iss4/4/.

Knop, D. (2023) 'Ransomware: Daten von Uni Duisburg-Essen im Darknet, Uni Innsbruck attackiert', *heise online*, 17 January [Online]. Available at https://www.heise.de/news/Ransomware-Daten-von-Uni-Duisburg-Essen-im-Darknet-Uni-Innsbruck-attackiert-7461603.html (Accessed 23 February 2023).

Martin, A. (2023) 'Switzerland's largest university confirms 'serious cyberattack'', *The Record from Recorded Future News*, 3 February [Online]. Available at https://therecord.media/switzerlands-largest-university-confirms-serious-cyberattack/ (Accessed 23 February 2023).

McCormac, A., Calic, D., Parsons, K., Zwaans, T., Butavicius, M. and Pattinson, M. (2016) 'Test-retest reliability and internal consistency of the Human Aspects of Information Security Questionnaire (HAIS-Q)', in *ACIS 2016 Proceedings*.

Melcer, E. F., Grasse, K. M., Ryan, J., Junius, N., Kreminski, M., Squinkifer, D., Hill, B. and Wardrip-Fruin, N. (2020) 'Getting Academical: A Choice-Based Interactive Storytelling Game for Teaching Responsible Conduct of Research', *International Conference on the Foundations of Digital Games.* Bugibba Malta, 15 09 2020 18 09 2020. New York, NY, USA, ACM, pp. 1–12.

Murray, J. H. (2018) 'Research into Interactive Digital Narrative: A Kaleidoscopic View', in Rouse, R., Koenitz, H. and Haahr, M. (eds) *Interactive Storytelling: 11th International Conference on Interactive Digital Storytelling, ICIDS 2018, Dublin, Ireland, December 5–8, 2018, Proceedings,* Cham, Springer International Publishing, pp. 3–17.

Nguyen, T. A. and Pham, H. (2020) 'A Design Theory-Based Gamification Approach for Information Security Training', *2020 RIVF International Conference on Computing and Communication Technologies (RIVF).* Ho Chi Minh City, Vietnam, 14.-15.10.2020, IEEE, pp. 1–4.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A. and Zwaans, T. (2017) 'The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies', *Computers & Security*, vol. 66, pp. 40–51.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. and Jerram, C. (2014) 'Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)', *Computers & Security*, vol. 42, pp. 165–176.

Peffers, K., Tuunanen, T., Rothenberger, M. A. and Chatterjee, S. (2007) 'A Design Science Research Methodology for Information Systems Research', *Journal of Management Information Systems*, vol. 24, no. 3, pp. 45–77.

Rajadell, M. and Garriga-Garzón, F. (2017) 'Educational videos: After the why, the how', *Intangible Capital*, vol. 13, no. 5, p. 903.

Ralston, W. (2021) *The untold story of a cyberattack, a hospital and a dying woman* [Online] (SECURITY). Available at https://www.wired.co.uk/article/ransomware-hospital-death-germany (Accessed 15 May 2022).

Ryan, R. M. and Deci, E. L. (2000) 'Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being', *American Psychologist*, vol. 55, no. 1, pp. 68–78.

Salem, Y., Moreb, M. and Rabayah, K. S. (2021) 'Evaluation of Information Security Awareness among Palestinian Learners', *2021 International Conference on Information Technology (ICIT).* Amman, Jordan, 14.-15.07.2021, IEEE, pp. 21–26.

Shelton, C. C., Warren, A. E. and Archambault, L. M. (2016) 'Exploring the Use of Interactive Digital Storytelling Video: Promoting Student Engagement and Learning in a University Hybrid Course', *TechTrends*, vol. 60, no. 5, pp. 465–474.

Taber, K. S. (2018) 'The Use of Cronbach's Alpha When Developing and Reporting Research Instruments in Science Education', *Research in Science Education*, vol. 48, no. 6, pp. 1273–1296 [Online]. DOI: 10.1007/s11165-016-9602-2.

Tischer, M., Durumeric, Z., Foster, S., Duan, S., Mori, A., Bursztein, E. and Bailey, M. (2016) 'Users Really Do Plug in USB Drives They Find', *2016 IEEE Symposium on Security and Privacy (SP).* San Jose, CA, 22.-26.05.2016, IEEE, pp. 306–319.

Tung, L. (2022) 'Ransomware warning: Cyber criminals are mailing out USB drives that install malware', *ZDNET*, 10 January [Online]. Available at https://www.zdnet.com/article/fbi-cybercriminals-are-mailing-out-usb-drives-that-will-install-ransomware/ (Accessed 23 February 2023).

Ulsamer, P., Schütz, A., Fertig, T. and Keller, L. (2021) 'Immersive Storytelling for Information Security Awareness Training in Virtual Reality', *Proceedings of the 54th Hawaii International Conference on System Sciences,* (HICSS).

Ulven, J. B. and Wangen, G. (2021) 'A Systematic Review of Cybersecurity Risks in Higher Education', *Future Internet*, vol. 13, no. 2, p. 39.

Venable, J., Pries-Heje, J. and Baskerville, R. (2012) 'A Comprehensive Framework for Evaluation in Design Science Research', *Design Science Research in Information Systems. Advances in Theory and Practice.* Berlin, Heidelberg, Springer Berlin Heidelberg, pp. 423–438.

Wahyudiwan, D. D. H., Sucahyo, Y. G. and Gandhi, A. (2017) 'Information security awareness level measurement for employee: Case study at ministry of research, technology, and higher education', *2017 3rd International Conference on Science in Information Technology (ICSITech).* Bandung, 25.-26.10.2017, IEEE, pp. 654–658.

Wang, F. (2022) ‘College Students' experience of using online video and educational video’, *2022 10th International Conference on Orange Technology (ICOT).* Shanghai, China, 10.-.11.2022, IEEE, pp. 1–4.

Wilson, M. and Hash, J. (2003) *Building an Information Technology Security Awareness and Training Program* [Online], NIST.

Yoo, C. W., Sanders, G. L. and Cerveny, R. P. (2018) ‘Exploring the influence of flow and psychological ownership on security education, training and awareness effectiveness and security compliance’, *Decision Support Systems*, vol. 108, pp. 107–118.