The Use of Story-based Gamification in USB-based Attack Prevention

VASCO RIKKERS, University of Twente, The Netherlands

Human error is one of the major causes of security incidents and data breaches in companies. An example of an attack type that relies on human error is USB-based attacks. A possible solution is gamification, as it has shown promise in influencing people's behavior. The goal of this study will be to test the effectiveness of story-based gamification in the prevention of USB-based attacks. To do this, an application has been developed that gamified USB-based attack prevention training. An empirical case study has been done to assess the effectiveness by analyzing participants' experiences with the gamified approach. Overall, they were positive and showed that it successfully educated them on USB-based attacks.

Additional Key Words and Phrases: **Cyber-security Awareness, Story-based Gamification, USB-based attacks, University students, Security behavior.**

1 INTRODUCTION

Human error is one of the main causes of security incidents. This can, for example, be seen in Egress's Insider Data Breach Survey from 2021. In this survey, they asked IT leaders in some of the biggest tech companies about the causes of serious data breaches. 84% of them said that within their company, human error was the leading cause of major incidents [14].

An example of an attack-type that relies on human error to be effective is USB-based attacks [48]. These are attacks that use a USB device [51] as a vector [34]. In recent years, an increase in the number of these types of attacks has been observed [39]. This shows that it is important to focus on prevention of these types of attacks, for example by training people and raising awareness. In the past, this has been effective in the prevention of other cyber-security attacks and in changing people's behaviour[11].

One tactic used to train people on cyber-security topics is gamification [9]. Gamification, or serious gaming, is applying games in a learning environment to engage students [53]. Examples of gamification include popular applications such as *Dualingo* [13] and *Headspace* [20]. These applications deploy leaderboards, badges, and points to engage their users and get them to enjoy learning.

1.1 Background Knowledge

Before going further into the current knowledge gap and the research itself, this subsection will give some background information on USB-based attacks and gamification. First, it goes into the USB based attack types, its effectiveness, and prevention. Then it dives into gamification, its effectiveness, key concepts, and storytelling.

1.1.1 USB-based Attacks. In past years, researchers have identified 29 different USB-based attacks. They range in function from infecting systems with malware to leaking sensitive information [35]. Also, research has been done on how effective USB-based attacks still are today. An example of this is research that was done on the University of Illinois, Urbana-Champaign campus in 2016 [50]. Researchers dropped around 300 different USBs on campus grounds. The goal was to test whether students would take the USBs they found and plug them into their computers. The researchers found that of the 297 USBs dropped, 98% of them were removed from where they were dropped, and 45% of them were connected to a computer.

Currently, measures exist can protect against USB-based attacks. Most of them either use pop-ups or filters to check the contents of the USB to see if it is malicious or not [30] [19]. But, in these cases, they need the user to have these measures installed and to be present at the laptop when the USB is plugged in. And newer forms of attack can bypass these security implementations [50].

In terms of prevention, there are examples of a narrative being used to teach people about the dangers of USB-based attacks. For example, Inspired eLearning [52] and Utwente Security Education Platform [47] both produced videos on about this topic. They use narrative and humor to engage the watchers and to give them information. But they both run into the same issue. They do not use choice or interact with the viewer. The stream of information is one way, unlike with gamification.

1.1.2 Gamification. Over the past few years, researchers have done more and more research on the use of gamification to train people [41] [28] [25]. For example, in the research conducted by Michael Sailer et al. [41], a meta-analysis of articles on gamification and learning was carried out. It found that gamification affects learning positively. A similar trend can be seen in cyber-security training. More and more research is being done on how gamification can be deployed to better train people in this field [9]. For example, in phishing prevention [33][24]. There are several key concepts that can be used gamification to make it effective. [4][25][12]. These include leader boards, badges/medals, points, providing a mission or goal, and giving feedback.

According to Kapp, Blair, and Mesch (2013, p.118), storytelling is one of the most under-used and effective methods to improve learning [23]. Research in 2014 has illustrated that the use of storytelling can improve learning in preschool education [18]. In this study, the researchers deployed a robot that told stories and incorporated motor movements for children to follow. It showed that this approach can be implemented to engage preschoolers in constructive learning. In cyber-security training, there are examples of gamification approaches that use perspective to engage the user and cause them to be less susceptible to attacks [42][2]. One of these examples is research done in 2015 in which the game was played from the perspective of the attacker [2]. But, this research was non-conclusive due to there being not enough practical and tested evidence. On the other side of the spectrum, there are also examples of researchers excluding narrative and storytelling when

TScIT 37, July 8, 2022, Enschede, The Netherlands

discussing important gamification concepts [54]. They argue gamification should be focused on non-fiction and so the narrative has no place in this. But others argue it can add a lot to the quality. For example, Nicholson proposed the term “meaningful gamification”, which goes beyond points and badges [32].

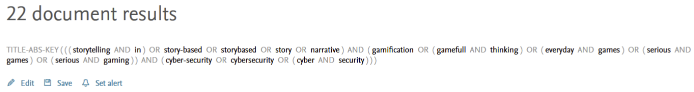
1.2 Knowledge gap

In 2020, a group of researchers at the University of Maryland did a systematic review of digital games related to cyber-security [8]. They looked at 181 different games related to this topic and found that 74% of those deploy story-telling. Yet, when doing searches on databases such as Scopus, there seems to be a lack of research on the effect of story-telling.

For example, a search has been done in Scopus for papers related to story-based gamification for cyber-security using the Query seen in Figure 1. This search resulted in 22 results, as shown in Figure 2.

```
TITLE-ABS-KEY (
        ( ( storytelling AND in ) OR story-based OR storybased OR story
        OR narrative )
    AND ( gamification OR ( gamefull AND thinking ) OR (every day AND games )
        OR ( serious AND games ) OR ( serious AND gaming )
        OR ( game AND fiction ) )
    AND ( cyber-security OR cybersecurity OR ( cyber AND security ) )
`
```

Fig. 1. Query used in Scopus for story-based gamification in cyber-security.


22 document results

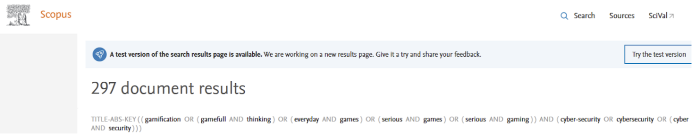
TITLE-ABS-KEY (((storytelling AND in) OR story-based OR storybased OR story OR narrative) AND (gamification OR (gamefull AND thinking) OR (everyday AND games) OR (serious AND games) OR (serious AND gaming)) AND (cyber-security OR cybersecurity OR (cyber AND security)))

Fig. 2. Results of query on Scopus with story telling (16/05/22).

But, searching only for papers related to gamification for cyber-security using the query from Figure 3, excluding the story-telling aspect returns 297 results, as seen in Figure 4.

```
TITLE-ABS-KEY (
        ( gamification OR ( gamefull AND thinking ) OR (every day AND games )
        OR ( serious AND games ) OR ( serious AND gaming )
        OR ( game AND fiction ) )
    AND ( cyber-security OR cybersecurity OR ( cyber AND security ) )
)
```

Fig. 3. Query used in Scopus for gamification in cyber-security.



A test version of the search results page is available. We are working on a new results page. Give it a try and share your feedback.

297 document results

TITLE-ABS-KEY ((gamification OR (gamefull AND thinking) OR (everyday AND games) OR (serious AND games) OR (serious AND gaming)) AND (cyber-security OR cybersecurity OR (cyber AND security)))

Fig. 4. Results of query on Scopus without story-telling (16/05/22).

A similar trend has been observed in other databases, such as Web of Science Core Collections. So, while research shows that a majority of cyber-security-related gamifications deploy story-telling, less than 10% of published papers seem to look at how effective it is. This is quite a difference. More research should be done on the effect of story-based gamification to see what the effects of it are on the effectiveness of gamification.

1.3 Research Question

Main research question

What is the impact of story-based gamification on USB-based cyber-attack prevention among students?

Sub research questions

1. What story-based gamification concepts were perceived as effective in previous gamification research?

2. Which of these concepts can apply to gamified USB-based cyber-attack prevention?

3. What is the perceived effectiveness of an application created using the characteristics from Sub-Question 2 when applied to USB-based cyber-attack prevention?

1.4 Objective

This research tried to see if a story-based gamified application can help prevent USB-based attacks. It comprises a literature review and the creation and testing of an application. The focus of the literature review was to gather background knowledge on story-based gamification. In the end, the goal was to create and test an application that uses story-based gamification to train users on USB-based cyber-attack prevention.

1.5 Scope

The literature review has provided information on the concepts of story-based gamification that in earlier research were observed to be effective. It included an analysis of five papers and articles on story-based gamification. They were conference and journal articles, and dissertations. The papers were selected based on the following criteria. First off, how many times have they been referenced by other articles? All the articles have at least 50 citations from other works. The second criterion was the journal in which they have been published. Is it known as a credible journal and conference that does high-quality peer checks? An example of such a conference is the ACM Symposium on Computer and Communications Security [1], which gets a h5 index of 94 [10]. The final criterion was the author of the research and to what institutions are they connected. An example of a credible institution that was used is the *Syracuse University School of Information Studies*.

The game itself took shape as a web-based game. Because of this, users don’t have to download applications to access it and it can be used over one platform. The programming language that would be most suitable for this would be JavaScript with HTML5 as a complementing mark-up language.

The research focused on students. The reason for this is that the past research from 2020 has found that students are susceptible to cyber-attacks [45]. At least 28 students needed to take part. This number allows for a power of 80% for a one-sided t-test on one group and a Wilcoxon signed rank test. This is based on commonly used standards for this kind of research [6] and the Gpower calculator from the University of Dusseldorf [16]. To incentivize people to take part, were offered the chance to get an overview of the results if they took part. Using this instead of, for example, monetary rewards reduces the risk of attracting reward seekers or introducing bias. [44] [22].

2 RELATED WORK

In the past, there have been several studies that have been done on the use of story-telling and gamification. They are described below.

2.1 Gamification of a University Course [37]

In their research, O'Donovan et al. [37] present the gamification of a university course on game development. Their goal was to increase lecture attendance, content understanding, problem-solving skills, and general engagement. To achieve this, they deployed several gamification techniques, including storytelling. It was set in a steampunk world where the students had to solve a mystery, which could be done by interacting with the classes in the course. The researchers also related it to the different gamer profiles that were out there to the "seeker nature". In the end, they found the students indicated they were happy with how the narrative was integrated, but they were not sure if it improved the gamification. They considered this might be because of the storyline being not sufficiently integrated into the course. The main takeaway from this research is that the storyline should be integrated with the work. It should relate to what gamification is and supplement it.

2.2 RECIPE for Meaningful Gamification [31]

In their research, Nicholson et al. [31] identified a problem with reward-based gamification. They found that this type of gamification creates a short-term change in behavior among participants. They discuss that there should be intrinsic motivation to cause long-term change even after rewards are stopped. To do this, Nicholson creates a framework they call "Meaningful gamification". Out of this framework, 2 concepts seem of interest for this research. These are exposition and information.

The exposition part of the framework talks about using stories in gamification. According to Nicholson, exposition is used to make users are more connected with the real-world setting. And he says that it comprises 2 main parts: developing and presenting a meaningful narrative element.

He identified two ways of doing this. The first one is to embed the story in the real-world, which creates a more simulation-like experience. Players can explore different paths, and it provides them with information on the real-world setting. The second way is to use analogies. Here, the game world might not be the real-world, but is directly related to it. He states that this could have an advantage in that it can offer richness over the real-world. So it might draw more people in. But, this can also be difficult to carry out and to make the link with the real world clear.

One thing that also should be considered is what type of narrative to use. Nicholson discusses four types. Evoked narrative, where the story is embedded in a pre-existing world. Enacted narrative, which uses a more cinematic approach, where cut-scenes and fixed game sequences limit gameplay in favor of more story-telling. In an embedded narrative, the user finds out about a story, which is shaped by the (player) character's choices and so they learn about the world through the game elements. And finally, emergent narrative, where the user shapes the story purely with their choices.

For the information concept, Nicholson discusses the idea of presenting the "why" and "how" to a user, not just the "what was done" or "what is the reward". He discusses different ways this can be done, but there are 2 relevant topics for story-telling. First, he mentions using an NPC as a guide. This guide provides the user with information and helps them. The second method is to integrate it with the exposition. Especially the method of "embedded narrative" was mentioned. This can not only give information about the game world, but also about the real-world with the same game elements.

There is also a general problem that applies to all gamification. That is the idea of relevance. Not all the information applies to everyone. Nicholson discusses the library approach, where a wide variety of information is provided, which can link to a wide variety of knowledge levels.

2.3 Using Narrative to Improve Reactions & Learning [5]

In their research, Armstrong et al. [5] Gamified an existing training with game fiction. They took Thorndyke's structure for creating simple stories [49] and used it to transform the training content into game fiction. They identified that TETEM suggested that game fiction-enhanced training will vary in effectiveness depending on an individual's pre-existing attitudes. From their research, they found that the use of narrative caused trainees to be significantly more satisfied with the training. They also looked at its influence of it on users' change in declarative knowledge and procedural knowledge. They found it did not affect the declarative knowledge score of a participant, but it lowered the score on the procedural knowledge. But, this lowering of the score. One thing that can be used from this is the use of Thorndyke's structure for creating simple stories and how the narrative was applied. It also shows that the use of story-telling can have different effects on types of knowledge.

2.4 Points, Stories, Worlds, And Diegesis [38]

In this research, the researchers compare points-based gamification to story-based gamification. To do this, they created two games and let participants play them. One of these games, Forgotten Island, was heavily story-based and had a mystery theme. The other is Happy Match. They were used to teaching the participants about classifying plants and insects from photos. In the end, the researchers found that the Forgotten Island was strongly preferred over Happy Match by participants.

The researchers differentiate between two types of fantasy/fiction: exogenous & endogenous. In exogenous fantasy, there is no direct link between the task someone does and the narrative. For example, doing correct calculations might launch a rocket, but these calculations might not relate to the launching. For example, calculating that 2 + 2 = 4. In endogenous fantasy, the task is thematically and/or narratively linked to the game world. So, for example, you calculate the trajectory of the rocket and then launch it.

One of the main topics discussed was the term "diegesis". The term diegesis refers to the difference between the "real world" and the "story world". Part of this is all things that affect the story and the world. So, for example, if someone finds a letter in the story and it is full of spelling mistakes, it might show that the writer is not educated. Participants showed that elements of the story and the world made them be more engaged with the system.

Outside of diegesis, the paper identifies 2 other elements that had a positive impact. This is sensory stimulation and agency. It was stated that the atmosphere, art style and other sensory aspects of the Forgotten Island were an incentive to play and made it enjoyable. By agency, the researchers mean the sense of control that the user felt to have. However, users did state that the story was less efficient and took longer to play.

2.5 Jail, Hero Or Drug Lord? [7]

This research used a story-based adventure game to supplement a cyber-security course. To do this, a "Choose Your Own Adventure Story" was created. Here the student was a new cyber-security employee and need to solve a mystery. Now, they can decide on their own what their decisions are and influence the ending. Different story paths are available that students can follow to personalize the experience.

The students showed the story increased their engagement with the material and that it made the material "fun". The researchers show that the people that partook in the story-based part of the course did better in their classes and outperformed the students who did not take part.

There are a few topics that can be taken from this research. The students praised the realism and the writing level. Researchers indicated that the quality of the writing could be one reason for the high-level engagement of students. One thing that the students were less excited about is the time commitment. It was indicated that students overestimated the time that would go into this extra story element. This made them reluctant to take part, even though they thought it was a good idea.

3 METHODOLOGY

To make it so that research happened in an organized fashion, it has been divided into different stages. Figure 5 depicts the stages and flow of the research. Each stage has a different color and answers one of the research sub-questions.

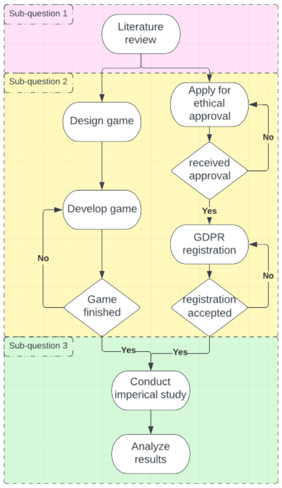


Fig. 5. Flow chart of the used method

Concerning sub-question 1, the method was as follows. A literature review has been done on story-based gamification concepts. The articles were summarized, and the main story-based concepts and their effectiveness were explained. This information was used to create an overview of what research already has been done for story-based gamification.

Using insights from the literature study, sub-Question 2 can be answered as well. This is the stage in which an application has been designed that implements the concepts found in the literature study. This way, the most relevant concepts of story-based gamification could be implemented into the game.

This application has been used in an empirical study, which answered sub-question 3. At the beginning of the study, all participants were asked to take part in a pre-game survey that asks about their background and how much they know about USB-based attacks. Following this, people played through the game from start to finish. Finally, all participants were asked to do a post-training survey. This survey checked what the perceived effectiveness of gamification. As well as how people thought it compares to other gamifications.

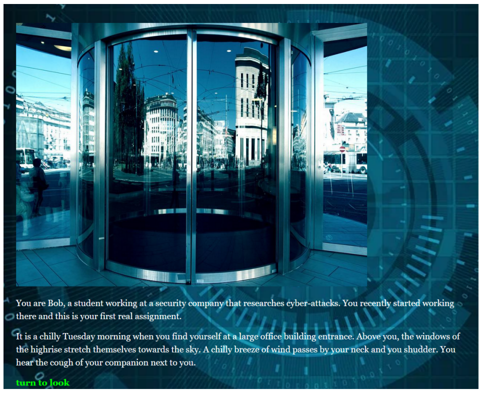
To do tests and surveys, it was necessary to get ethical approval from the university [43]. This permission was obtained.

4 GAME & SURVEY DESIGN

This section discusses the design of the game and surveys which were used to answer the sub-research question 3. First, it goes into how the game was designed and build. Second, it discusses how the measurements were done and data was obtained.

4.1 Game design

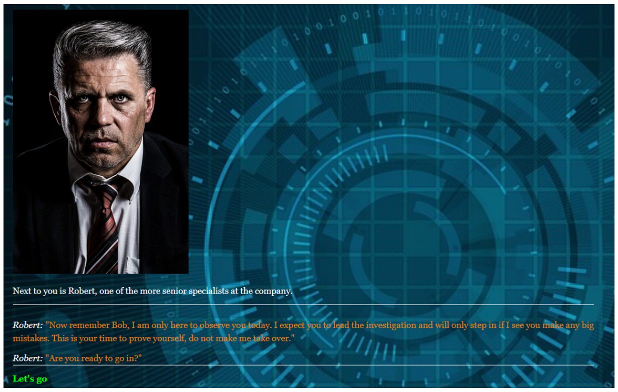
The game is an adventure text-based game that resembles the interactive novel genre [15]. In the game, the user's decisions influence the story. The reason for picking this type of game as inspiration is to leave out any non-story-related aspects that might affect the effectiveness of the games. So, for example, leader-boards & badges.


You are Bob, a student working at a security company that researches cyber-attacks. You recently started working there and this is your first real assignment.

It is a chilly Tuesday morning when you find yourself at a large office building entrance. Above you, the windows of the highrise stretch themselves towards the sky. A chilly breeze of wind passes by your neck and you shudder. You hear the cough of your companion next to you.

Fig. 6. Example of a frame in the game.

The game was built in Twine [17]. Twine is an engine that lets one build adventure games using cards. As seen in Figure 8, the cards are connected. Each connection represents a transition between cards in the game logic. Each card is a frame which comprises an image, some text, and one or more buttons to switch between frames. This can be seen in Figure 6. The images helped build a mood or aesthetic for the scene they were shown in. They were also used to give a face to all the characters, such as seen in Figure 7. In the end, someone can export the story created with Twine into an HTML file that is ready for use.



Next to you is Robert, one of the more senior specialists at the company.

Robert: "Now remember Bob, I am only here to observe you today. I expect you to lead the investigation and will only step in if I see you make any big mistakes. This is your time to prove yourself, do not make me take over."

Robert: "Are you ready to go in?"

Let's go

Fig. 7. Example of a frame showing a character.

The story was designed using Thorndyke's (1977) framework for creating simple stories. It has been divided into different sections which Thorndyke calls episodes. These episodes are comprising a goal and a subset of other features. In the game, a combination of frames, such as the one shown in Figure 6, makes an episode. Each episode discusses a different aspect of the USB-based attack prevention. For example, one episode talks about how to handle unknown USBs.

In the story, a company has been attacked by a ransomware attack. The company has contained the attack and limit its effects. But, they do not know how their computer system got infected with the ransomware software. This is where the player comes in. They play as a young security researcher who has been called in to find the origin of the attack. With the player, there is a guide, someone who can correct the player and explain things to them. In the story, the guide watches the player and the decisions they make. Throughout the story, the player learns about what happened, how the attackers got in, and if there are more security risks. In the end, they need to reconstruct what they learned, and they can get one of 4 endings.

The story itself has a "trial" structure [29] with different endings. In this structure, the user has some challenges to overcome and alternate paths they can take, but they follow one story. A comparison of the structure of part of the story and the trial structure can be found in Figure 8. Every card in the story is comparable to hexagons in the structure above. In the story, the challenges allow the game to test the user on what they learned, and the alternate paths allow the user some agency. Where this game differs is in using alternate endings. In trial games, usually the story is of a railroad structure, where it leads down a path to one end. In this game's ending, the user is told how many mistakes they made in the game and this influences the ending.

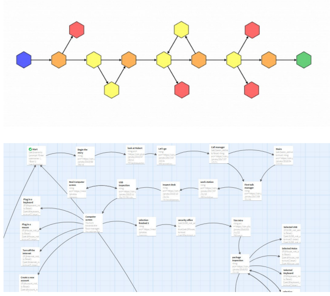
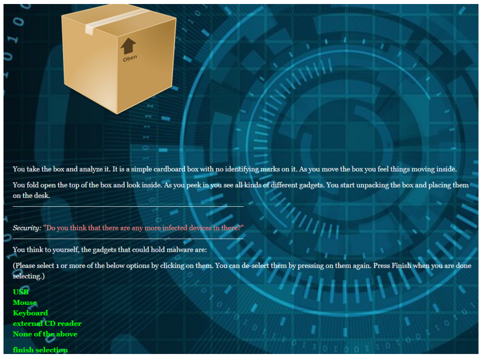


Fig. 8. Comparison of the trial structure VS story [29].

During the literature review, several aspects were identified that could be implemented in a story-based game. First off, one can discuss the interweaving of the information and the story. Several of the reviewed pieces of literature mentioned the importance of fully integrating the information in the story [37][31]. For example, in the game, there is a direct link between the USB-based attack knowledge and the mystery in the story. This is helped by making the story simulation-like, where it shows a scenario that could happen in the real world [37] [7]. All the tasks that are present in the game are endogenous and are narratively linked to the game [38]. For example, having to select which hardware could be infected so that the company might not get into trouble again, as seen in Figure 9. For spreading information, both a "guide" and the embedded narrative were used. They help them if they make mistakes, and are a driving force behind the action. The information provided is as wide as possible, with general useful information [31].



You take the box and analyze it. It is a simple cardboard box with no identifying marks on it. As you move the box you feel things moving inside.

You fold open the top of the box and look inside. As you peek in you see all kinds of different gadgets. You start unpacking the box and placing them on the desk.

Security: "Do you think that there are any more infected devices in there?"

You think to yourself, the gadgets that could hold malware are:

(Please select 1 or more of the below options by clicking on them. You can de-select them by pressing on them again. Press Finish when you are done selecting.)

USB
Mouse
Keyboard
external CD reader
None of the above

finish selection

Fig. 9. Example of a frame where users have to overcome a challenge.

How the story was built and structured is based on the literature review results. It combines enacted and emergent narrative [31]. Some set sequences of interactions are used for exposition, especially at the start of the game, which resembles enacted narrative. Later on, the user gets to make choices and can influence the story, which leans more towards an emergent narrative. Inside the story, the information used is a combination of declarative and procedural knowledge [5]. There is a focus on how to avoid attacks and detect them.

Some things are different compared to previous work. This game has more emphasis on the story part. Other research has story-based as an extra focus or implements other known features. The improvement points mentioned in the other games are picked up on and implemented . For example, in [37] it was mentioned that the game and material should be integrated with the game. This gamification does not have a focus on the gamer types out there. The goal was to create a general game and see how the story-based gamification performs for general students. Also the format differs from other games. This game falls close to the interactive novel genre. Others leaned away from the story and tried to do more surrounding the game.

4.2 Research Deployment

As mentioned before, the game is web-based. It has been hosted on a website and made so that only people with a link can access it. The game contains all relevant links to the consent form and surveys. So, when distributing the game and asking people to take part, only the link to the game had to be sent.

To test the effectiveness of the game, two surveys have been created. The first had to be filled in before the game is played, called the pregame survey, and the second one after the game is played, the post-game survey. These surveys were analyzed with the use of qualitative analysis and a one-sided t-test for a one-sample case and a Wilcoxon Signed Rank Test [26][27][36]. While the one-sided t-test is normally used for continuous data, it can be used for low amounts of discrete data [3]. Below are the links to the two surveys:

- pre-game survey: https://qfreeaccountssjc1.az1.qualtrics.com/jfe/form/SV_bgh9wuCLVPV9K7k
- post-game survey: https://qfreeaccountssjc1.az1.qualtrics.com/jfe/form/SV_39rz7RJECQRYs5g

The pre-game survey focuses on getting an idea of the knowledge that the participant already has on the topic. So, for example, they are asked what their study is and what they think their level of security knowledge is.

The post-game survey focuses on the perceived effectiveness of gamification. For example, how much do they think the game engaged them, how much did they learn, and how does it relate to any previous gamifications they have done? This is done using a Likert scale of 5 points. Participants are shown some statements and have to state how much they agree. The answers they can give are as follows.

- Completely disagree
- Partly disagree
- Neither disagree nor agree
- Partly agree
- Completely agree

The surveys have been designed according to frameworks for testing the effectiveness of gamification [21][40].

5 RESULTS & DISCUSSION

In the following section, the results of the surveys will be shown. The discussion section then relates the results of the literature review and empirical research to the research questions.

5.1 Evaluation of the game

First, the pre-game survey will be presented. Figure 10 shows the different fields of study participants come from. About 59%, are from fields that focus on the creation and use of technology, which is also reflected in how participants rate their technical knowledge. As seen in Figure 11, most participants rated their technical knowledge to be above average. In terms of perceived cyber-security knowledge, a more even spread between average and above-average knowledge can be seen, as seen in Figure 12

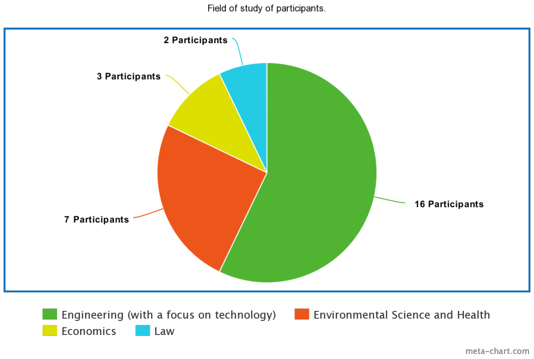


Fig. 10. Pie chart showing distribution of studies among participants.

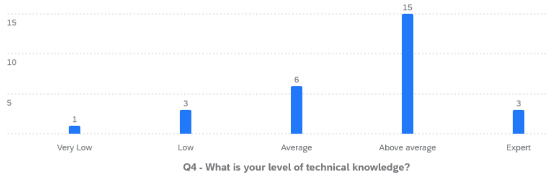


Fig. 11. Distribution in perceived technology knowledge

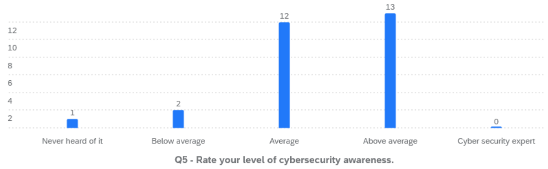


Fig. 12. Distribution in perceived cyber-security knowledge

In terms of USB-based attacks, perceived knowledge was found to be the following. A majority of participants were aware of the attack and showed safe behavior in USB usage. However, for one situation unsafe behaviour was shown. About 50% of participants stated they use the same USB for work and private purposes. Further, in terms of previous training experience, a majority was never trained in cyber-security and only half ever partook in a gamified training.

Next up, the focus will be on the post-game survey. Overall, the participants stated that the game helped them understand USB-based attacks more and caused a positive effect . This is seen in Figures 13 & 14

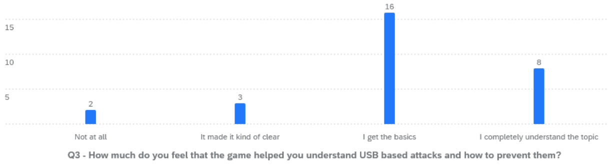


Fig. 13. Perceived increase in USB-based attack knowledge.

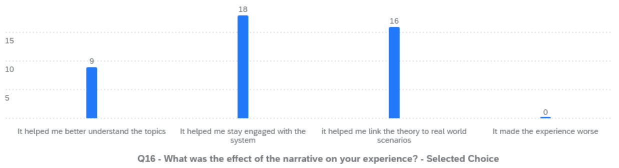


Fig. 14. Perceived effect of the story.

The post-game survey also contained more specific questions which relate to elements used to measure gamification effectiveness [21][40]. And to rate them, a scoring system as shown below was setup.

- Completely disagree = -2
- Partly disagree = - 1
- Neither disagree nor agree = 0
- Partly agree = 1
- Completely agree = 2

This was then used to calculate an average score, where a score greater than 0 shows a positive effect. On this data, a single-sided t-test was performed, as well as a Wilcoxon Signed Rank Test. The results are in table 1. Here, the null hypothesis is that there is no noticeable positive effect on the specified element. So, a mean score of 0 or lower on the scale. The t-test score for 27 participants, a power of 80%, an alpha of 0.05, and degrees of freedom of 26, is 1.71. And for the Wilcoxon Signed Rank Test, the value is 117. Now, as seen, 1, all the mean scores are positive and pass the t-test.

Table 1. Overview of the average score per question.

element	score	passes t-test	passes Wilcoxon
engagement	1.111	Y	Y
clarity	0.852	Y	Y
theory real-world link	1.482	Y	Y
increase in cyber-security knowledge	0.852	Y	Y
increase in USB-based attack knowledge	1.0	Y	Y
comparison with video	0.852	Y	Y

At the end of the survey, participants were asked about how this game compared to previous cyber-security and gamified training they had done. As seen in Figures 15 and 16, it was said to be better than other cyber-security training and just as good as other gamified trainings. In both cases, not enough participants could compare the game to training to do significance testing.

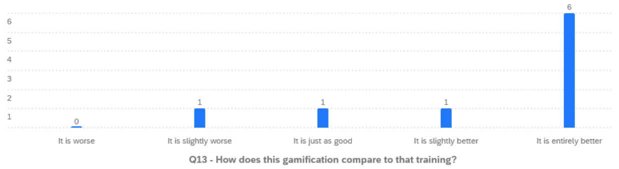


Fig. 15. Comparison of this game and other cyber-security training

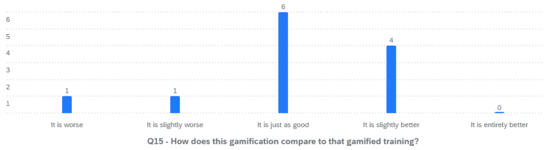


Fig. 16. Comparison of this game and other gamified pieces of training.

In the end, both surveys were compared to see if there were relations. No difference in perceived effectiveness of the game was observed between participants with or without cyber-security training. As well as between people with or without past gamified training experience. This can be seen in Figure 17 as the distribution is almost the same for both groups.

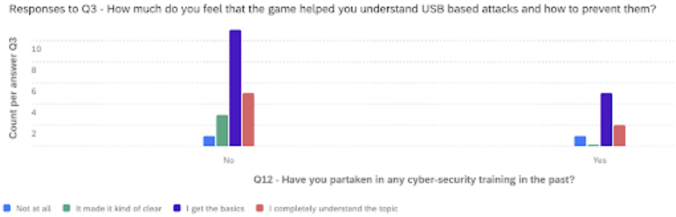


Fig. 17. Chart showing answers regarding USB-based attack understanding.

When comparing students who do (tech. student) or do not (non-tech. student) do a technical study, the following was observed. As seen in Figure 2, non-tech. students score the game higher, except on engagement.

Table 2. Overview of difference average score.

element	score non-tech. student	score tech. student
engagement	0.926	1.322
clarity	1.214	0.5
theory real-world link	1.641	1.362
increase in cyber-security knowledge	1.147	0.604
increase in USB-based attack knowledge	1.438	0.600
comparison with video	1.4	0.304

5.2 Discussion

This section will go over the results and relate them to the sub-research questions.

First off, the results of the literature review will be used to discuss sub-research question 1. There are a few concepts that influence the effectiveness according to the literature review.

- Choose a story-design framework that works well for the goal of your game [49][5].
- Have a clear connection between the story, and training information [37][31].
- Use the correct narrative types [31].
- Balance the use of analogies and realism of the story to both engage the participant and have them see the connection to the real world [31][7][38].

- Make sure that the type of information presented fits the target audience [5][31].
- Present information in such a way that they become linked to actions in the game [37][31][38].
- Find a correct balance between agency and forced sequences to give the users' background information [38][31].

There doesn't seem to be a specific way of implementing these concepts that works for all story-based gamifications. For example, a balance of analogy and realism is something that will differ per game [31]. This means that there are also concepts that were not relevant for the papers in the literature review, but that still might influence effectiveness. So this answer is likely not all encompassing.

To answer sub-research question 2, the concepts mentioned above were implemented as follows. For the initial design of the story, Thorndyke's structure was chosen as it improves story-element memorization by readers [49]. The story tries to simulate what could happened in the real world and makes very little use of analogies. The user needs to be relate the information to the real world and use it there [31][38]. Information that is presented in the game is broad and a combination of declarative and procedural knowledge because users need to know what to do to avoid attacks and what common attack patterns are [5]. Because of the simulation-like nature, all the tasks in the game are directly related to the narrative [38]. Seeing that the game needs to provide information to all users, the agency was limited. If the user is given a lot of freedom in a true sandbox experience, they might not see all parts of the game and might miss information [31]. Hence enacted and emergent narrative were used [31].

To answer sub-research question 3, the results from the surveys will be used. As seen in Figures 1314, participants found the game overall had a positive effect. Now, by looking into the results in Figure 1, a more in-depth analysis can be done. For all the measures of effectiveness, a positive effect can be noticed. And for all of those results, there is a one-sided t-test and the Wilcoxon test was passed. So it is possible to say that these are significant results[26][27]. Based on this, it is possible to state that overall story-based gamification is perceived to have a positive effect on USB-based attack prevention training. No real differences were found between different participants, except based on studies. The results for the measures of effectiveness divided up between technical and non-technical students are shown in Figure 2. Here, it is possible to see that overall, non-technical students perceived the game to be more effective, except for engagement. However, there are not enough people in both groups for a two-sample t-test or Wilcoxon test [46].

6 CONCLUSION & FUTURE WORK

6.1 Conclusions

As there is an increase in USB-based attacks, it is important to understand its perceived effectiveness of story-based gamification in their prevention. By doing a literature review on past paper, it was found that several aspects affect the effectiveness of story-based gamification. These include the story design framework, which information is presented in what way, narrative types, and balancing agency levels. These concepts were then used to design a game to teach people about USB-based attacks. It was found that for USB-based attacks; it is important to firmly root the story in reality. This way, it is easy for the participant to use the information in real life. Actions were directly linked to the story, so that users can learn for real scenarios. For narrative, it was used as set sequences to get the information across, limiting some agency. This way, all participants get all the information.

This game was tested in an empirical study. It was found that the participants overall perceived the training to have a positive effect. The same can be said on individual elements, such as engagement. When looking at individual differences between participants and the results, only one thing of note was found. Non-technical students were more engaged with the game, but also more critical. However, it is unknown if the difference was significance.

Finally, by combining the answers for all the sub-research questions, the overarching research question can be answered. This gamification has a positive impact on USB-based cyber-attack prevention when tested among students.

6.2 Limitations

Several limitations have affected the research. One of the first limitations to be identified is the influence that the analysis of previous research. These papers might have influenced how this paper was shaped and the conclusions. The second limitation is how comparison to other training was done. Because no other training could be found that goes this far into USB-based attacks, there was a reliance on the participants' experience. Third, the field of cyber-security is constantly changing and updating. The research and concepts that this research is based on might not be relevant anymore tomorrow. Another limitation is the topic on which this research is based. The knowledge gap for story-based gamification goes beyond this sub-topic focused on in this paper. The effects of this type of gamification might be different for different topics. There are also some limitations with how the measurements have been done. People took the surveys and played the game at home without supervision. Hence, it is difficult to do quality insurance and some things might not have been measured.

6.3 Future work

In the future, more research can be done on the effectiveness of gamification on other cyber-security topics. Another interesting thing to look at would be to get more students, to further look at the link with other gamified trainings and different backgrounds. And this also would show if there is a real difference as was observed. And finally, seeing as there are a lot of factors that affect story-based gamification, perhaps a more standard framework for how to apply a story in gamification can be created.

ACKNOWLEDGMENTS

The author would like to thank Wessel van Haarlem, Ziga Jug, and Remi Heeres for testing the game during the development. And he would like to thank Dr. Dipti K. Sarmah for supervising and reviewing the research.

REFERENCES

[1] ACM/SIGSAC. 2021. Acm css 2021. (2021). https://www.sigsac.org/ccs/CCS2021/.

[2] Mackenzie Adams and Maged Makramalla. 2015. Cybersecurity skills training: an attacker-centric gamified approach. *Technology Innovation Management Review*, 5, (January 2015), 5–14. issn: 1927-0321. doi: http://doi.org/10.22215/timreview/861. http://timreview.ca/article/861.

[3] Admin. 2019. Can i use parametric analyses for my likert scales? a brief reading guide to the evidence-based answer. (April 2019). https://lindeloev.net/can-i-use-parametric-analyses-for-my-likert-scales-a-brief-reading-guide/.

[4] Faisal Alotaibi, Steven Furnell, Ingo Stengel, and Maria Papadaki. 2016. A review of using gaming technology for cyber-security awareness. *International Journal for Information Security Research*, 6, 2, (June 2016). doi: 10.20533/ijisr.2042.4639.2016.0076. https://doi.org/10.20533/ijisr.2042.4639.2016.0076.

[5] Michael B. Armstrong and Richard N. Landers. 2017. An evaluation of gamified training: using narrative to improve reactions and learning. *Simulation & Gaming*, 48, 4, (May 2017), 513–538. doi: 10.1177/1046878117703749. https://doi.org/10.1177/1046878117703749.

[6] Marc Brysbaert. 2019. How many participants do we have to include in properly powered experiments? a tutorial of power analysis with reference tables. *Journal of Cognition*, 2, 1. doi: 10.5334/joc.72. https://doi.org/10.5334/joc.72.

[7] Tom Chothia, Sam Holdcroft, Andreea-Ina Radu, and Richard J. Thomas. 2017. Jail, hero or drug lord? turning a cyber security course into an 11 week choose your own adventure story. In *2017 USENIX Workshop on Advances in Security Education (ASE 17)*. USENIX Association, Vancouver, BC, (August 2017). https://www.usenix.org/conference/ase17/workshop-program/presentation/chothia.

[8] Merijke Coenraad, Anthony Pellicone, Diane Jass Ketelhut, Michel Cukier, Jan Plane, and David Weintrop. 2020. Experiencing cybersecurity one game at a time: a systematic review of cybersecurity digital games. *Simulation & Gaming*, 51, 5, (June 2020), 586–611. doi: 10.1177/1046878120933312. https://doi.org/10.1177/1046878120933312.

[9] Alexis Le Compte, David Elizondo, and Tim Watson. 2015. A renewed approach to serious games for cyber security. In *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace*. IEEE, (May 2015). doi: 10.1109/cycon.2015.7158478. https://doi.org/10.1109/cycon.2015.7158478.

[10] 2022. Conference top publications ratings. (2022). https://scholar.google.nl/citations?view_op=top_venues&hl=en&vq=eng_computersecuritycryptography.

[11] CISS Derek E. Brink. 2017. SECURITY AWARENESS TRAINING: SMALL INVESTMENT, LARGE REDUCTION IN RISK. Technical report. Proofpoint, Wombat.

[12] Indrel Doney. 2019. Research into effective gamification features to inform e-learning design. *Research in Learning Technology*, 27, 0, (January 2019). doi: 10.25304/rlt.v27.2093. https://doi.org/10.25304/rlt.v27.2093.

[13] Duolingo. 2012. Learn a language for free. (June 2012). https://www.duolingo.com/.

[14] Egress. 2021. Insider Data Breach Survey 2021. Technical report. Egress.

[15] Matthew Farber. 2015. Interactive fiction in the classroom. (April 2015). https://www.edutopia.org/blog/interactive-fiction-in-the-classroom-matthew-farber.

[16] F. Faul, E. Erdfelder, A.G. Lang, and A. Buchner. 2020. Gpower. (March 2020). https://www.psychologie.hhu.de/arbeitsgruppen/allgemeine-psychologie-und-arbeitspsychologie/gpower.

[17] Interactive Fiction Technology Foundation. [n. d.] Twine is an open-source tool for telling interactive, nonlinear stories. (). http://twinery.org/.

[18] Marina Fridin. 2014. Storytelling by a kindergarten social assistive robot: a tool for constructive learning in preschool education. *Computers & Education*, 70, (January 2014), 53–64. doi: 10.1016/j.compedu.2013.07.043. https://doi.org/10.1016/j.compedu.2013.07.043.

[19] Federico Griscioli, Maurizio Pizzonia, and Marco Sacchetti. 2016. USBCheckIn: preventing BadUSB attacks by forcing human-device interaction. In *2016 14th Annual Conference on Privacy, Security and Trust (PST)*. IEEE, (December 2016). doi: 10.1109/pst.2016.7907004. https://doi.org/10.1109/pst.2016.7907004.

[20] Headspace. 2014. Meditation and sleep made simple - headspace. (June 2014). https://www.headspace.com/.

[21] Johan Högberg, Juho Hamari, and Erik Wästlund. 2019. Gameful experience questionnaire (GAMEFULQUEST): an instrument for measuring the perceived gamefulness of system use. *User Modeling and User-Adapted Interaction*, 29, 3, (February 2019), 619–660. doi: 10.1007/s11257-019-09223-w. https://doi.org/10.1007/s11257-019-09223-w.

[22] Annette Jäckle and Peter Lynn. 2008. Respondent incentives in a multi-mode panel survey: cumulative effects on nonresponse and bias. *Survey Methodology*, 34, (January 2008), 105–117.

[23] Karl M Kapp. 2013. *The gamification of learning and instruction fieldbook*. en. John Wiley & Sons, Nashville, TN, (November 2013).

[24] Joakim Kävrestad, Allex Hagberg, Marcus Nohlberg, Jana Rambusch, Robert Roos, and Steven Furnell. 2022. Evaluation of contextual and game-based training for phishing detection. *Future Internet*, 14, 4. issn: 1999-5903. doi: 10.3390/fi14040104. https://www.mdpi.com/1999-5903/14/4/104.

[25] Jonna Koivisto and Juho Hamari. 2019. The rise of motivational information systems: a review of gamification research. *International Journal of Information Management*, 45, (April 2019), 191–210. doi: 10.1016/j.ijinfomgt.2018.10.013. https://doi.org/10.1016/j.ijinfomgt.2018.10.013.

[26] Wayne W. LaMorte. 2021. Module 7 - comparing continuous outcomes. (October 2021). https://sphweb.bumc.bu.edu/otlt/MPH-Modules/PH717-QuantCore/PH717-Module7-T-tests/PH717-Module7-T-tests4.html.

[27] Wayne W. LaMorte. 2017. Wilcoxon signed rank test. (May 2017). https://sphweb.bumc.bu.edu/otlt/mph-modules/bs/bs704_nonparametric/BS704_Nonparametric6.html.

[28] Ana Manzano-León, Pablo Camacho-Lazarraga, Miguel A. Guerrero, Laura Guerrero-Puerta, José M. Aguilar-Parra, Rubén Trigueros, and Antonio Alias. 2021. Between level up and game over: a systematic literature review of gamification in education. *Sustainability*, 13, 4. issn: 2071-1050. doi: 10.3390/su13042247. https://www.mdpi.com/2071-1050/13/4/2247.

[29] Albert van der Meer. 2019. Structures of choice in narratives in gamification and games. (September 2019). https://uxdesign.cc/structures-of-choice-in-narratives-in-gamification-and-games-16da920a0b9a.

[30] Tobias Mueller, Ephraim Zimmer, and Ludovico de Nittis. 2019. Using context and provenance to defend against USB-borne attacks. In *Proceedings of the 14th International Conference on Availability, Reliability and Security*. ACM, (August 2019). doi: 10.1145/3339252.3339268. https://doi.org/10.1145/3339252.3339268.

[31] Scott Nicholson. 2014. A RECIPE for meaningful gamification. In *Gamification in Education and Business*. Springer International Publishing, (October 2014), 1–20. doi: 10.1007/978-3-319-10208-5_1. https://doi.org/10.1007/978-3-319-10208-5_1.

[32] Torsten Reiners and Lincoln C. Wood, editors. 2015. *A recipe for meaningful gamification. Gamification in Education and Business*. Springer International Publishing, Cham, 1–20. isbn: 978-3-319-10208-5. doi: 10.1007/978-3-319-10208-5_1. https://doi.org/10.1007/978-3-319-10208-5_1.

[33] J.G.W. Nijland. 2022. Gamification of cyber security awareness training for phishing against university students. (February 2022). http://essay.utwente.nl/89424/.

[34] Nir Nissim, Ran Yahalom, and Yuval Elovici. 2017. USB-based attacks. *Computers & Security*, 70, (September 2017), 675–688. doi: 10.1016/j.cose.2017.08.002. https://doi.org/10.1016/j.cose.2017.08.002.

[35] Nir Nissim, Ran Yahalom, and Yuval Elovici. 2017. Usb-based attacks. *Computers & Security*, 70, 675–688. issn: 0167-4048. doi: https://doi.org/10.1016/j.cose.2017.08.002. https://www.sciencedirect.com/science/article/pii/S0167404817301578.

[36] Geoff Norman. 2010. Likert scales, levels of measurement and the "laws" of statistics. *Advances in Health Sciences Education*, 15, 5, (February 2010), 625–632. doi: 10.1007/s10459-010-9222-y. https://doi.org/10.1007/s10459-010-9222-y.

[37] Siobhan O'Donovan, James Gain, and Patrick Marais. 2013. A case study in the gamification of a university-level games development course. In *Proceedings of the South African Institute for Computer Scientists and Information Technologists Conference on - SAICSIT '13*. ACM Press. doi: 10.1145/2513456.2513469. https://doi.org/10.1145/2513456.2513469.

[38] Nathan R. Prestopnik and Jian Tang. 2015. Points, stories, worlds, and diegesis: comparing player experiences in two citizen science games. *Computers in Human Behavior*, 52, (November 2015), 492–506. doi: 10.1016/j.chb.2015.05.051. https://doi.org/10.1016/j.chb.2015.05.051.

[39] Proofpoint. 2022. State of the Phish. Technical report. Egress.

[40] S. Ros, S. González, A. Robles, LL. Tobarra, A. Caminero, and Jesus Cano. 2020. Analyzing students' self-perception of success and learning effectiveness using gamification in an online cybersecurity course. *IEEE Access*, 8, 97718–97728. doi: 10.1109/ACCESS.2020.2996361.

[41] Michael Sailer and Lisa Homner. 2019. The gamification of learning: a meta-analysis. *Educational Psychology Review*, 32, 1, (August 2019), 77–112. doi: 10.1007/s10648-019-09498-w. https://doi.org/10.1007/s10648-019-09498-w.

[42] Ana Cláudia Guimarães Santos, Wilk Oliveira, Juho Hamari, Luiz Rodrigues, Armando M. Toda, Paula T. Palomino, and Seiji Isotani. 2021. The relationship between user types and gamification designs. *User Modeling and User-Adapted Interaction*, 31, 5, (August 2021), 907–940. doi: 10.1007/s11257-021-09300-z. https://doi.org/10.1007/s11257-021-09300-z.

[43] Ethics Committee Computer & Information Science. 2022. Ethics committee: faculty of electrical engineering, mathematics and computer science (eemcs). (June 2022). https://www.utwente.nl/en/eemcs/research/ethics/.

[44] Eleanor Singer and Cong Ye. 2012. The use and effects of incentives in surveys. *The ANNALS of the American Academy of Political and Social Science*, 645, 1, (November 2012), 112–141. doi: 10.1177/0002716212458082. https://doi.org/10.1177/0002716212458082.

[45] LexisNexis Risk Solutions. 2022. LexisNexis Risk Solutions biannual Cybercrime Report. Technical report. LexisNexis Risk Solutions.

[46] 2022. Spss tutorials: independent samples t test. (June 2022). https://libguides.library.kent.edu/spss/independentttest.

[47] 2022. Take the cyber security course and learn whether your data is protected properlyut launches e-learning courses on new security education platform. (May 2022). https://www.utwente.nl/en/service-portal/services/lisa/news-events/news-events/news/2021/10/35194/take-the-cyber-security-course-and-learn-whether-your-data-is-protected-properly#e-learning-programme-inventory-and-exercises.

[48] Jeremiah Talamantes. [n. d.] Usb drop attacks: the danger of. (). https://www.redteamsecure.com/blog/usb-drop-attacks-the-danger-of-lost-and-found-thumb-drives.

[49] Perry W. Thorndyke. 1977. Cognitive structures in comprehension and memory of narrative discourse. *Cognitive Psychology*, 9, 1, (January 1977), 77–110. doi: 10.1016/0010-0285(77)90005-6. https://doi.org/10.1016/0010-0285(77)90005-6.

[50] Matthew Tischer, Zakir Durumeric, Sam Foster, Sunny Duan, Alec Mori, Elie Bursztein, and Michael Bailey. 2016. Users really do plug in USB drives they find. In *2016 IEEE Symposium on Security and Privacy (SP)*. IEEE, (May 2016). doi: 10.1109/sp.2016.26. https://doi.org/10.1109/sp.2016.26.

[51] Indiana University. 2018. What is usb? (January 2018). https://kb.iu.edu/d/afad.

[52] 2019. Usb baiting: don't take the bait: inspired elearning resources. (October 2019). https://inspiredelearning.com/resource/usb-baiting-dont-take-bait/.

[53] Jennifer R. Whitson. 2013. Gaming the quantified self. *Surveillance &amp; Society*, 11, 1/2, (May 2013), 163–176. doi: 10.24908/ss.v11i1/2.4454. https://doi.org/10.24908/ss.v11i1/2.4454.

[54] Gabe Zichermann and Christopher Cunningham. 2011. *Gamification by design: Implementing game mechanics in web and mobile apps*. O'Reilly Media.