Immersive VR cybersecurity training for physical and technical cyber threats in the healthcare sector

Sven Sonneveld

Supervisor: Dr. ir. R.W. van Delden,
Critical observer: Dr. J.H. Bullee
Bachelor Graduation Project for Creative Technology, University of Twente
Jul 5, 2024

Table of Contents

1. Introduction

Recently a successful cyberattack had stolen 23.6 million euros from a company in Hong Kong. A financial worker had received a message that they needed to make a money transfer. They were initially suspicious of it and had assumed it was a phishing attempt. However, after taking part in a multi-person video conference, where there were several colleagues and the chief financial officer present, the financial worker transferred the money. It turned out that everyone except himself during the conference was faked and that the phishing attempt was successful. The damages for this was 200 million Hong Kong dollars, or around 23.6 million euros (Chen & Magramo, 2024).

Cyber threats are always changing and because of this cybersecurity also needs to be improved to keep up. Cybersecurity however has many links which all need to be strong for digital data to be secure, because with 1 point of failure data can already be lost to those trying to get access to it. The weakest link in cybersecurity is people (Khatari, 2023), which is an important and also difficult link to improve. This is because it is time-consuming to train people. There are also many training methods and they all vary in effectiveness. They also need to be taught about cybersecurity practices as it is constantly evolving to keep up with the best practices. An effective method found to help teach people about cybersecurity is VR (Klooster, 2022). They have found that the use of VR cybersecurity training had shown a significant increase in the average cybersecurity performance.

In sectors with sensitive data, like the healthcare sector, this is especially prevalent as the importance of keeping this data as secure as possible. The data from the healthcare sector would contain private medical data that would be important for the patients and employees to keep secure. This is because such private medial data could be exploited by malicious actors and could cause harm to the patient. An example for this could be a contreversial medical procedure, which could affect the patient when this information gets released. A successfull cyberattack would also impact the functioning of the hospital, which could negatively impact the current patients that need medical attention. While the results from this cybersecurity training would be best applicable to the healthcare sector, where the amount of data security should be as high as possible, it would also apply to other sectors where the expected level of data security can be less stringent.

With this in mind the following research question can be asked: "*How could a VR experience be made to be able to help train healthcare employees to be more aware of the cybersecurity aspect of their actions to minimize physical and technical cyberthreats?"*

This question can be subdivided into several smaller sub-questions, which are:
sRQ 1: What are commonly found cyber threats in the healthcare sector?
sRQ 2: What are the state-of-the-art cybersecurity training methods?
sRQ 3: What is the perceived effectiveness of the state-of-the-art cybersecurity training methods by experts?
sRQ 4: What method of training, positive or negative, would be more effective when used for cybersecurity training?
sRQ 5: What cybersecurity training method for VR?

sRQ 6: How much does the designed VR cybersecurity training help with training healthcare employees?
sRQ 7: How much do the different elements regarding the specification of the healthcare sector impact the perceived effectiveness of cybersecurity training?

This research starts with background research to try to obtain answers to these sub-research questions. This will be done in a literature research and this will be expanded upon with the use of expert interviews. After the literature review the design process will start. In this process the VR training experience will be developed and in the evaluation phase it will be tested.

2. Background research

To be able to answer the sub-research questions background knowledge is required. This is to find out what knowledge is already available through research. The background research will consist of a literature review and expert interviews. The literature review will try to answer the sub-research questions 1 and 2.

2.1 Background research

2.1.1 Different methods of cybersecurity training

There are many different possible methods to train people in cyber security. In the paper from Švábenský et al. (2020) a literature review was conducted and it was found that there are several different training methods are used. The most common methods made use of a form of hands-on learning or self-study. As the intent is to implement these methods in VR the focus will be on the hands-on learning methods and not the self-study. The top 3 mentioned training methods consist of Labs, exercises and practical assignments. An exercise could consist of writing down which characteristics they have been taught a secure password should have. The labs training method could consist of a person applying what they have learned in a practical situation (Chatmon et al., 2010). An example of this could be changing a password after having been taught what good requirements are for a password. If they have been taught to use multiple different kinds of letters, numbers and special characters they should be using them all in the labs assignment. A practical assignment could be changing a password of the trainee if it would not be considered to be secure according to the material taught. From Hatzivasilis et al. (2020) the top 3 mentioned training methods consists of seminars, simulations and workshops, which are all hands-on learning methods. Specifically mentioned are the educational processes, which would involve serious games, simulation and/or collaboration learning. With these educational methods several examples are given where a combination of the methods is used. An example of this would be a capture the flag (CTF) challenge, where a person or a team would need to find a piece of text, the flag, in given vulnerable software (Team, z.d.). Depending on how the CTF is organized and executed one or a combination of the mentioned educational processes will be applied. From Hatzivasilis et al. it was found that specifically the use of serious gaming is considered to be a generally positive when included into the learning process. This is as the participant would be able to become more familiar with cybersecurity in a relaxed manner. Furthermore, in Prümmer et al. (2023) different types of training methods are found in which cybersecurity training can be given. The top 3 most commonly found cybersecurity training methods are: game-based training, presentation-based training and simulation-based training. These categories of training methods could be used in combination with the previously mentioned training methods to have a final idea of how the cybersecurity training should be structured. From these training methods there is a similarity. For Švábenský et al. (2020) the three methods given are all hands-on training methods. While for Hatzivasilis et al. (2020) there is also a focus on background knowledge in combination with the hands-on training for the user to know what they are about to learn and to make use of it. With a combination of those ideas, where first a bit would be explained, and afterwards the explained content would be expanded

upon with a practical example. This would prompt the user for what is to come, which could cause them to make fewer mistakes in the practical part of the training. This part could consist of a serious game to simulate possible scenarios and consequences of performing the correct or incorrect actions. In Cain and Piascik (2015) it was found that well-designed serious games have been more enjoyable compared to lectures when used in higher education. While simulations or serious games are not mentioned in the top three of Švábenský et al. (2020) educational game was mentioned as the fourth option. The best possible training methods used in the context of cybersecurity training would be simulations and serious games, as. These two possible training methods will be further expanded upon.

2.1.2 Advantages and disadvantages of the training methods

The different cybersecurity training methods can have advantages and disadvantages. According to Prümmer et al. (2023) simulation-based training had positive feedback from the users. Chernikova et al. (2020c) found that simulation-based training would be advantageous as real scenarios where experience can be gained do not happen often. When these scenarios do happen any practice without systematic guidance can come with risk. If the situation is handled poorly the negative consequences of a successful cyberattack could have a real effect. In Chernikova et al. (2020c) it was also found that simulations have a positive effect on the development of complex skills. The positive effect of the skill development was increased with a higher simulation duration. In Al-Elq (2010) and Cant and Cooper (2009) physical simulations are discussed in the medical education. Both find that physical simulations have advantages. Cant and Cooper (2009) specified that these advantages depend on context and subject method. Al-Elq (2010) argues that a high-fidelity simulation can provide a unique experience. They found that the cost of the simulation increases with a higher fidelity. Virtual reality could be incorporated into the simulations, but this doesn't reach the required level of realism as this is set as an important requirement for the simulation. In Pohl et al. (2009) a simulation-based game was used, in which the goal was for students to learn more about sustainability. This simulation was made to be quite complex, which made it feel like an educational program. They had gotten feedback from the students it was difficult in the beginning, but became easier at the end. If this method would be used for the cybersecurity training it cannot be too complex. This is because the content would need to be easy to understand to be an effective training method. The need for high fidelity in a simulation is not necessarily needed for cybersecurity training. This is because the cybersecurity training would need to increase the awareness of the users who are being trained. While the actions of the user would have consequences when done poorly comparable to Al-Elq (2010) the focus of the cybersecurity training is not to train highly trained personnel but to increase the awareness of an average personnel in a company. This would mean the requirements for fidelity can be lowered compared to those discussed in the paper.

The use of serious gaming can have several advantages and some disadvantages. In Lunn et al. (2016) it was found that one of the advantages is that is that immediate feedback can be given to the user if a wrong action has been taken. This way the user can recognise the mistake they made and learn from it. In Chang et al. (2019) it was found that if the feedback would be given later it is also possible to accurately capture data regarding the actions taken and their possible consequences. This can even be done in a multiplayer setting, where a

person could pretend to be a hacker. An overview could be made when certain actions are taken and what the best response would have been. The overview could be used to see the performance of the user or by an investigator to check the average cybersecurity knowledge. However, there are also some disadvantages to the use of serious games. Also according to Chang et al. (2019) the serious game would need to be created in high-fidelity to be able to generalize the finding with the real world. This can be costly and time-consuming depending on how high the fidelity needs to be and how many different scenarios would need to be created. If the scenarios makes use of multiple menus, drop down menus and/or other computer-based interaction it would influence the immersion and functional fidelity. This could make the interaction with the serious game feel artificial and/or tedious. This could decrease the effectiveness of serious games. The disadvantages of serious gaming are not high. The high-fidelity problem can be partially solved by having the scenarios be in the same environment. This way only new scenarios need to be made, while the environment can be the same or similar. The disadvantages of having multiple menus can be mitigated by minimizing their amount during the development of the serious game. The advantages of serious gaming can work well when used in the context of cybersecurity training. Both immediate feedback and feedback, when it is finished, could help the user in improving their cybersecurity knowledge and awareness of their actions. With the precise data gathered on the actions taken, it would be easy to create a report on the specific cyber threats that would need more attention for each employee. If used in a multiplayer setting the training multiple people can be trained at the same time.

2.1.3 Conclusion

Several different training methods have been found, of which serious games and simulations are looked at in more detail. The advantages and disadvantages of both serious games and simulation are similar and also can be found in Table 1. With both methods rare occurrences can be simulated, like a cyberattack, and be experienced with no actual consequences if handled poorly. With both methods data on the actions of the user can be accurately taken and analyzed. For both methods a high fidelity would be preferable to make it comparable with real scenarios, which could be expensive and time-consuming depending on how high the requirement is set for the fidelity. The difference between the methods lies in the expected realism. With the serious games method a requirement is set for game elements present in the cybersecurity training method that will be developed. In the simulation-based training method the requirement would be to have these game elements absent, as it would need to be realistic. To determine which of the two methods is preferable would depend on the specific requirements of the target group of the cybersecurity training method. As these specific requirements can be different for each target group both the serious game and the simulation-based training methods could be viable options.

For this cybersecurity training the choice will be made to focus on serious games, because the focus will be on the training. The importance of the experience to the user will have a higher priority compared to the realism that the simulation-based training would bring. While simulation-based training could also be effective it is not where the focus of the training will be. If the cybersecurity training would be made as a test the simulation-based training should be used

with this argument as in the training the importance would be on the reaction of the user in a realistic scenario.

	Serious games	Simulation
Accurate action tracking	✔️	✔️
Simulate rare scenarios	✔️	✔️
No real consequences for mistakes	✔️	✔️
Focus on gamified experience	✔️	❌
Focus on accurate real scenarios	❌	✔️

Table 1, Advantages and disadvantages of serious games and simulation-based training

2.2 Expert interviews

To get the most accurate information regarding specific cybersecurity knowledge experts will be interviewed. However to minimize risk the information regarding the names and place of employment of the experts will be anonymized. The information gathered in the context of cybersecurity could potentially reveal unknown weaknesses. If an expert makes use of training method A, they might be more vulnerable to attacks that focus on vulnerabilities that are better prevented by using method B. Even if method A works as well as method B in preventing any vulnerabilities the perception of having a potential weakness could cause an increase in cyber attacks. To be able to minimize any potential risk and harm that the experts might be exposed to it is necessary that the knowledge of who the experts are be spread to as few people as possible. This means who the experts are will not be shared outside of the research team. The expert interview questions can be found in Appendix A

2.2.1 Expert Interview 1

From the expert interview, several points of interest are gathered. First, it was gathered that the focus of cybersecurity training should not be very specific. This is a detailed training method regarding one specific cyber threat that leaves holes in the gained awareness and knowledge of other possible cyberattacks. If there is a large focus on phishing other threats like unknown USB sticks or other threats and best practices. Second, they said that there are many phishing attempts each day using email, however there are email rules active to prevent most of them. The expert also mentioned when asked about spear phishing that it is difficult to filter out these emails, as they are made to perform a cyberattack on a specific individual. Some attacks, like ‘lost’ USB sticks are difficult to detect. They get handed in by the reception to lost and found in the event someone lost it. The expert does not get notified of this, which means it is not clear if attacks like these are commonly used. No real attempts have been made to get physical

access to restricted areas as most areas on the location of work of the expert is open. While there are not a lot of restricted areas the location of the servers of the company is one. It gets protected by several layers of defence. A test has been done to check the effectiveness of the defence, where the ‘attacker’ was able to gain access. However, the employee who had given access argued they knew it was a test and wanted to see what the ‘attacker’ would do. Regardless if this is true or not, it is bad practice to give access to those who are not authorized. Furthermore, the expert had advised that cybersecurity training is not something to do once. This is as the awareness of the cybersecurity aspect of the actions taken by employees decreases over time. The result of this is that cybersecurity training would need to be followed often to be effective.

2.2.2 Expert Interview 2

From the second interview several insights are gathered. According to the expert there are set standards for their information security they need to follow as a healthcare organisation, which are the ISO27101 and NEN7510. They make use of login credentials in combination with MFA when viewing or changing patient files from their work laptops. When logging in they also need to make use of their access card. This access card is an RFID card, specifically a MIFARE card. These MIFARE cards are all encrypted, however the level of encryption is different between their different possible RFID cards. The MIFARE access card needs to be used by the employees if they want to view or edit the patient files. This can be done with both their laptops and a central computer and the access is monitored to check if the employee should be able to access the patient’s files, as specified in the NEN7510. This access is monitored to be able to track an employee in the event they access a patient's files without a valid reason. The MIFARE access card is in addition to this also used to gain access to restricted areas, where employees only have access to the areas where they need to have access. When asked specifically about USB devices the expert answered by telling us that the USB ports on their devices are blocked in the bios. This causes the USB port to be unable to have any data transfer between the laptop or PC and the USB device. When the expert was asked about their opinion regarding the use of serious games against simulation they argued that serious games would be a better fit for training as it would be in a light-hearted manner. When asked about simulation-based training they had mentioned this would be a better fit for testing the effectiveness of the training, as in a simulation the scenarios would need to be as realistic as possible. This would give a clear result on how they, the person being tested, would react to a real scenario of a cybersecurity threat. The expert had also specifically mentioned to make the user feel at ease. This is because if something happens the user needs to notify IT as soon as possible if they, the user, thinks something is wrong. If the user would wait or not notify someone if they do think something is wrong the potential damages that could happen would be high. The attitude towards the user will need to be positive to be able to minimize the risk of the delay of the detection and actions against a potential cyberattack. The place where the export works is already making use of preventive measures to minimize the risk of a successful cyberattack. However, these measures can be perceived as annoying by the employees. To be able to make the user aware of why these measures are important it was mentioned by the expert that the results could be if these measures would be disabled, which would help create understanding for the users. Examples of

these preventive measures could be blocked USB ports and access cards with a clip to keep it with the user.

2.2.3 Conclusion of expert interviews

From these expert interview several points have been learned that help the development of the VR cybersecurity training. These points are that there is a need for RFID cards in hospitals. This is because it is used in the login process for employees and to gain access to restricted areas. The experts themselves make use of MIFARE cards, which are a type of RFID card with encryption. This makes it so that the MIFARE cards can be used in a setting where there is a focus on and a requirement for cybersecurity. While the MIFARE cards are safer to use compared to normal RFID cards because they are encrypted they are only secure to an extent, as the encryption can be broken. Some versions of MIFARE are already compromised and should not be in use because of this for anything requiring security. A few examples of these compromised versions are the MIFARE Classic (Courtois, 2009) and the MIFARE DESFire (Kasper et al., 2010). For both of these versions, it is possible to break the encryption and copy the content of the MIFARE card, which would make them insecure. It was also mentioned by the expert that the USB ports are blocked on the devices the employees use to log in and potentially access patient files. However, there is still a chance some USB ports are not blocked. Should the central PC make use of the mouse and keyboard there need to be some USB ports not blocked, otherwise the mouse and keyboard would not work. Should a ‘lost’ USB stick be found it could be used by an employee to plug in a computer. Even if it doesn’t work and the computer doesn’t get hacked they might bring it to the general reception as lost and found. This would make it difficult for IT to know about these kinds of attacks, where one might fall through the cracks and have the cyberattack be successful. To improve the cybersecurity of this potential weakness the swiss cheese cybersecurity model needs to be used (Shabani et al., 2023). In this model failures, weaknesses or in the cybersecurity measures are represented as holes, where each slice represents a layer of defense. With multiple layers of defense, which get represented as multiple slices of cheese, more of the holes in the slices of cheese gets covered. Meaning with multiple layers of defense each layer contributes by mitigating the weaknesses of other layers, which would result in a higher amount of effective cybersecurity compared to each individual layer of defense.

In addition to this, the experts also mentioned keeping the experience of the user in mind when designing and creating the VR cybersecurity training for them. The users do not need to be made afraid of making mistakes and being afraid of possible consequences. If they are the employee could delay notifying IT or the personnel responsible for fixing these kinds of issues, which could result in higher potential damages for their place of employment. It was specifically mentioned that employees who make mistakes and do notify IT should be welcomed and received as positively as possible to make sure they and other employees do not delay notifying IT in the future.

2.3 State of the art training methods

Looking at different state-of-the-art VR cyber security training methods to see what they did well and what they could do better.

2.3.1 CiSE-ProS

CiSE-ProS (Seo et al., 2019) is created with a high focus on training students about the physical side of cybersecurity. The user would need to find and replace faulty equipment in a data center as can be seen in figures 1, 2 and 3. While this would be interesting for some groups of users it is not very relatable to the knowledge needed for the average healthcare employee.

Figure 1, from CiSE-ProS locate rack B5

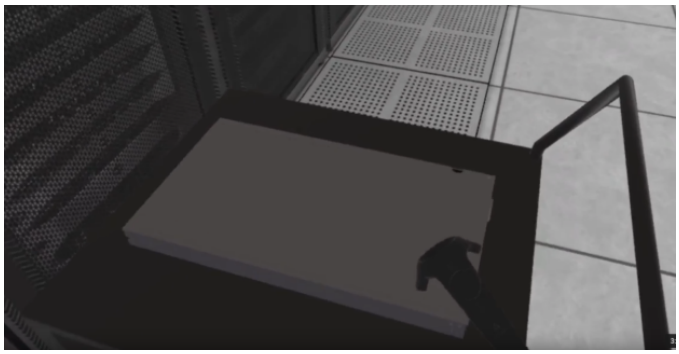


Figure 2, from CiSE-ProS place faulty node on cart

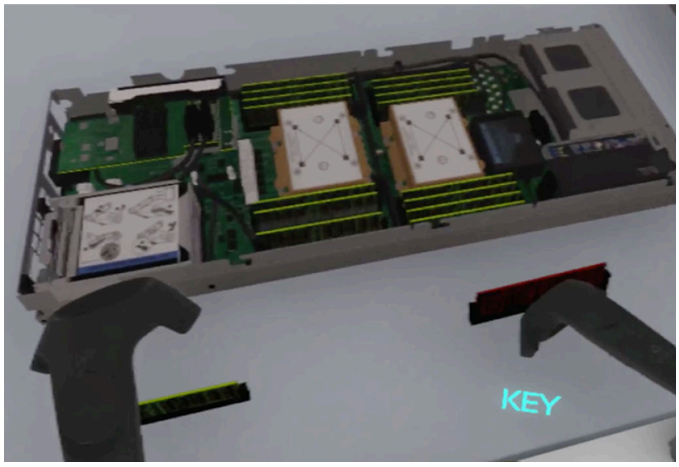


Figure 3, from CiSE-ProS replace defective component

2.3.2 Infosequre - Security awareness game

Infosequre (*Security Awareness Game | Infosequre*, n.d.) is a company that created a VR escape room game called Security Awareness Game to train employees about cybersecurity. They are a company that already makes use of VR cybersecurity training and other non-VR cybersecurity training methods. They do not mention what different topics of cybersecurity they will train and how many different topics.

2.3.3 Conclusion

Of these state-of-the-art training programs Infosecure is already a commercial company, which also is making use of VR technology. This shows there is a market available and a possibility for the adaptation of VR in cybersecurity training. This means people are open to different cybersecurity training methods and that there is a chance for VR cybersecurity training to be used in the healthcare sector. CiSE-ProS looks very immersive and engaging, which can be seen from the quotes given by the students who have made use of this cybersecurity training. Their approach to training cybersecurity is proven by themselves to be effective, which could be looked at while developing the VR cybersecurity training.

For infosecure not clear what topics are used to train people. This could be by design to not disclose their used cybersecurity topics to make sure any potential weaknesses of topics not used in cybersecurity training gets leaked. Could potentially be assumed all topics will be discussed, but this is unrealistic as there too are many different topics to fit in a concise cybersecurity training. For CiSE-ProS the only focus is on the physical access, specifically for datacenters. With this specialization other potential cyberattacks could be a risk if only making use of CiSE-ProS. Other cybersecurity training would need to be used in addition to CiSE-ProS to properly train someone.

The Security awareness game from Infosequre focuses on employees of companies, both larger and smaller companies. This is a very wide focus group, which means there is no specialization for the different work sectors. Different work sectors can have different needs for cybersecurity training. For the cybersecurity training CiSE-ProS the focus is on students on a career track towards STEM, which means science, technology, engineering, and math, fields for

the physical access of cybersecurity. CiSE-PRoS is specifically created to simulate a data centre, where the focus lies for this training. This user group is not comparable to general healthcare workers as they will have a different background experience and different needs for cybersecurity training.

The cybersecurity training that will be developed for this thesis will have a specific audience, which is the same as CiSE-ProS and different from what Infosequre does. It will also have multiple different cybersecurity topics, which is different from CiSE-ProS.

3 Methods and Techniques

In this chapter the choice for the design process will be explained. The chosen design process is the creative technology design process (Mader & Eggink, 2014). This design process was chosen as it is an iterative process, where the ideas will be refined and improved. This design process consists of four different phases, which are ideation, specification, realization and evaluation. Each of these phases makes use of a converging model, where it will start wide and will become narrower towards the end to end up with a final design. The four different phases will be expanded upon in the following paragraphs below.

3.1 Ideation

During the ideation phase many ideas for scenarios will be made with the use of brainstorming. With this the different possibilities will be written down and considered which will fit best considering the requirements that will be specified during the specification. During this phase the lotus blossom (Digital Society School, n.d. -a) and the wwwwwh (Digital Society School, n.d.-b) methods will be used. The lotus blossom method will be used to gain many different possible scenarios. And afterwards, the wwwwwh method will be used to get a few specific scenarios from all of the scenarios gained in the lotus blossom method. The requirements set from the wwwwwh method will be used in combination with the expert interviews to create the different scenarios that will be used in the VR cybersecurity experience. However, after using the wwwwwh method it becomes clear that this method would need to be used before other ideation methods to create specifications the following ideation method would follow. This means this ideation method doesn't work well when used after another ideation method with the intent for the specification of the generated ideas. In place of the wwwwwh method, the KJ method (Digital Society School, n.d.-c) will be used to generate ideas specifically for the results of the lotus blossom method. This method will be used in a group of people where different ideas will be generated and written down on post-its. Afterwards, all the ideas are shuffled around and read out loud, during which anyone can ask for clarification and afterwards the ideas are categorized into different groups. When all ideas are categorized the group will vote for the best ideas. After the KJ method will be used to generate ideas specifically for those generated using the lotus blossom method the storyboard ideation method (Digital Society School, n.d.-d) will be used to specify the ideas to a possible scenario. For each of the scenarios, a global storyline is written and afterwards, they are drawn to convey the important information of each scenario.

3.2 Specification

During the specification phase the functional and non-functional requirements will be specified. With the use of early prototypes, preliminary ideas will be tested to check different design choices. Expert interviews will be used to be able to specify which requirements are set by possible users. The interviews could result in the conclusion that a higher focus compared to the current state of the art is needed on specific threats. This would result in this training method

having a higher focus on these specific threats as there is a gap for the state-of-the-art methods for these specific user groups.

3.2.1 Functional requirements

The VR cybersecurity training needs to have several different functional requirements to for it to be defined as functional. These requirements are:

- The program shall be usable in combination with a VR headset, specifically for the Meta Quest 2.
- The program shall let the user walk around in the real world and with the use of their controllers.
- The program shall let the users be able to press buttons and grab objects with the use of their controllers.
- The program shall contain several different scenarios related to cybersecurity with the focus on physical and technical cybersecurity.

3.2.2 Non-Functional requirements

In addition to the functional requirements the VR cybersecurity training also needs several different non-functional requirements. These requirements are:

- The program should educate users on cybersecurity topic, specifically cybersecurity topic that are relevant for the healthcare sector.
- Parts of the objects in the environment of the program should contain elements that should be related to the healthcare sector.
- The experience should make use of serious games

3.2.3 Exploration of VR Platform

Many different possible platforms can be used to create a VR cybersecurity training program. Some of those possibilities are Unity, Unreal Engine or Resonite. Of these options, Resonite was chosen because of its ease of use. In Resonite it is very easy to quickly make prototypes in VR as those prototypes can directly be made with the use of VR. With Unity and Unreal Engine changes made in the environment when VR can be used are not saved and would need to be manually saved each time any changes are made. With Resonite all changes made with both VR and desktop mode can be saved with one button. Furthermore, Resonite can seamlessly switch between VR and desktop mode, which makes development where those different modes have the advantage easier. Resonite also has many different examples that can be used for inspiration and to look at how these examples work. These different examples are worlds created by other users, which can be visited and experienced. One of these examples is the protoflux community tutorial. In this tutorial, protoflux is explained with several different examples and challenges that need to be solved to progress through the tutorial. One of these challenges is an elevator that needs to be fixed for the user to go up the elevator. For this challenge, all the tools are given to solve it with an example of how it should be solved close by. Another example would be an earthquake training experience. This experience makes use of

audio, text, teleport points and more to teach the user what they should do during an earthquake. With examples like these, it became clear that a VR cybersecurity training is possible to be created in Resonite and should difficulties arise during the development it is possible to view and take inspiration from how others solved these challenges.

3.3 Realization

During the realization phase the final prototype design will be created for it to be tested. The final design should be according to the requirements set during the specification phase. The design will be created in Resonite and will contain multiple different examples of cyber threats or best practices to minimize cyber threats. Each example will have different elements, which consist of an introduction, a small game and a conclusion. The introduction can consist of an example of how the to-be-discussed cyberattack could be used or how the best practice can minimize the chance of a successful cyberattack.

3.4 Evaluation

In the evaluation phase the final prototype will be tested to see if all functional and nonfunctional requirements are met. It will also be tested if all user requirements are satisfied. In addition to this the effectiveness of design will be evaluated. This will be done with user testing using the pre-post method. This method was chosen because the effectiveness of the design will need to be tested to answer sRQ 6 and sRQ 7.

4. Ideation

During this ideation phase many ideas for scenarios will be created with the use of brainstorming. During this phase the lotus blossom and the KJ are used. The lotus blossom method will be used to generate many different ideas and the KJ method will be used to create more depth to the ideas by creating possible different scenarios. After this storyboards will be created to have a definite experience to realization with a clear message.

4.1 Lotus blossom Ideation method

In the first round of the ideation the lotus blossom will be used of which the results can be found in Appendix B. For this ideation round the general scenarios are ideated, where the different possible topic for the scenario was created. The topics chosen to ideate further upon are: what to do before or during a cyberattack, best practices for passwords, the risk of USB devices, possibilities and use of keyloggers in attacks, brute force attacks, wifi disruption, attempted physical access in a cyberattack and preventive measures that can be taken by a user. These are chosen to further ideation on because they are related to physical or technical cyber threats or best practices regarding these kinds of cyber threats.

During the second round of using the lotus blossom ideation method ideas are generated for the topic of what to do before, during and after a cyberattack. An idea for a scenario the user could check a list of passwords to see if there are any weak passwords which could be hacked. This would show the user examples of good and bad passwords and would teach them what to look for in good passwords. Another idea would be that the user gets notified of an account leak at another company, where the user would need to compare accounts and check if the password is the same or not. This would teach them about the bad practice of using the same passwords everywhere and the potential consequences this could have. During a cyberattack, the user could perhaps be in the role of the cybersecurity expert to become more aware of the work and effort needed for cybersecurity. Examples of these potential scenarios would be where the user has to limit the spread of a cyberattack. This could be simulated by opening and closing doors, where the virus has to be stopped by blocking all of its paths. The user could actively look into suspicious activity of accounts, for example, a janitor account that is requesting access to files it should have no reason to access. Or with a very high amount of requests per second, which wouldn’t be possible for a person to do. The user could also start making backups of the data before a computer virus gets access to it with a checklist of the steps they need to follow. And if they do get access to it temporarily shut down a section of that data. Where the user has to restore all the backups at the end and not restore the virus itself. After a cyberattack, the user could try to find out how the cyberattack had happened. They could look into who got hacked and how. This could be done by checking which employee account looks suspicious and what they were doing before the attack had happened. This could lead to different results where the employee might have installed software they had thought they needed, they might have been fooled by a phishing email, or their password was not secure enough. The reasons why the employee might have been hacked can be expanded further to tailor the experience to the requirements of the company that is receiving the cybersecurity training. This would show the user the different bad practices and how they could be better.

Should this be shown after another scenario where a cyberattack happened it would fit in the context and show the importance of good cybersecurity behavior. The user could also be shown a different point of view where they need to ‘hack’ a company and look for potential weaknesses. This would make the user aware of what weaknesses could be exploited and how to increase awareness and show bad behaviour.

During the third round of the lotus blossom ideation ideas are generated for password security and best practices. The user could be prompted that there are someone is attempting to login to their account or that a data breach occurred and that they will need to change their password. This would prompt the user to change their password where they can choose from different options. They could choose to reuse old passwords from a list of passwords. They could choose to type a password themselves. This password would afterwards be graded on password strength and the time could be shown how long it would take to crack the password using a brute force attack, which is an attack where a hacker is attempting to guess the password by going through all possible combinations. The password itself could also be visualized with a lock. A strong password would look like a strong secure lock, while a weak password would look like a small, rusted lock which looks very insecure. A password could be created by having letters and numbers on notes, which would need to be arranged in a certain order. After a password is created they could also be prompted to enable multi-factor authentication for an added layer of protection. To make sure the user is not only creating a strong password, but also a usable one they could be prompted to fill in their final password to check if they can remember it. All these ideas would make the user more aware of the best practices for creating passwords.

During the fourth round of the lotus blossom ideation the ideas are generated for physical access. Here the user could be put in the role of a security guard who needs to look out for suspicious people or they could be in the role of an employee who is arriving to someone having trouble gaining access to a restricted area. When the person having trouble is asking for help they might make use of deception. They could introduce themselves as a member of IT, a repair man, an inspector, someone from head office or even a new employee. During this interaction this suspicious person might perform suspicious actions to try to gain access to the restricted areas. This could include trying to copy or steal the access card. They could also have a stolen access card of another employee, where the picture of the person on the card would be different to how the suspicious person looks. These ideas would make the users more aware of the security regarding their access cards and more aware of people trying to deceive them to gain access to their access card and potentially also to restricted areas. It would also give an idea of what to look out for, however there are many different ways someone could try to deceive them. As such not all different methods can be included which the user needs to be aware of.

During the fifth round of the lotus blossom ideation the ideas are generated for unknown USB devices. This could include scenarios where a USB stick is on the ground or freely given away, but also other USB devices like USB cables as these kinds of cables already exist (Hak, n.d.) and could also be used as keyloggers to record usernames and passwords. These kinds of devices could also be received over physical mail looking like legitimate packages, even if they could be sent specifically to be used in a cyberattack. If the user is placed in a scenario where

they are the target of such an attack they become aware of the potential risks this would have and how easy it is to fall for such attacks and be wary of such attacks in the future.

4.2 KJ Ideation method

After the lotus blossom method the KJ ideation method was used to generate more ideas specifically for different cyberattack methods that can be used in the scenarios. This resulted in different ideas based on the ideas from the lotus blossom method. The results of the KJ ideation method can be found in Figure 4 below.

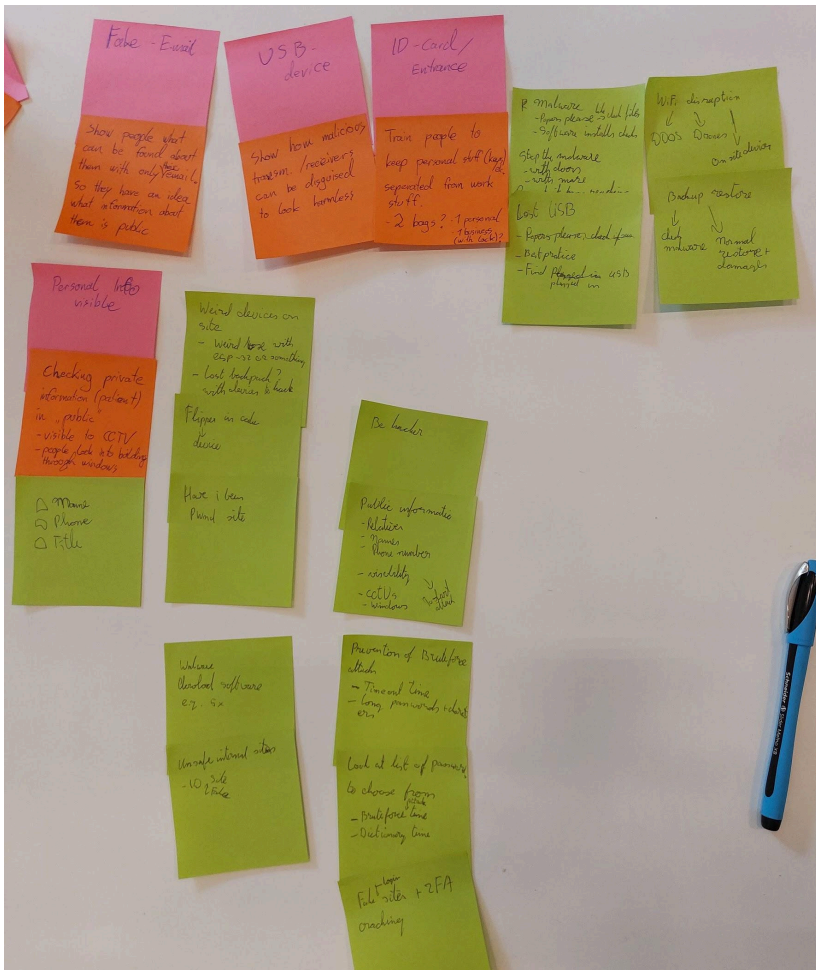


Figure 4, KJ ideation method

Users could be shown how much public information them is online and this link could be linked to a possible cyberattack. This could be done from the perspective of a hacker, where the user would need to find specific information about a person to login into their account. This could also be done from the perspective of an IT person who needs to look into why someone had gotten hacked, where all the information gain access to an account can be found online. This could result in showing the advantages of keeping a higher separation between personal and work activities.

A game can be used where the user needs to install software where they need to look out for common misdirection or deception methods. With this they would be more aware of these kinds of attacks.

For the physical devices examples might be shown about common and uncommon tools that could be used in a cyberattack that would look suspicious. This could make the user aware of potential devices that would be suspicious and how to respond to them, which is to make IT aware for them to look further into it. If the physical device is a USB device an interaction could be created where the user would need to remove them from PCs to stop a cyberattack.

Instead of the technical aspects the focus could also be on the physical aspects, where someone might look over the shoulder of a person to see what they are doing or looking at. Small cameras could be placed to look at computers or laptops to see what login credentials they use or to directly see what patient files they are looking at.

Internal websites could be faked if the hacker has access to the internet, which the user could fall for.

4.3 Storyboards

With this structure the following scenarios and storyboards are made. these storyboards will be described below and can be also found in Appendix C. The storyboard for each scenario follows a standard structure. This structure consists of an example, a game and the results of the game. During the example the cyberattack that will be discussed will be shown to the user. This way they are aware of what to expect, how it can be dangerous and the possible consequences of a successful cyberattack. This way the user becomes more aware of why it is important and why certain restrictions are in place to prevent these kinds of cyberattacks. After the example a small game will be played, which is themed around the cyberattack discussed before. What happens after the game is completed will be dependent on the results of the game. If the user performs poorly they will need to go to IT for them to help fix the problem, otherwise the user can continue to the next scenario.

The first storyboard consists of a scenario where the user will learn about USB devices. In the example the user will learn about the dangers of such devices where they need to charge their phone, where the only cable they can find is not their own and a trap for a potential cyberattack. Afterwards, the user would need to stop a cyberattack by unplugging several USB sticks from several different computers nearby. Should the user unplug all USB devices in time they can continue to the next game. Otherwise, they need to go to IT to report the potential cyberattack after which they can continue to the next game. The second storyboard consists of a scenario where the user needs to change their password. First, they will be made aware of a data breach at another company where they had an account. They need to change their current password for the hospital because they make use of the same password that had gotten leaked. After this is told to the user they need to create a password from several objects in the environment. Each object would have a different letter assigned to it, which would be the first letter of the name of the object. An example of this could be a cup, which would have the letter ‘c’. With this the user needs to create several strong passwords in a limited amount of time. If they do create enough strong passwords they can continue to the next scenario. Otherwise they need to go to IT to report the issue and ask for help with changing the password. The third and

last storyboard consists of a scenario where the user needs to point out suspicious or unsafe behaviour. This scenario will start with an example where the user gets on an elevator and someone else joins them. In the elevator the other person is standing close by, which could be seen as suspicious. Afterwards the user will be notified that this was an example of an attempted cyberattack where the goal was to copy the content of the user's access card. For the game the user will need to walk through several rooms where people might be acting suspicious and trying to clone or steal the access card. If the user can walk through all the rooms without someone being able to clone or steal the access card they have completed the game and have completed the cybersecurity training. If their access card did get clones or stolen they need to go to IT for them to disable the access card and to start the process of getting a new access card. This scenario is however difficult to create and would create unnecessary suspicion for a user and because of these reasons is decided to not be used.

The scenarios created with the use of the storyboard ideation method will be slightly changed. The RFID access in the current scenario would take too much time to properly create. Because of this it is left out from the scenarios that will be used. Some elements of this scenario are however reused, for example the 3D model of the RFID access will be used as decoration in the environment and for the password scenario. The flowchart can be found in Figure 5 where the different scenarios and their order in the VR cybersecurity training are placed.

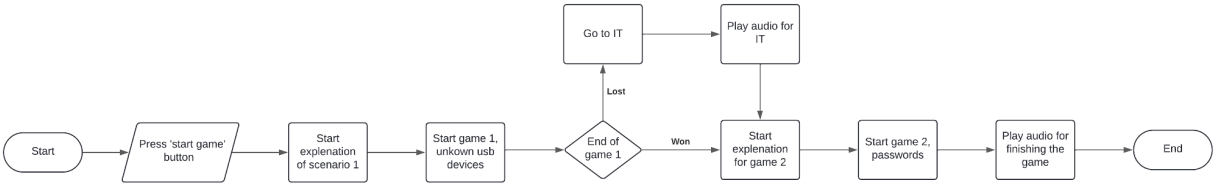


Figure 5, the flowchart of the different scenarios

4.4 Lo-Fi Testing

To be able to see how these different scenarios could be viewed by users several Lo-Fi tests are conducted and the most promising ones will be further developed to be used for the Hi-Fi prototype. The goal for this lo-fi testing is to receive feedback on unclear elements, which could be considered to be unclear and other possible points for improvement. With this several Lo-Fi prototypes of the scenarios are made and the users are asked to walk through the actions they would take in a given scenario. For some scenarios, the participant will be asked to interact with different physical objects. For the other scenarios, the participant will be asked to explain what actions they would take and the reasoning for their actions.

4.4.1 Selection of participant

The ideal selection of participants would consist of people who are currently working in the healthcare sector. However, it is not ideal to ask this group to participate in this Lo-Fi testing as it would take too much of their time, and the potential benefits this would bring would not be high enough. Because of this, the choice was made to make use of convenience sampling

where it was chosen to gather feedback from students of the UT. Students are chosen for them to give feedback on the different scenarios and to evaluate the different Lo-Fi prototypes of the scenarios.

4.4.2 Setup of evaluation

The Lo-Fi prototype tests are conducted in the SmartXP at the University of Twente. Before the start of the Lo-Fi testing, each participant is asked to read and sign a consent form. At the start of each interview, only the prototype was on the table related to the scenario being discussed to not distract the user during their interaction with the different scenarios. After this, the scenario was described to the participant and they are asked to make use of the think-aloud method to convey their reasoning as to why they are performing their actions. This is repeated for each scenario after which a small interview will be conducted. These scenarios consist of their phone being empty, for the keyboard to stop functioning and for them to need to quickly transfer a file. For the first scenario there are several USB devices nearby, which is a USB cable, a keyboard and a USB stick. The participants are asked what actions they would take during a scenario for each USB device. Afterwards, the participants are asked a series of questions related to this. For the second scenario, the participants are given a few physical objects with sticky notes attached to them containing letters related to the name of the object. The participants are asked to create a password from these objects, after which they are asked a few questions. For the third scenario context is given regarding a hypothetical scenario where they would be in an elevator and someone would be standing very close to them. After this, the participants are asked a few questions.

4.4.3 Conclusion / Discussion

With these Lo-Fi prototypes several insights are gathered for each different scenario. For the unknown device scenario it was shown that USB cables are not seen as suspicious by any of the participant in the context of cybersecurity. Keyboard however were seen as slightly suspicious by the participants. A participant had given the reason that there is no reason why such a keyboard would be in a random place without any reason. While the keyboards were seen as slightly suspicious and would not be used by the participants they were not suspicious enough to notify someone of them being there. The flash drives were seen as suspicious by all of the participants and not used by any of them. For the password scenario all participants seemed to be interested. A participant had asked if password strength would be shown. This was not explained during Lo-Fi testing itself, but considered to be added as it would show direct feedback to the user. Another participant asked a question regarding the amount of passwords that would need to be created. With this the user can make many different passwords, where they can receive feedback on multiple passwords. The next participant had also asked about the password amount and they had asked if the required password would increase in strength for each subsequent password. This idea of having multiple password with increasing strength is a good idea and will be considered to be added. For the RFID card scenario, where someone is standing close to the user in an elevator the feedback the participants gave was very different. Some of the participant found this suspicious and others not at all. The reasoning behind this was that different cultures would have a different perspective on this. From this it became clear

that this scenario would need to be changed because of how people can perceive the same scenario very differently, which could cause confusion for the users.

5. Design process of Hi-Fi prototype / Realization

During this phase of the design process, the hi-fi prototype will be realized. This section consists of the general layout of the office in which the VR cybersecurity training will take place, the final versions of the different scenarios to be discussed and the different assets that will be used during the realization of the Hi-Fi prototype.

5.1 Creation of environment

To start the creation of the environment different parts need to be worked out first. The first part is seeing what is possible in Resonite itself. Simple primitive shapes can be made consistent of boxes, capsules, cones, cylinders and other primitive shapes. However, in Resonite it is difficult to create more complex shapes and have them be at specific locations. Each different object would also need to be given each component individually which it requires, like colliders and specifically character colliders. While the character collider is a setting that can be enabled within the collider component this setting would need to be enabled for each different primitive object that gets created as it is not possible to easily enable to for multiple objects at the same time. For this reason, the 3D modelling software Blender was used to create and design the environment the cybersecurity training will take place. Here the different objects can be combined into one object, for example from multiple different wall sections to one object. This object can be given a mesh collider by itself and can be made a character collider once for all the different parts of the walls. However, objects that need to be intractable will be created and added separately to make sure the scale of each object is correct compared to the other objects and the size of the rooms when using VR. The final version of the environment can be found in Appendix G. As mentioned in the non-functional requirements several healthcare elements need to be added to the environment to try to increase the immersion and to answer sRQ 7, where these effect of these elements will be tested. In the environment subtle healthcare elements will be added. These elements will be in the form of a framed children's drawing of a doctor helping a child, which can be found on multiple different desks in the environment. During the serious game of the first scenario, where a data is being hacked, the hack will be specifically about patient files. This can be seen in the progress bar of how the percentage of the cyberattack being completed, where the text will show “X% of patient data hacked”.

5.1.1 Layout of Environment

The office environment needs to have several different locations where the scenarios can take place. The first scenario will be in the office area of the layout, the password scenario will be in the starting area and the IT scenario will be in the IT area of the layout. The final version of the layout can be found in Figure 6 below.

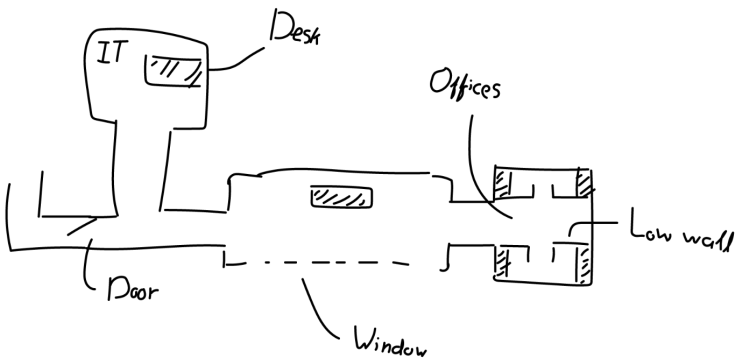


Figure 6, the final version of the layout of the cybersecurity training environment

5.2 Final scenarios

In the Hi-Fi prototype, 3 different scenarios are realized. Those scenarios are the unknown USB device scenario, the going-to-IT scenario, and the password scenario. The content of each scenario will be explained below. Before and after each scenario a voiceover will tell the user what the scenario will be about by giving an example of the topic. For example in the USB devices scenario an example will be given of a unknown USB cable. After the serious game of the scenario is finished the voiceover will explain more about the scenario about points which might be missed or the performance of the user during the serious game.

5.2.1 Scenario 1 - USB devices

During the first scenario, the user will first learn about that this scenario will be about the dangers of unknown USB devices. They will be given an example where a voiceover will verbally tell them an example of a dangerous USB cable. Afterwards, the voiceover will tell the user that someone plugged in multiple USB drives, which are actively hacking the computers to attempt patient information in the part of the environment called ‘offices’. The sign of the offices can be seen from the user's desk to the left. When the user arrives they can see a progress bar of the hack percentage, which is filling from 0 to 100%. To win this game the user needs to unplug 5 USB sticks in 120 seconds from 4 different computers. If the user can unplug the USB devices in time they are congratulated by the voiceover and they can continue to the next scenario about password security. If the user fails to unplug the USB devices in time the patient data is ‘hacked’ and the user needs to go to IT for them to help and fix the problem.

5.2.2 Scenario 2 - Going to IT

In the second scenario, the user needs to go to IT for them to help ‘fix an issue’. This happens when the user is not able to unplug all USB devices from the different computers in the offices at a given time. For this scenario, the user needs to walk towards the IT helpdesk for them to help solve the issue. When the user arrives there the robot behind the IT desk will talk to the user and will tell the user that they, the robot, will help them. After this, the user will need to wait a bit for the IT robot to fix the issue. After the issue is fixed the IT robot will thank the user

for coming to IT and will tell them that issues like these can happen. They will also tell them if it happens again go to IT again. This is to tell and teach the user that in the event something goes wrong they can go to IT for help. This would help because IT can minimize potential damages during a cyberattack by starting countermeasures earlier compared to when they would notice the cyberattack by themselves. After the help of the IT robot is finished the next scenario will start.

5.2.2 Scenario 3 - Password security

In the third scenario, the user will hear from the voiceover that another company had a data breach and that the user had an account there. The voiceover also recommends the user change their password as they often use the same one for multiple accounts. After this, the voiceover will start explaining that the user can make a new password with the objects in their environment. When they put those objects, which are all on a table in the first room, on pedestals, which are also on the table, they can create a password. The user needs to recreate the password that is given to them above the table and they need to do this 3 times. Each password builds on the previous one and will become longer. When the user has finished creating their password they will be told that this is not yet a strong password. This is because it only contains letters and strong passwords contain letters, capital letters, numbers and special characters. Afterwards, they will tell the user that passwords also should be long, as short passwords are not very secure. When the voiceover is done explaining about passwords a different voice will be heard thanking the user for participating, that the VR cybersecurity training is finished and that they can take off the headset.

5.3 Assets used

To create an environment of an office several objects need to be in the environment for it to be recognisable as an office. Some objects also need to be created for the different scenarios to function. For these reasons several different 3D models where created, which can be found in Figure 7 below. References for the different assets gathered from others can be found in Appendix E.

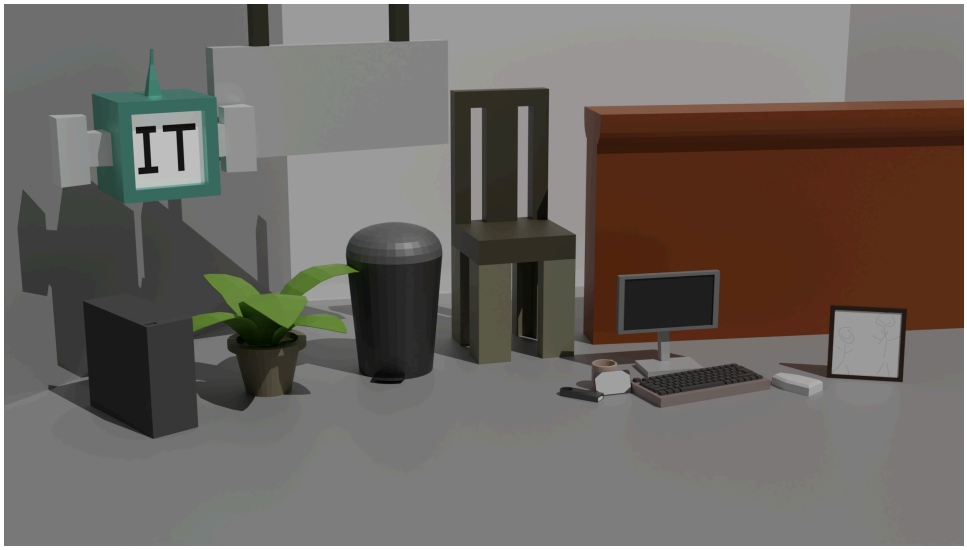


Figure 7, Assets used in the environment rendered in blender. Not to scale to each other

5.4 Protoflux code

To be able to create the different scenarios inside Resonite the use of protoflux is used. Protoflux is the visual coding language used in Resonite to write code. For the first scenario the protoflux code can be found in Figure 8 and 9. This scenario has several elements required for it to function as a serious game. This serious game need to have a timer to have a time pressure to unplug all the devices. This is done with a stopwatch that sends activates when the scenario starts and stops when all the USB drives are unplugged. It also need to stop the game when the timer is over. The USB drives need to be grabbable and it needs to be detected when they are considered to be unplugged. This is done by calculating the current position of the flash drive and the position where it starts at. When the USB drive is not grabbed anymore a check will be made if the USB drive is far away enough from its starting position. If this check fails nothing will happen, but if it succeeds the grabbed USB drive will turn invisible, will move back towards the starting position, a random USB stick will be activated and an internal score is increased by 1. If this score reaches 5 the game is completed successfully and the user will continue to the third scenario, the password scenario. If they fail and the stopwatch reaches 120 seconds, which is 100% of patient data hacked. The timer will stop and the user will continue to scenario 2, the IT scenario.

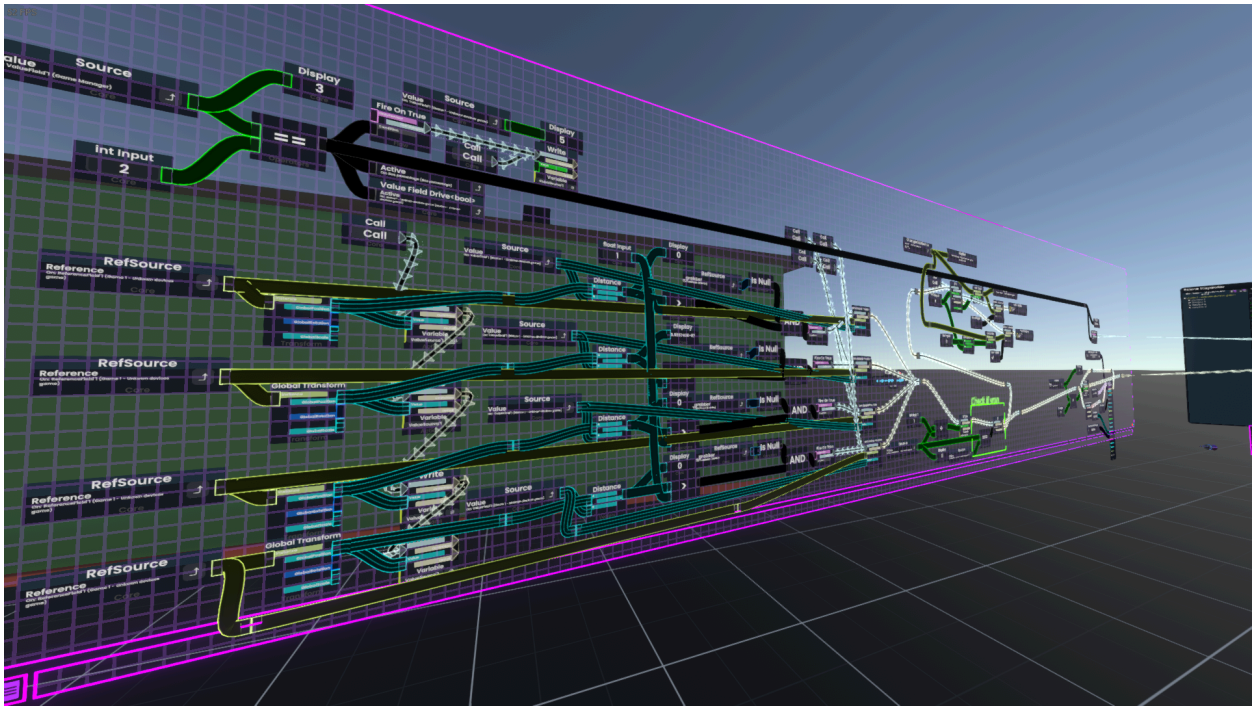


Figure 8, Protoflux code for scenario 1, without stopwatch

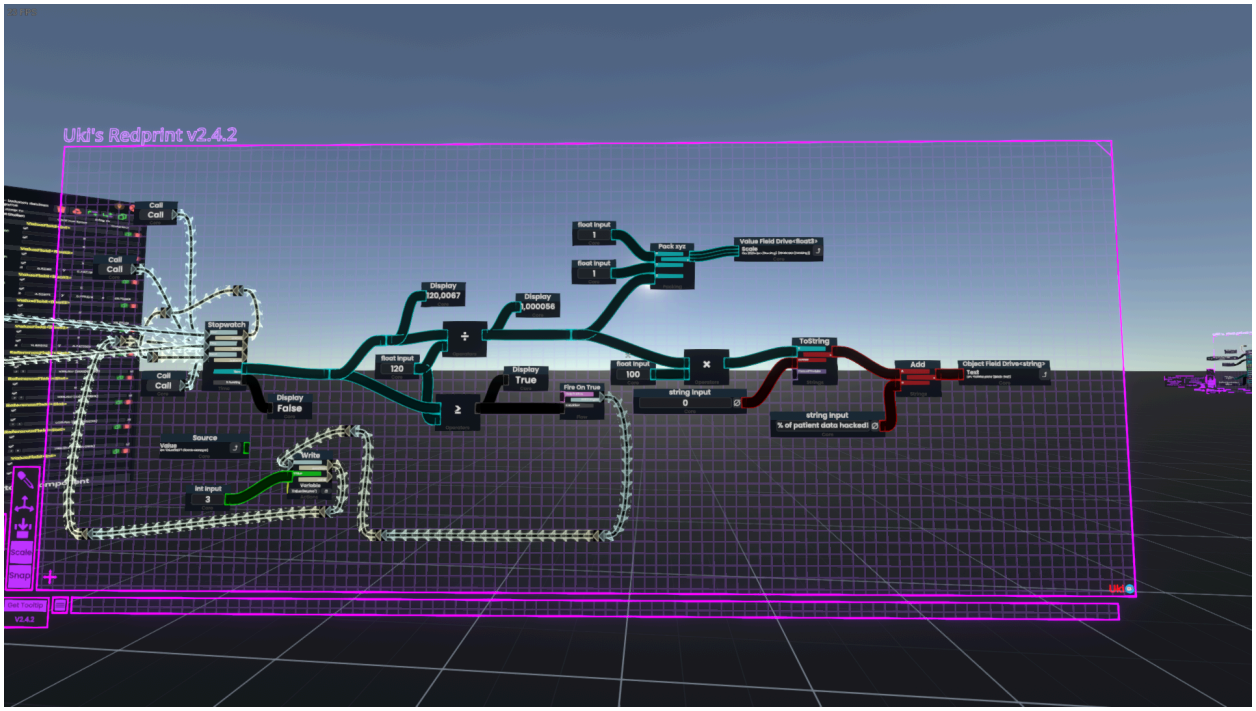


Figure 9, Protoflux code for scenario 1, stopwatch with display and time left

For the second scenario the protoflux code needs to be able to detect if the user is in the IT helpdesk area. This is done by checking for collision with an invisible box after failing the first

scenario. If the box detects collision with the player the audio for this scenario will start playing and when it is finished will the next scenario will start, the password scenario.

For the password scenario several different functions need to work to be able to fill in a password and for the password to be checked against a predetermined active password. The protoflux code of this scenario can be found in Figure 10. This is done by checking all children of the pedestal object, where the password object with a letter in the tag will be put when snapped to the pedestal object. When this password string is calculated it is compared with the current active password. If the given password is the same as the current active password the next password will become active, unless it is the last password. If the last password is completed audio will play and afterwards the next scenario will start, which is to let the user know the VR cybersecurity training is finished and that they can take of the VR headset.

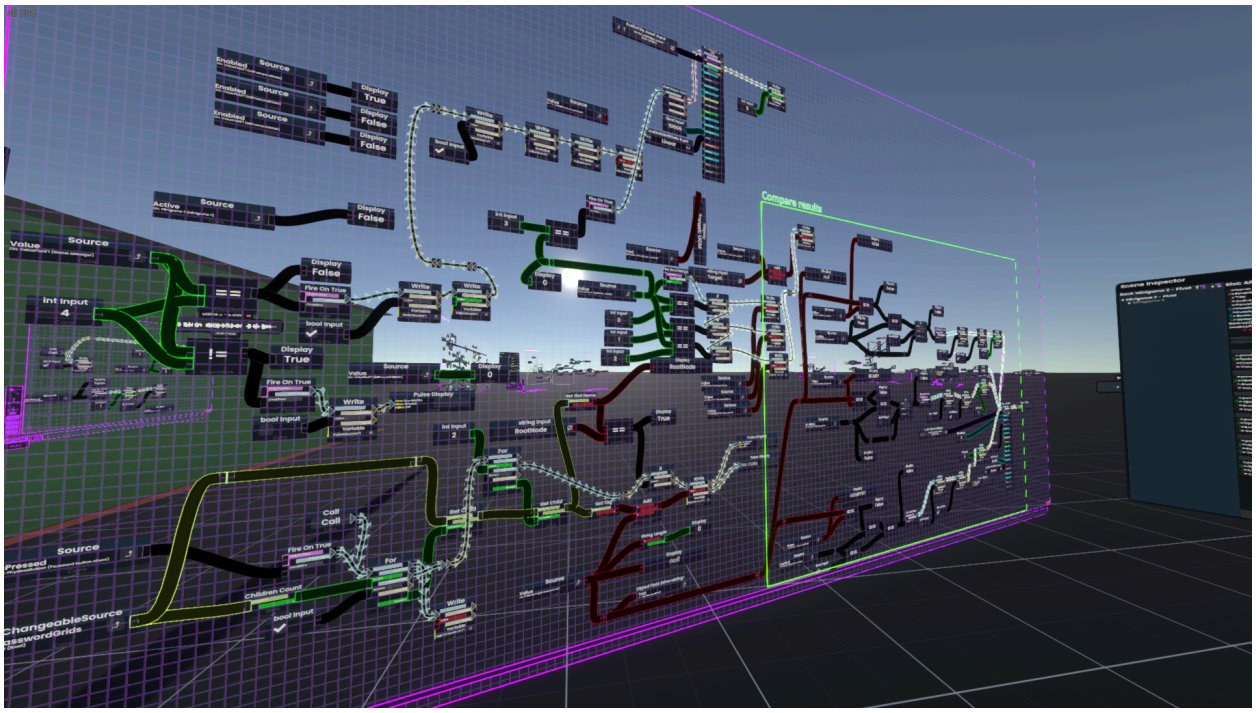


Figure 10, Protoflux code for scenario 3, comparing of passwords and playing audio when finished

6. Evaluation / User testing

To be able to answer sRQ 6 and sRQ 7 where the effectiveness of the VR cybersecurity training for healthcare needs to be evaluated an evaluation needs to be performed. This will be done with the use of a pre-post test, where all participants will fill in a questionnaire before and after they make use of the VR cybersecurity training. This will be done with the HAIS-Q validated questionnaire. In addition to this open questions will be asked regarding the experience with the Hi-Fi prototype and regarding the current healthcare elements. This research is approved by the EEMCS ethics committee of the University of Twente with the RP number 240530.

To answer sRQ 6, where the effectiveness of the VR cybersecurity training will be evaluated, and sRQ 7, where the different elements in the environment which are related to the healthcare sector will impact the perceived experience of the cybersecurity training, an evaluation needs to be conducted. This evaluation will make use of a pre-post test where the participants will be asked to fill in two questionnaires, one before and one after making use of the VR cybersecurity training. Both of the questionnaires will consist of questions from the validated HAIS-Q questionnaire. The pre-test questionnaire will include questions related to the demographics of the participants. The post-test questions will include questions related to the experience of the hi-fi prototype and the different elements this contains.

6.1 Participants

To be able to evaluate and confirm or deny the H0 and H1 the participants need to have a relation to the healthcare sector. Ideally, this would be healthcare professionals, however, it is not ideal to ask this group to participate in this user testing as it would take too much of their time. Instead of current professionals working in the healthcare sector students are chosen that follow a study that is related to healthcare, specifically BMT, TG and Health Science students at the University of Twente. This group would represent the future workforce of the healthcare sector and because of this would be a possible substitute for the healthcare professionals. The distribution of participants for the usertesting is 50% male and 50% female and can be found below in figure 11. The distribution of of the studies followed by the participants is 75% TG, 25% Health Science and 0% BMT and can be found in Figure 12.

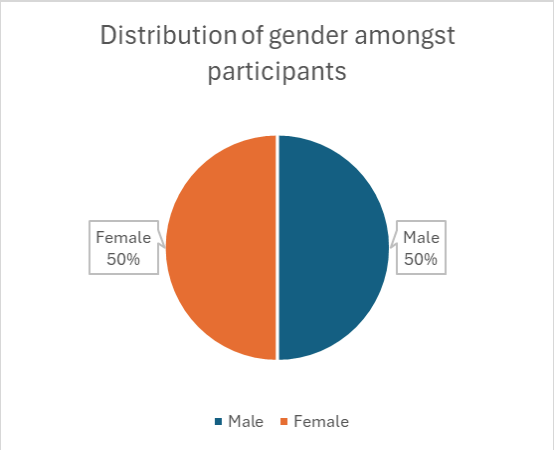


Figure 11, distribution of gender amongst participants

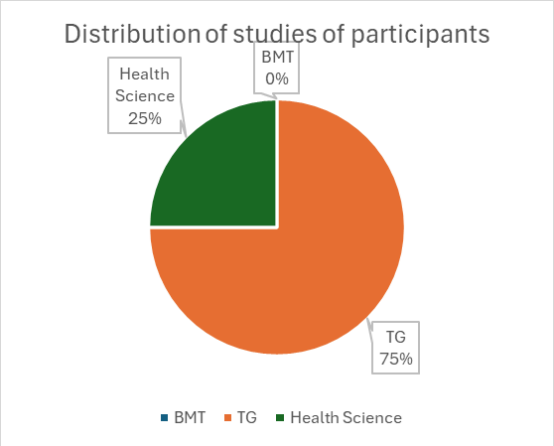


Figure 12, distribution of the current study amongst participants

6.1.1 Participant criteria

There are some criteria which the participants would need to follow for them to participate in the user testing. The inclusion criteria consist of students who follow a healthcare-related study, specifically BMT, TG, or HealthScience. This is because the VR cybersecurity training is specifically targeted for the healthcare sector. To be able to make claims regarding the effectiveness of the VR cybersecurity training related to the healthcare sector the participants need to have a connection to this. The exclusion criteria consist of people who experience motion sickness, as VR can cause motion sickness for people. To minimize the possible discomfort that people can experience they are excluded.

6.1.2 Sample size

The sample size for the user testing is 4 participants that follow a healthcare-related study. This sample consists of a distribution of students who identify themselves as 50% males and 50% females. The mean age is 23, and the age sample variance is 1.41. The distribution of the study of the participants is 75% TM, Technical Medicine, 25% Health Science and 0% BMT.

6.1.3 Recruitment

For the recruitment students of the healthcare-related studies at the University of Twente are asked if they are able and willing to participate. Multiple different methods are used to get in contact with as many students as possible. The first method used was to get into contact with the study association Paradoks, which is a study association for BMT and TM students. They are asked if it would be possible to forward a message asking students to participate. Paradoks and another study association called Sirius were given flyers and asked if they could be put in their study association room for members to see and possibly join the user study. The flyers that are created for the gathering of participants can be found in Appendix F. These flyers were also distributed and given to students interested in participating in the Technohal at the University of Twente, as both the study organization Paradoks and Sirius are located there. Furthermore, flyers were distributed and students were asked in person if they would be interested in participating in the user study. Another study association that was contacted was Sirius as they are a study association for Health Science. Students of the Creative Technology course of years 3 and 4 are also contacted in a whatsapp group chat asked if they know someone who would be interested in participating for the user testing. With each method of gathering participants, it is mentioned to them that there is compensation in the form of snacks when the user test is completed. This compensation consists of chocolate cookies or a chocolate bar.

6.2 Materials and Location

The user testing was conducted with the use of the software Resonite. This was done with the use of an Oculus Quest 2 VR headset with the use of air-link. Air-link is a wireless method of connecting the VR headset to a computer to run the program. This method was chosen to not make use of a cable, which could tangle and influence the immersion of the VR cybersecurity training. Resonite was used in combination with the researcher's account to further anonymize the participants as they do not need to create an account and login for the VR cybersecurity training to function. The user testing was performed at the University of Twente in the Citadel in room H106. In Figure 13 the setup can be found, which was used in room H106. In addition to this, a walkthrough of the VR cybersecurity training can be found in Appendix H.

Figure 13, test setup in room H106 in the Citadel on the University of Twente. Interviews are taken at the left table, and the equipment is on the right table.

6.3 Procedure during testing

Before the user testing starts the participant will be asked to read the information letter and read, fill in and sign an informed consent form. They will receive a short briefing about the study itself. They will be told that they are not the ones being tested, but that the prototype is. They will be reminded about the risks they will experience as also mentioned in the information letter and the informed consent form. When this short briefing is finished the participant will be asked to fill in a pre-test questionnaire with a randomly given participation number. After the pre-test questionnaire is filled in a short briefing will be given about the buttons on the controllers they will need to use in VR cybersecurity training and they will be asked if it is the interviewer can touch their shoulder if they are about to bump into objects in the room.

The participants will be asked for consent to record their gameplay without audio from the microphone. This way the recording will not contain any personal information of the participants themselves as the account of the interviewer will be used. When this is finished the VR cybersecurity serious game will start. When the cybersecurity training is finished the participant will be asked to fill in a post-test questionnaire, which also needs the participant number from before. When the participant is finished with the post-test questionnaire they will receive a debriefing and will have the opportunity to receive a small snack.

6.4 Questionnaire

To gather results from the user testing a pre-post test is conducted. This pre-post test uses a questionnaire with questions containing from the HAIS-Q validated questionnaire for cybersecurity as discussed in Parsons et al. (2017) This HAIS-Q questionnaire is a validated questionnaire to measure the information security awareness of those who answer this questionnaire. Groups of questions which are relevant to the created cybersecurity training are taken and added to the questionnaire of the pre-post test. These groups are password management and information handling. With the questions taken from both groups to be about the knowledge and attitude questions of the participant. In addition to the questions from the HAIS-Q questionnaire several open questions are added in the pre and post test. In the pre-test before the HAIS-Q questionnaire questions a few questions are asked about the demographics of the participants to gain an understanding of the demographics of the user test group. In the post test the open questions asked are out the experience of the participant with the Hi-Fi prototype. These questions are about the perception of the participants about the experience with the cybersecurity training and elements in used in the training. This is to check if any notable differences exist between the intended experience and the perceived experience. These questions are about the healthcare elements in the environment the participants have notices, the effect of these healthcare elements, what examples where given on USB devices by the voice over, the perceived messages being told by the different scenarios and if the user would change anything from the experience. The questions from the pre-post test questionnaire can be found in Appendix I.

6.5 Hypothesis / Statistical Design

The question to be answered with this quantitative evaluation is sRQ 6 and sRQ 7 can be answered with the qualitative result from the usertesting. To test the statistical significance for the results from the HAIS-Q test the results would need to be tested for normality. This can be done by testing the sample skewness, the sample kurtosis and afterwards the Shapiro-Wilk test of the average results from the HAIS-Q questionnaire. The Shapiro-Wilk test is used because this test works with small sample sizes to test the normality. With H0: normal distribution and H1: not normal distribution. If the data is normally distributed a one sample t test can be used to check the result are significant. Where H0: not significant and H1: significant difference in data

6.6 Design and Analysis

The results from the HAIS-Q test would first need to be extracted properly. The HAIS-Q test has negative questions, of which the answers need to be reversed. This can be done by taking the answer to the negative question and subtracting it from the number six. This is reverses the score from 5 to 1 likert scale to a 1 to 5 likert scale as the same as the positive questions. After this is done all the answers can be summed up and divided by the amount of questions to get the average improvement for each participant. To get the average improvement for each participant the average results of the participants needs to be summed up and divided by the amount of participants. If the average results are positive there is a average improvement of the performance for the participants. If the results are negative there is a deterioration of the performance of the participants. If the results are zero there is no change in performance of the employees. The normality of the results will also be checked by calculating the sample skewness and the sample kurtosis.

6.6.1 Problems during testing

During the usertesting there were some problems present. The first being that each time before the start of the VR cybersecurity training the the VR headset would need to be reconnected to the PC running Resonite. This had caused some delay and confusion when this did not work as expected. In addition to this two participants opened the Resonite menu by pressing a wrong button, this was however quickly resolved by pressing the same button again. During the third scenario with the password serious game two participants had put one of the password objects in outside the environment they could reach. Because of this the serious game was not able to be completed. This was solved by telling the participant something had gone wrong and that they are able to take of the VR headset. When the VR headset was taken off the participant would be thanked for testing the VR cybersecurity training and be asked to fill in a post test questionnaire.

7. Results

After the user testing has been performed the results of the answers of the participants can be calculated. From the four participants, the average HAIS-Q score is 0.375. The normality of these results is tested with the use of the sample skewness and the sample kurtosis. This resulted in a sample skewness of 0 and a sample kurtosis of 0.060. The sample skewness does indicate a normal distribution, however the sample kurtosis does not. To indicate normality the sample kurtosis should be close to 3. With this it can be concluded that there is an indication that the results of the HAIS-Q questionnaire are not normally distributed. The Shapiro-Wilk test is used to calculate if the results of the HAIS-Q questionnaire is normally distributed with H0: normally distributed and H1: not normally distributed. With a 5% significance level, there is no evidence to discard the H0: normal distribution and the normality of the data can be assumed. With the one-sample t-test, the significance of the results can be calculated to test if the results from the user test sample are significant to the larger population. With H0: $\mu=0$ and H1: $\mu > 0$ with $\alpha = 5\%$. This results in a significance of 0.197, which means that the data is not significant. This is likely because the amount of participants is very low, because of this no comparison can be made between the sample and the population. Because of this no definite conclusions can be drawn from these results, however, the results can show indications to possible conclusions. These indications need more research to be confirmed or to be denied.

From answers to the qualitative questions asked several insights can be gathered. During the user testing the participant had to walk to different rooms within the VR environment, however, the participants did not notice when this was expected of them. This indicates it is likely not clear enough for the participant that they are expected to move to a different room in the VR environment for the next scenario. Some healthcare elements are present in the cybersecurity training to make the experience more relatable. This could have an impact on the effectiveness of the cybersecurity. However, non of the added healthcare elements have been noticed by the participants. Because of this, no conclusion can be drawn for RQ 7. The different scenarios want to convey different messages and teach different things about cybersecurity. In the first scenario, the message would be that the participant would need to be careful about unknown USB devices, however, this message for this scenario was perceived as the need to be careful about USB flash drives instead. While this difference is small the importance is to be careful about the unknown USB devices as this contains more devices than just flash drives, which could be used in a cyberattack. The message for the third scenario was perceived as the need to make use of a strong password. However, the intended message for this scenario is what the best practices are to create a strong password. The difference between the messages is for the scenario not to teach to create a strong password, but for the participant to learn what makes a password strong. This difference could be explained by a difference in the created message and the intended message when creating this scenario. It could also be explained by having the message not be conveyed clearly enough.

8. Discussion

A feature considered to be added, but later not, to the VR cybersecurity training was detailed reports of the actions of the user. However, this would have some ethical consequences for the user of the cybersecurity training and their employer. With the detailed feedback given to the employee, they would be able to receive cybersecurity training on the topics they are not yet sufficiently scoring well enough yet. This however can be misused by their employer, if the employee scores poorly they would reasonably expect to receive more training, but they might be fired instead. The employee would start the cybersecurity training expecting it to be training, however, should it be used in this manner it would be a test instead of training. If this is not conveyed properly to the employee by accident or by clear intent the expectations would be different regarding the cybersecurity training. To minimize the risk of an accidental mismatch between the user and their employer the results will be aggregated and summarized to not be able to get individual feedback for each employee. Instead, the data will show which cybersecurity risks would need to be addressed more. This possible solution carries several problems by itself. One of those is the decrease in efficiency regarding cybersecurity training as multiple people will need to follow unnecessary cybersecurity training if someone scores poorly. Should the results be individualized each employee would be able to follow the specific cybersecurity they need. Employees who are outliers will not be caught. Should they score extremely poorly it will only be shown in the aggregated results. If they continue their work with these poor results, it would be difficult to have an entire group of employees in the healthcare sector stop working because of the urgency of their jobs. This would put the cybersecurity of the place of employment at unnecessary risk of cyberattacks as the employee with the bad score is still working and actively needing to take action, which would risk a successful cyberattack. With this, the question can be asked if the results of the cybersecurity training should aggregated or not.

9. Conclusion

The results from the user testing shown that there in an indication of improvement of the information security awareness of the participants. Normality has not been achieved and because of this sRQ 6 cannot be answered with certainty. This is because no definite conclusions can be drawn from the results. The results however can show indications for conclusions instead. With this the results, where a HAIS-Q score has been achieved of 0.375, the conclusion can be drawn that the cybersecurity training indicates helping training healthcare employees about information security awareness. More research is needed to reach a definite conclusion to answer this question. In addition to the quantitative conclusions, some qualitative conclusions can be drawn from the open questions of the questionnaire. Healthcare elements were not noticed by any of the participants during the user testing. Because of this, no conclusions can be drawn if these elements change the experience in a positive or negative manner. Because of this sRQ 7 cannot be answered. However, an indication is given that it is likely the different healthcare-related elements are not noticeable enough to be recognised. This could indicate that the healthcare-related elements should be more important in the different scenarios or be more noticeable to be recognised and have a potential impact on the experience.

Indications are found with the current Hi-Fi prototype of the VR cybersecurity training to have a positive impact on information security awareness. This cybersecurity training consists of different scenarios, in which each scenario consists of an explanation and a serious game. The scenarios are based on expert interviews and background research where the topic of cybersecurity training is created specifically for healthcare. While no definite conclusion can be drawn from the results an indication can be found that it does help with the information security awareness of the participants of the cybersecurity training. This would mean that cybersecurity training consisting of different scenarios, where each scenario has an explanation and serious game, could indicate to help train healthcare employees to be more aware of the cybersecurity aspect of their actions to minimize physical and technical cyber threats. More research is needed to confirm or deny the indication of this.

10. Future work

While the Hi-Fi prototype of the VR cybersecurity is finished there are several way it could be improved in the future. It could contain more diverse cybersecurity scenarios to have more variety. Follow-up serious games could be added to the different scenarios if the user scores poorly on the given topic. More visible and more important healthcare elements could be added to the different scenarios. This would link the cybersecurity training more to the healthcare sector. This could be tested if it has any effect on the effectiveness of the VR cybersecurity training. A possible example could be healthcare-related machines or devices that get disrupted, healthcare machines or devices like MRI machines or similar devices that are important to the functioning of a hospital. A system for feedback could be added with the use of detailed reports for each different scenario if the possible disadvantages are properly accounted for. Some scenarios could also be created with more dept. With scenario 3, the password scenario, the password that needs to be created could contain letters, numbers and symbols instead of just letters to create more diverse passwords. Perhaps different ‘machines’ can be added that enlarge objects to create capital letters, ‘machines’ that increase the count of an object and more. With the first scenario about the unknown USB devices, multiple different USB devices could be used instead of only USB flash drives. This could lead to a more diverse understanding of the dangers of USB devices for users. Future work should also try to validate the claims made for this paper by testing a larger amount of participants with a connection to the healthcare sector.

References

Al-Elq, A. H. (2010). Simulation-based medical teaching and learning. Journal of Family and Community Medicine/Mağalaẗ Ṭib Al-usraẗ Wa Al-muğtama', 17(1), 35. https://doi.org/10.4103/1319-1683.68787

Cain, J., & Piascik, P. (2015). Are serious games a good strategy for pharmacy education? American Journal of Pharmaceutical Education, 79(4), 47. https://doi.org/10.5688/ajpe79447

Cant, R., & Cooper, S. (2009). Simulation‐based learning in nurse education: systematic review. Journal of Advanced Nursing, 66(1), 3–15. https://doi.org/10.1111/j.1365-2648.2009.05240.x

Chang, T. P., Sherman, J. M., & Gerard, J. (2019). Overview of serious gaming and virtual reality. In Springer eBooks (pp. 29–38). https://doi.org/10.1007/978-3-030-26837-4_5

Chatmon, C., Chi, H., & Davis, W. (2010). Active learning approaches to teaching information assurance. 2010 Information Security Curriculum Development Conference. https://doi.org/10.1145/1940941.1940943

Chen, H., & Magramo, K. (2024, February 4). Finance worker pays out $25 million after video call with Deepfake "chief financial officer." CNN. https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html

Chernikova, O., Heitzmann, N., Stadler, M., Holzberger, D., Seidel, T., & Fischer, F. (2020c). Simulation-Based Learning in Higher Education: A Meta-Analysis. Review of Educational Research, 90(4), 499–541. https://doi.org/10.3102/0034654320933544

Digital Society School. (n.d. -a). Lotus blossom. Design Method Toolkits. https://toolkits.dss.cloud/design/method-card/lotus-blossom-2/

Digital Society School. (n.d.-b). WWWWWH. Design Method Toolkit. https://toolkits.dss.cloud/design/method-card/wwwwwh-2/

Digital Society School. (n.d.-b). WWWWWH. Design Method Toolkit. https://toolkits.dss.cloud/design/method-card/the-kj-method-2/

Digital Society School. (n.d.-b). WWWWWH. Design Method Toolkit. https://toolkits.dss.cloud/design/method-card/storyboard-2/

Courtois, N. T. (2009, May 4). The dark side of security by obscurity and cloning MiFare Classic rail and building passes anywhere, anytime. IACR Cryptology ePrint Archive. https://eprint.iacr.org/2009/137

Hak. (n.d.). O.MG Cable. Hak5. https://shop.hak5.org/products/omg-cable

Hatzivasilis, G., Ioannidis, S., Smyrlis, M., Spanoudakis, G., Frati, F., Goeke, L., Hildebrandt, T., Tsakirakis, G., Oikonomou, F., Leftheriotis, G., & Koshutanski, H. (2020). Modern aspects of Cyber-Security training and continuous adaptation of programmes to trainees. Applied Sciences, 10(16), 5702. https://doi.org/10.3390/app10165702

Security awareness game | Infosequre. (n.d.). https://www.infosequre.com/security-awareness-game

Kasper, T., Von Maurich, I., Oswald, D., Paar, C., & Horst Görtz Institute for IT Security, Ruhr-University Bochum, Germany. (2010). Cloning cryptographic RFID cards for 25$ [Journal-article]. http://www.proxmark.org/files/Documents/13.56%20MHz%20-%20MIFARE%20DESFire/Cloning_Cryptographic_RFID_Cards_for_25USD-WISSEC_2010.pdf

Khatri. M (2023). The Human Element is the Weakest Link in Cybersecurity. LinkedIn. https://www.linkedin.com/pulse/human-element-weakest-link-cybersecurity-mousam-khatri

Klooster, L. (2022). VR CyberEducation : improving the human factor in cybersecurity through an educational virtual reality program. University of Twente. https://purl.utwente.nl/essays/93717

Lunn, J., Khalaf, M., Hussain, A. J., Al-Jumeily, D., Pich, A., & McCarthy, S. (2016). The use of serious gaming for open learning environments. Lunn | Knowledge Management & E-Learning: An International Journal. https://www.kmel-journal.org/ojs/index.php/online-publication/article/view/318

Mader, A., & Eggink, W. (2014). A DESIGN PROCESS FOR CREATIVE TECHNOLOGY. ResearchGate. https://www.researchgate.net/publication/265755092_A_DESIGN_PROCESS_FOR_CREATIVE_TECHNOLOGY

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. Computers & Security, 66, 40–51. https://doi.org/10.1016/j.cose.2017.01.004

Pohl, M., Rester, M., & Judmaier, P. (2009). Interactive Game based learning: Advantages and disadvantages. In Lecture notes in computer science (pp. 92–101). https://doi.org/10.1007/978-3-642-02713-0_10

Prümmer, J., Van Steen, T., & Van den Berg, B. (2023). A systematic review of current cybersecurity training methods. *Computers & Security*, *136*, 103585. https://doi.org/10.1016/j.cose.2023.103585

Team, C. (z.d.). CTFtime.org / What is Capture The Flag? CTFtime. https://ctftime.org/ctf-wtf/

Seo, J. H., Bruner, M., Payne, A., Gober, N., McMullen, D. "., & Chakravorty, D. K. (2019). Using virtual reality to enforce principles of cybersecurity. Journal of Computational Science Education, 10(1), 81–87. https://doi.org/10.22369/issn.2153-4136/10/1/13

Shabani, T., Jerie, S. & Shabani, T. A comprehensive review of the Swiss cheese model in risk management. Saf. Extreme Environ. 6, 43–57 (2024). https://doi.org/10.1007/s42797-023-00091-7

Švábenský, V., Vykopal, J., & Čeleda, P. (2020). What Are Cybersecurity Education Papers About? A Systematic Literature Review of SIGCSE and ITiCSE Conferences Proceedings of the 51st ACM Technical Symposium on Computer Science Education, Portland, OR, USA. https://doi.org/10.1145/3328778.3366816

Appendixes

Appendix A - Expert interview questions (Combined)

As an important note, the expert interviews were conducted together with another student working on their bachelor thesis with the same topic, but with a different direction. Because of these expert interview questions will be the same as they will have.

Upfront:
We would like to conduct this interview to gain insight into the current state of cyber security in different organizations.
If any of the questions are considered too sensitive regarding the cybersecurity of your organization, please don't answer the question and let us know.

Demographics questions

1. What is your educational background in cybersecurity?
2. What sector do you work in?
3. In which type of organization do you currently work in, e.g. healthcare?
4. What is your current function?
5. How do you interact with cyberattacks in your current function?
6. How many years of work experience do you have in your current function?

General questions healthcare situation

1. What type of login method/system does you database software require where the data of the patients is stored?
    a. *Examples*
        i. *Username + password*
        ii. *Email + password*
        iii. *Security key*
        iv. *Fingerprint*
        v. *MFA in combination with others*
2. Why (previous answer) instead of the others?
3. How do the different employees interact with computers?
    a. Do they take a laptop/tablet with them when entering patient data?
    b. Do they write it down to be later added into the data management system?
    c. How is this done
4. How often do the employees need to login to this system?
5. What is currently the protocol for an on the floor healthcare worker when there is a cybersecurity incident? *Can be used as one of the steps to take in the program*
6. Any other cybersecurity things regarding a healthcare organisation in particular that we should take into consideration that were not mentioned yet?

Education / awareness training questions

1. What cyberthreats do you think cybersecurity training should be more in focus?
    a. Why those cyberthreats?
2. What cyberthreats do you think are currently relevant for your type of organization?
    a. Why those cyberthreats?
3. What kind of cybersecurity threats do you currently train employees on?
    a. If there is a different answer for 2 and 3, ask why those cyberthreats
4. How effective do you think the current solution is in your field of work?

Explain simulation and serious game here, or ask whether they are familiar with these terms?

5. What do you think the benefits are of teaching about cybersecurity through a simulation based approach?
    a. And what do you think the drawbacks are?
6. What do you think the benefits are of teaching about cybersecurity through a serious game based approach?
    a. And what do you think the drawbacks are?
7. All in all, of these two, which one do you think is the best, considering the benefits and drawbacks?
    a. Why do you think this approach is better?

“Now we would like to ask a few questions regarding the social engineering types of cyberattacks”

Social engineering questions

1. What technological/organizational elements are there in your organization that a cyber attacker could use to do social engineering? *(USBs, phone calls are commonly used in the company for example, can be used to create a scenario in the VR simulation)*
    a. Of those mentioned, what do you see as the most important weakness?
        i. Why do you see this as the most important weakness?
2. What possible social engineering dangers would be good to teach employees in your organization about?
    a. Why these social engineering dangers?
3. Do you think in person persuasion / social engineering is a relevant threat for your type of organisation?
    a. Why yes / why no?
4. What type of social engineering methods have attackers tried to target your organization with, be it successful or not? *Do not need concrete examples*
5. What type of social engineering attacks are already successfully prevented because of current cybersecurity training?

“Now we would like to ask a few questions regarding the physical types of cyberattacks”

Physical cyberthreats questions

1. What kind of examples in general can you give of attempted physical access cyberthreats? An example could be an attempt at accessing a restricted area or it could be someone asking to lend an access pass.
    a. *More examples: Someone unknown asks you to hold the door open (which needs special access)*
2. Do you make use of RFID tags?
3. What kind of examples can you give of attempted technological physical cyberthreats?
    a. *Example of finding an usb drive on the ground, which gets plugged into a computer*
    b. *Maybe random unknown cables/devices that where received via post*
    c. *RFID tags missing or stolen*
4. What kind of examples can you give of any noteworthy recent failed attempted cyberattacks for your organization? *(If too sensitive ask for your type of organization)*
    a. *Examples*
        i. *Unauthorized access*
        ii. *Unknown usb drives*
        iii. *Phishing emails*
        iv. *Network disruption attempts (like continuous deauthentication attacks)*
5. What types of physical cyber attacks have been successfully prevented because of the current cybersecurity training?

Concluding questions

1. What are sources that you consult to stay up to date on cybersecurity?
2. Finally, do you have any other remarks you would like to give us as we conclude this interview?

Give a thank you and conclusion to the interview

Possible added question topic (Sven)

7. Do you currently make use of healthcare software
8. If yes: What type of login credentials does it require?
    a. *Examples*
        i. *Username + password*
        ii. *Email + password*
        iii. *Security key*
        iv. *Fingerprint*
9. Why (previous answer) instead of the others?
10. Do you make use of RFID tags?
11. How do the different employees interact with computers?
    a. Do they take a laptop/tablet with them when entering patient data?

b. Do they write it down to be later added into the data management system?
c. How is this done

General healthcare situation questions (Sem)

1. What is currently the protocol for an on the floor healthcare worker when there is a cybersecurity incident? *Can be used as one of the steps to take in the program*

Any other cybersecurity things regarding a healthcare organisation that we should take into consideration?

Appendix B - Ideation method Lotus blossom

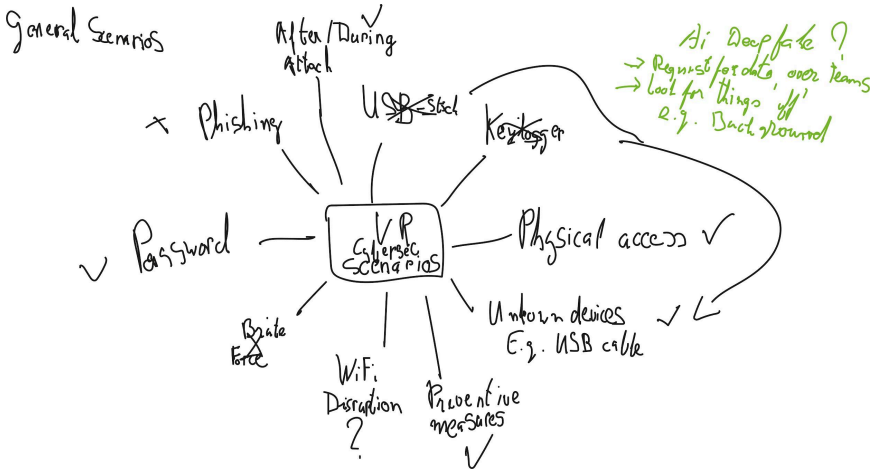


Figure 14, lotus blossom of the general topics for the different scenarios

Include steps for actions during attack https://cyberprecedent.com.au/lawcouncil/images/cyber/CP-What-to-Do.pdf

Figure 15, lotus blossom of the 'before, during, and after' scenarios

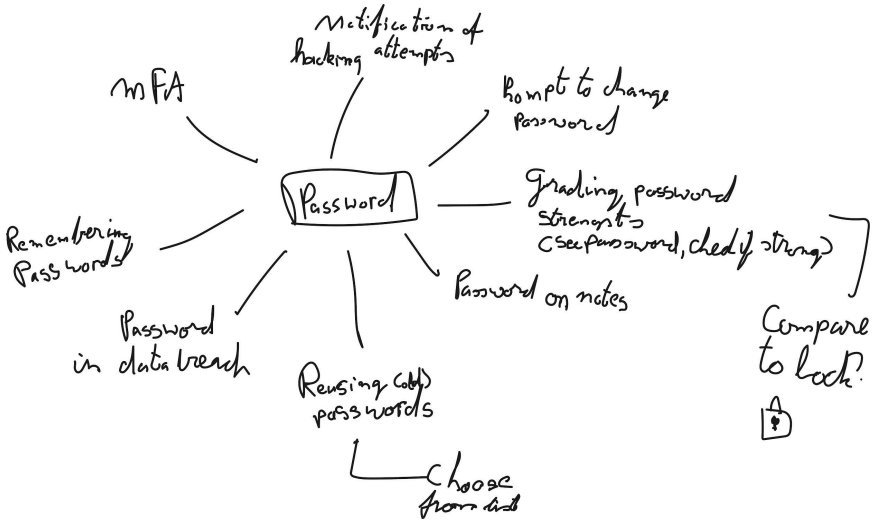


Figure 16, lotus blossom of the 'password' scenarios

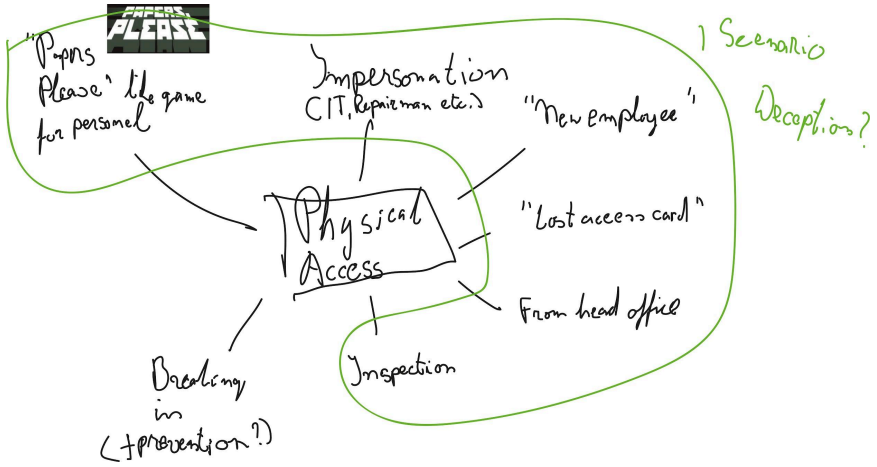


Figure 17, lotus blossom of the 'physical access' scenarios

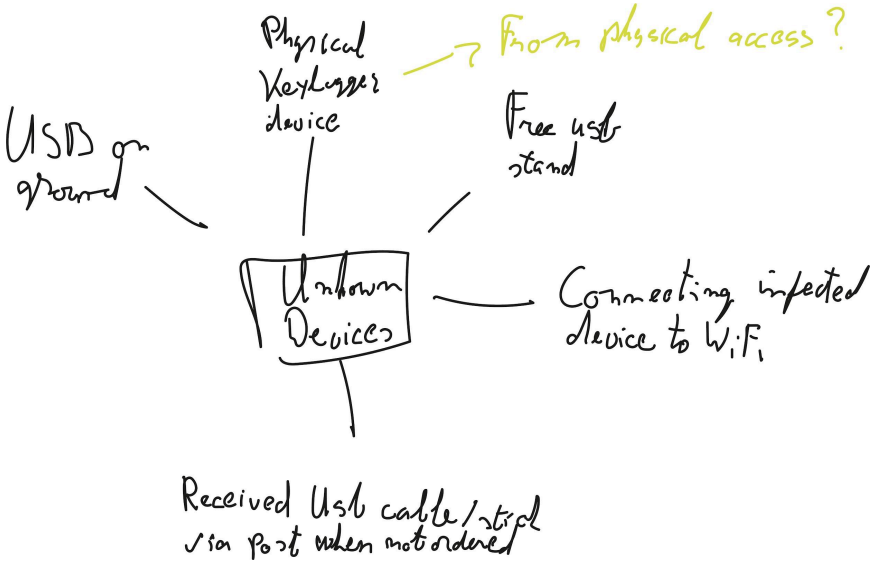


Figure 18, lotus blossom of the 'unknown device' scenarios

Appendix C - Ideation method Storyboards

Figure 19, storyboard 1

Figure 20, storyboard 2

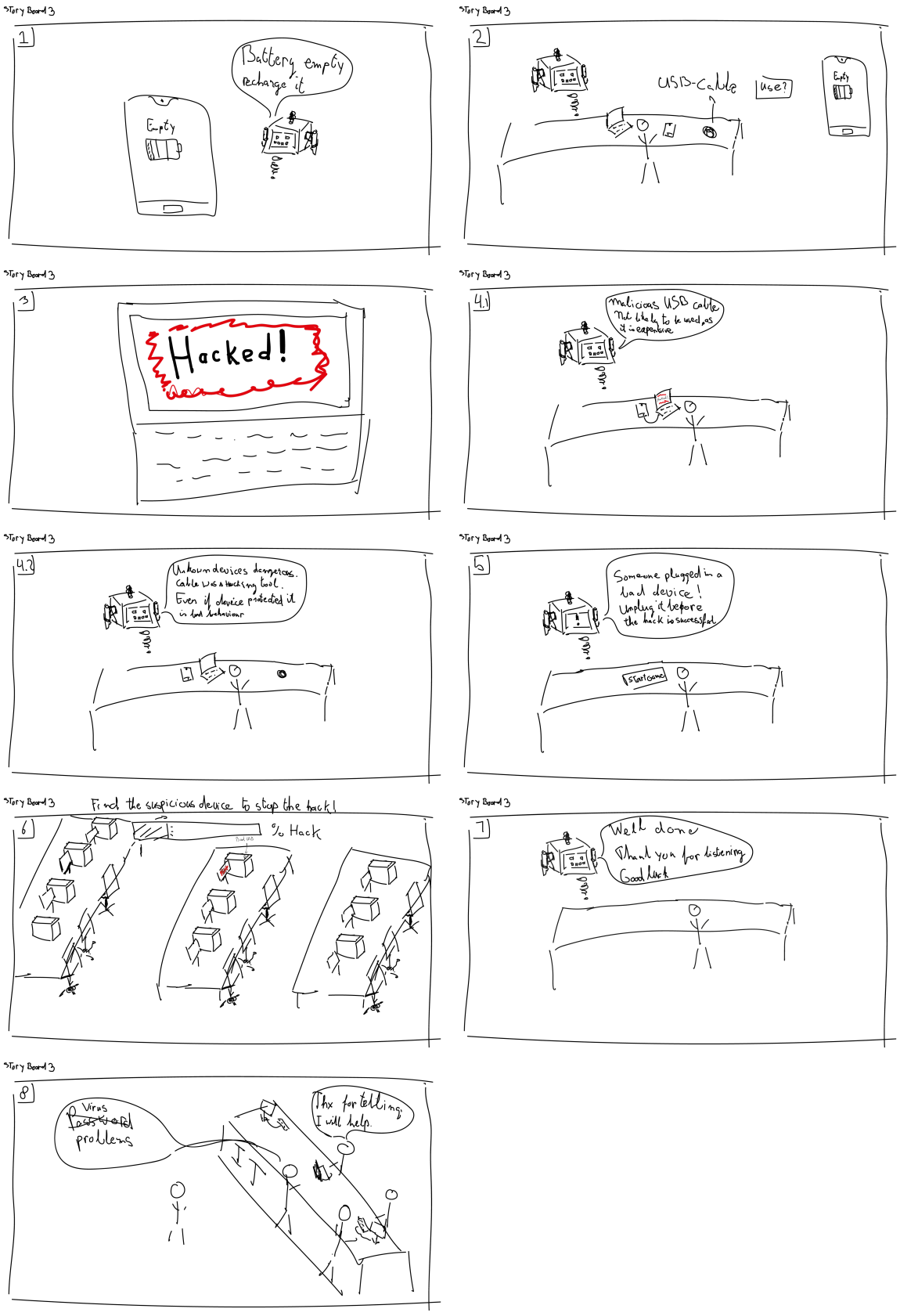


Figure 21, storyboard 3

Appendix D - Lo-Fi user test questions

Unknown devices

What do you think the message was?
What were the 3 least clear elements?
What was suspicious about these devices?

Password

What do you think the message was?
What were the 3 least clear elements?
How many passwords do you think should the user need to create?
Can you give your opinion about an increasing difficulty for the passwords?

RFID

What do you think the message was?
What were the 3 least clear elements?

General questions

If you had a magic wand to wave, and you could change, add, or remove anything from the experience, what would it be?

Appendix E - References for used assets

Models and images

Office layout and 3D model

- Created by Sem Bakker for their own graduation project and shared with me for my graduation project.

Blue futuristic networking technology vector (Background used in the flyer)

- Author: rawpixel.com on Freepik
  URL: https://www.freepik.com/free-vector/blue-futuristic-networking-technology-vector_19601032.htm
  License: Free license, attribution required

Blue futuristic networking technology vector (VR headset used in the flyer)

- Author: Freepik
  URL: https://www.freepik.com/free-vector/realistic-virtual-reality-headset_11583265.htm
  License: Free license, attribution required

Window image used in office environment to simulate the outside

- Author: X
  URL:
  License: Free license, attribution required

Plant leaf 3D model in blender (tutorial)

- Author: U.K Creations
  URL: https://youtu.be/Ej93hfu-Zww?si=ryxzeadGZFoyfnlO

Sounds

Keyboard typing

- Author: grcekh
  URL: https://freesound.org/people/grcekh/sounds/546164/
  License: CC0 license

Mouse click

- Author: Pixeliota
  URL: https://freesound.org/people/Pixeliota/sounds/678248/
  License: CC0 license

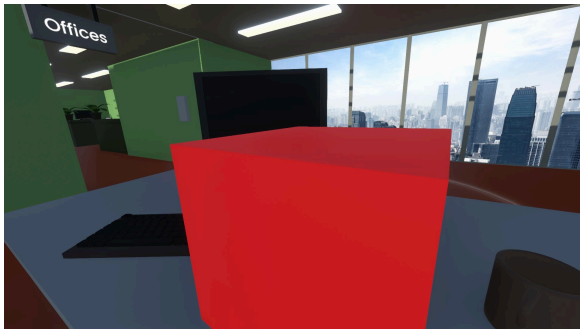
Bell ding

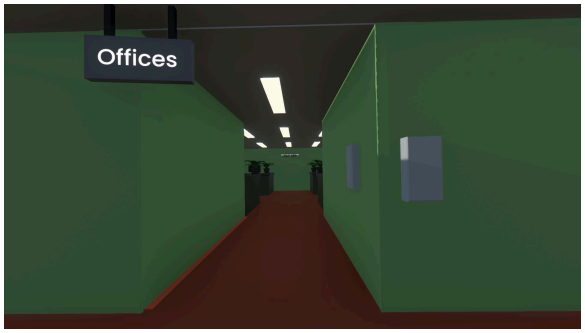
- Author: 5ro4
  URL: https://freesound.org/people/5ro4/sounds/611112/
  License: CC0 license

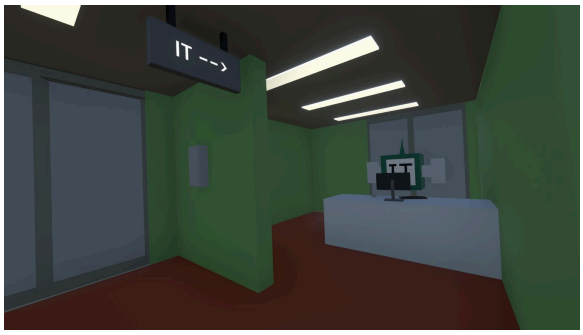
Appendix F - Flyers used for recruitment

Figure 22, the flyer used for the requitement of participant, front and back side printed in A5. Created by Sven Sonneveld and Sem Bakker using images from Freepik.

Appendix G - First person perspective of the VR cybersecurity training







Appendix H - Informed consent form + information letter for Hi-Fi testing

Information Letter Hi-Fi prototyping for Graduation Project 'Virtual Reality and Cybersecurity'

You have been asked to participate in testing a Hi-Fi prototype for a bachelor thesis for a gradation project. The graduation project is about designing a VR serious game that will train the awareness of the actions of the user around cybersecurity. The researcher would like to ask you to try out a Hi-Fi prototype of scenarios in the VR cybersecurity training.

Before and after the testing of the Hi-Fi prototype you are asked to fill in an anonymous questionnaire of which the answers will be used as part of the validation phase of the VR cybersecurity training. The anonymous questionnaires and the testing of the prototype will take roughly 45 minutes of your time in total. Questions in the questionnaire will be about your knowledge regarding cybersecurity and a short part about your experience with the Hi-Fi prototype.

During the VR cybersecurity training the gameplay footage will be recorded without the audio to be able to look back and analyze this data. Without audio this gameplay footage is anonymous, as all participants use the same researcher avatar.

There is a known risk involved in participating in this study, which is the risk of motion sickness. If you feel any motion sickness during the testing of the Hi-Fi prototype you can take off the headset and the testing will stop. In addition, there is also a minor risk of bumping into objects or walls, however the researcher will try to prevent this.

In addition to the risk of motion sickness there is the risk of discovering and sharing potential cybersecurity weaknesses. The study itself will contain cybersecurity training containing a few tasks of which the performance could indicate weaknesses when performed poorly. These weaknesses can form a risk for potential cyberattacks. To minimize this risk the questionnaires will be anonymous to prevent the researchers from knowing how each participant performs. Any sensitive information will not be shared beyond the research team and there will be no statements regarding specific participants. Should such risk be relevant you, the participant, will be made aware of this and the risk it would pose.

The study has been reviewed by the Ethics Committee Information and Computer Science. The main benefit of the study is helping in the validation process of a VR application that will help educate about and combat cybercrime, and learning to recognise signs of cybersecurity threats.

If the participant wishes to withdraw from the study, they have the right to do so at any time during the Hi-Fi prototype session, or up until one week after the testing has concluded. In that case, the participants' answers and data will be deleted.

Any data gathered will be anonymised and not be shared beyond the research team. During the interactions with the Hi-Fi prototype observations will be made and written down. Quotes made by you during the interaction with the Hi-Fi prototype can be used for the research if consent is given to this. The participant has the right to request access to and rectification or erasure of data.

Study contact details for further information:

Sem Bakker, [redacted]

Sven Sonneveld [redacted]

Contact Information for Questions about Your Rights as a Research Participant

If you have questions about your rights as a research participant, or wish to obtain information, ask questions, or discuss any concerns about this study with someone other than the researcher(s), please contact the Secretary of the Ethics Committee Information & Computer Science:
ethicscommittee-CIS@utwente.nl

Figure 23, Information letter for the Hi-Fi user testing with redacted contact details

Consent Form for Hi-Fi testing GP 'Virtual Reality and Cybersecurity'

YOU WILL BE GIVEN A COPY OF THIS INFORMED CONSENT FORM

Please tick the appropriate boxes	**Yes**	**No**
Taking part in the study		
I have read and understood the study information dated [7/6/2024], or it has been read to me. I have been able to ask questions about the study and my questions have been answered to my satisfaction.	○	○
I consent voluntarily to be a participant in this study and understand that I can refuse to answer questions and I can withdraw from the study at any time, without having to give a reason.	○	○
I understand that taking part in the study involves participating in a Hi-Fi prototype or a serious game in VR. Before and after testing the Hi-Fi prototype you will be asked to fill in an anonymized questionnaire. During the Hi-Fi prototype anything interesting to the researcher will be noted down.	○	○
Risks associated with participating in the study		
I understand that taking part in the study involves the following risks: The risk of motion sickness. If I feel any motion sickness during the testing the Hi-Fi prototype I understand that I can take off the headset and that the testing will stop. In addition to this there is a small risk to bump into objects or walls, however the researcher will try to minimize this risk.	○	○
I understand that taking part in the study involves the following risks: The risk of discovering and sharing potential cybersecurity weaknesses. The study itself will contain cybersecurity training containing a few tasks of which the performance could indicate weaknesses when performed poorly. These weaknesses can form a risk for potential cyberattacks. To minimize this risk the questionnaires will be anonymous to prevent the researchers from knowing how each participant performs. Any sensitive information will not be shared beyond the research team and there will be no statements regarding specific participants.	○	○
Use of the information in the study		
I understand that information I provide will be used for a bachelor thesis and that this thesis will be publicly available in the University of Twente thesis repository.	○	○
I understand that personal information collected about me that can identify me, such as [e.g. my name or where I live], will not be shared beyond the study team.	○	○
I agree that my information can be quoted in research outputs	○	○
I agree to share the following demographics: age, gender and type of study.	○	○
I agree that my anonymous gameplay footage will be recorded without audio.	○	○
Future use and reuse of the information by others		
I give permission for the answers of the anonymized questionnaire that I provide to be archived in University of Twente thesis repository so it can be used for future research and learning.	○	○

Signatures

_____	_____	_____
Name of participant	Signature	Date

I have accurately read out the information sheet to the potential participant and, to the best of my ability, ensured that the participant understands to what they are freely consenting.

_____	_____	_____

UNIVERSITY OF TWENTE.

Researcher name Signature Date

Study contact details for further information:

Sem Bakker, [redacted]

Sven Sonneveld, [redacted]

Figure 24, Informed consent form for the Hi-Fi user testing with redacted contact details

Appendix I - Hi-Fi user test questions

Pre-test

Questions VR cybersecurity training

What is your age?

What gender do you identify as?

What study do you follow?

What is your participant number? (Will be given by interviewer)

It's acceptable to use my social media passwords on my work accounts						
Strongly Disagree	1	2	3	4	5	Strongly agree

I am allowed to share my work passwords with colleagues						
Strongly Disagree	1	2	3	4	5	Strongly agree

A mixture of letters, numbers and symbols is necessary for work passwords.						
Strongly Disagree	1	2	3	4	5	Strongly agree

Sensitive print-outs can be disposed of in the same way as non-sensitive ones

Strongly Disagree	1	2	3	4	5	Strongly agree

If I find a USB stick in a public place, I shouldn't plug it into my work computer.						
Strongly Disagree	1	2	3	4	5	Strongly agree

I am allowed to leave print-outs containing sensitive information on my desk overnight						
Strongly Disagree	1	2	3	4	5	Strongly agree

It's safe to use the same password for social media and work accounts						
Strongly Disagree	1	2	3	4	5	Strongly agree

It's a bad idea to share my work passwords, even if a colleague asks for it						
Strongly Disagree	1	2	3	4	5	Strongly agree

It's safe to have a work passwords with just letters.						
Strongly Disagree	1	2	3	4	5	Strongly agree

Disposing of sensitive print-outs by putting them in the rubbish bin is safe.						
Strongly Disagree	1	2	3	4	5	Strongly agree

If I find a USB stick in a public place, nothing bad can happen if I plug it into my work computer						
Strongly Disagree	1	2	3	4	5	Strongly agree

It's risky to leave print-outs that contain sensitive information on my desk overnight.

Strongly Disagree	1	2	3	4	5	Strongly agree

Post-test

Questions VR cybersecurity training

What is your participant number? (The same as before)

It's acceptable to use my social media passwords on my work accounts						
Strongly Disagree	1	2	3	4	5	Strongly agree

I am allowed to share my work passwords with colleagues						
Strongly Disagree	1	2	3	4	5	Strongly agree

A mixture of letters, numbers and symbols is necessary for work passwords.						
Strongly Disagree	1	2	3	4	5	Strongly agree

Sensitive print-outs can be disposed of in the same way as non-sensitive ones						
Strongly Disagree	1	2	3	4	5	Strongly agree

If I find a USB stick in a public place, I shouldn't plug it into my work computer.						
Strongly Disagree	1	2	3	4	5	Strongly agree

I am allowed to leave print-outs containing sensitive information on my desk overnight						
Strongly Disagree	1	2	3	4	5	Strongly agree

It's safe to use the same password for social media and work accounts

Strongly Disagree	1	2	3	4	5	Strongly agree

It's a bad idea to share my work passwords, even if a colleague asks for it						
Strongly Disagree	1	2	3	4	5	Strongly agree

It's safe to have a work passwords with just letters.						
Strongly Disagree	1	2	3	4	5	Strongly agree

Disposing of sensitive print-outs by putting them in the rubbish bin is safe.						
Strongly Disagree	1	2	3	4	5	Strongly agree

If I find a USB stick in a public place, nothing bad can happen if I plug it into my work computer						
Strongly Disagree	1	2	3	4	5	Strongly agree

It's risky to leave print-outs that contain sensitive information on my desk overnight.						
Strongly Disagree	1	2	3	4	5	Strongly agree

What elements of healthcare did you notice in with the VR cybersecurity training?

How did those healthcare elements influence the VR cybersecurity training?

What examples of other USB devices where given in the first scenario by the voice over?

What do you think the message was in the first scenario?

What do you think the message was in the second scenario?

If you had a magic wand to wave and you could change, add, or remove anything what would you change?