VR CyberEducation

Improving the human factor in cybersecurity through an educational virtual reality program

Lara Klooster
Supervisor: Dr. ir. R.W. van Delden, Critical observer: Dr. J.H. Bullee
Graduation Project Creative Technology, University of Twente
08-07-2022

Abstract

This research aims to improve the role of human error in cybersecurity by creating an educational Virtual Reality (VR) program. Based on extensive background research, the Creative Technology Design Process is applied consisting of an ideation, specification, realisation and evaluation. Through this process an interactive VR program is created that lets the user perform basic cybersecurity related tasks in a virtual environment. The program monitors the user's cybersecurity knowledge and behaviour and provides feedback upon completion. Evaluation with the program shows that the average cybersecurity performance is significantly increased after exposure to the program. Furthermore, it identified a mean SUS score of 72.5, indicating an above average usability. These findings show the potential and possibilities of the program, defining a new method of effective education in the increasingly important and growing field of cybersecurity.

Table of contents

Table of figures

Table of abbreviations

Here is an overview of the abbreviations used in this paper, naturally they are explicitly defined in the text when firstly discussed.

ENISA	European Network and Information Security Agency
GP	Graduation Project
ISA	Information Security Awareness
ISAT	Information Security Awareness Training
OS	Operating system
UT	University of Twente
VR	Virtual Reality

1. Introduction

Due to technological advancement, cybersecurity has become one of the company's top precedents. Although many technical facets have been implemented, breaches have increased excessively in recent times [1]. Costs related to cybercrime have grown from $3 trillion dollars in 2015 to $6 trillion in 2021 and are predicted to be over $10,5 trillion in 2025 [2]. Approximately 95% of these security incidents are caused by some form of human error [3], [4]. Hence, this area has room for powerful improvements. There are various methods that aim to improve this aspect, one of which is training and education. Programs for training and education vary from classroom or online-based lessons to real-life phishing simulations. Although these programs have been found to increase cybersecurity awareness there are several impediments involved. Among others are, a monotonous and boring user experience [5]. Furthermore, existing methods don't allow for simple monitoring of skills progression. A recent development in this domain is the use of gamified experiences to educate users, research shows among others increased interactivity and engagement [6]. A specific implementation of gamification is through Virtual Reality (VR) which in this paper is adopted to be the use of computers and a headset to let users immerse in a simulated three-dimensional world [7]. This project aims to continue these developments and address the aforementioned problems by creating a VR-based environment in which users can maintain, monitor and practise their cybersecurity knowledge and skills. This leads to the following main research question.

How to design a VR-based game that educates people on the basics of cybersecurity?

To answer this question the following six sub research questions have been created.
SQ 1 What is the role of human error in cybersecurity threats?
SQ 2 What are the differences between existing delivery methods in cybersecurity awareness training programs?
SQ 3 Which topics should be included in a cybersecurity awareness training program?
SQ 4 What content can represent the selected topics in a cybersecurity awareness training program?
SQ 5 What are the benefits of the use of virtual reality in (cybersecurity) education?
SQ 6 How does the created VR-program influence one's cyber security awareness?

This project starts by obtaining background information on the various topics which are at the foundation of cybersecurity education programs. Firstly, related literature provided information, after which this is expanded with expert interviews. Then the ideation and specification start where the concept is further specified before it is executed in the realisation phase. At the end of this phase the created platform is evaluated with potential users. Key findings are that the created program does increase average cybersecurity performance and VR has a key role in the learning process of the program and obtaining these results.

The contributions of this work are in the improvement of cybersecurity education. With the realised VR platform, cyber and physical threats are combined into an educational immersion coming close to a real-life situation. It creates a new method of effective education in the increasingly important and growing field of cybersecurity.

This paper will continue as follows; in Chapter 2 the background research will be described including scientific related work. Chapter 3 will define the applied design process,

whose elements the ideation, specification, realisation and evaluation are extensively discussed in Chapters 4, 5, 6, and 7 respectively. The aggregated results are presented in Chapter 8 and further contextualised and related in Chapter 9. The conclusion is treated in Chapter 10.

2. Background[1]

This section will discuss background information that forms the foundation towards addressing the main research question.

2.1 Threats in cybersecurity

The threats related to cybersecurity can be categorised in various ways. Samy et al. [8] took a broad approach and identified 22 threats to cybersecurity in healthcare. Huang et al. [9] adopted this same strategy and established 12 categories of cybersecurity threats. Baide and Lashkari [10] on the other hand, only defined nine less generalised factors. All defined categories are related to one another in Table 1, it becomes clear that although there is a difference in scope and generalisation, they are highly comparable. The foundation of the table are the threats identified by Huang et al. [9], they took the broadest approach by defining eminently generalised factors. As the other authors identified more specified elements these are subdivided under Huang et al.'s [9] categories.

The full list of categories is displayed in table 1, in the following section those discussed in multiple researches are elaborated upon. A first threat is deliberate acts of theft, Samy et al. [8] agree and add the risk of repudiation which stops the system from monitoring users' actions. Badie and Lashkari [10] specify acts of theft to identity theft or the use of an unauthorised copy. A second threat defined by Huang et al. [9] is deliberate acts of espionage or trespass. Given specifications of this category are unauthorised use of an application, misuse of system resources, communications infiltration and excess privilege. This privilege means that a user gets access to information out of their scope, this can be done through masquerading, posing as someone else [8] [10]. A third threat is deliberate software attacks [9]. Samy et al. [8] specifically elaborate on malware attacks, which is the enclosure of malicious code and can appear in various forms (e.g. virus, Trojan horses or worms). Badie and Lashkari [10] agree but add denial of service which aims to shut down a network by disrupting services. The next highly discussed threat is acts of human error or failure [9]. Badie and Lashkari [10] specifically mention phishing and social engineering, both techniques aiming to exploit human vulnerability to gain access to cybersecurity networks. Furthermore, when taking a more organisational point of view, staff shortage and operational issues can be included [8]. Lastly, Huang et al. [9] define forces of nature as a cybersecurity threat, for example natural or environmental disasters or power failure [8]. Despite the fact that these are all important threats this project will solely focus on trainable elements within human control.

Although the created framework provides a clear overview there is a limiting factor. Human error can be related to several other categories. It is often even the cause of some of these other elements such as theft, trespass or software attacks. For example, malware is often installed on one's computer through causes of human error (e.g. through phishing or a USB). Similarly, unauthorised copies usually source from human mistakes such as bad physical security like leaving documents at the communal printer.

[1] Sections 2.1, 2.2 and 2.3 are based on the literature review from Academic Writing

Table 1: categorised threats of cybersecurity

Huang et al. [9]	Samy et al. [8]	Badie and Lashkari [10]
Deliberate acts of theft	Repudiation Deliberate acts of theft	Identity theft Unauthorised copy
Deliberate acts of espionage or trespass	Unauthorised use of a health information application Misuse of system resources Masquerading Communications infiltration	Unauthorised access Excess privilege
Deliberate acts of information extortion		
Deliberate acts of sabotage or vandalism	Wilful damage Terrorism	
Deliberate software attacks	Malware attacks	Denial of service Malware
Compromises to intellectual property		
Technical hardware failures or errors	Hardware failures or errors	
Technical software failures or errors	Software failures or errors Network infrastructure failures or errors	
Technological obsolescence	Technological obsolescence	
Deviations in quality of service	Deviations in quality of service	
Forces of nature	Environmental support failure/ natural disasters Power failure	
Acts of human error or failure	Acts of human error or failure Staff shortage Operational issues	Error and omission Phishing Social engineering

2.2 Role of human error

Acts of human error is one of the 12 threat categories defined in the previous section; however it is the biggest source of security breaches. In the past this human aspect has regularly been disregarded [11], [12]. Metalidou et al.[13] even assert that technology is regularly recognized as the only fix of these problems. However, despite technology being a crucial part in this domain it is not the only thing ensuring cybersecurity [12], [14], many security breaches are around [13]. This matter is also visible in research, Gilliam and Foster [14] state that only 4% of research between 1996-2018 in cybersecurity includes human behaviour. Nonetheless, Pollini et al. [12] mention there is consensus in literature on the importance of addressing this human factor. This importance is acknowledged by Huang et al. [9], delineating the human factor as the weakest point in information security. The most

frequent attacks stem from human error [4], [12].

However, the field of human error is very broad, to make an impact the most vulnerable factors are identified. When looking at literature there is consensus on two human factors, firstly lack of knowledge [4], [9], [12], [13], [15]. Desolda et al. [4] delineate that this shortfall of insight and experience can induce inferior choices. The second factor is the lack of awareness, which can be related to a lack of knowledge [4]. Zimmerman et al. [12], [15] and Pollini et al. [12], [15] both expand this list with the human vulnerability of lack of skills. Furthermore, Metalidou et al. [13] appoint risky belief, risky behaviour and inadequate tech use as vulnerable human factors. This is strengthened by Pollini et al. [12] who include violations in these human factors. Risky belief, risky behaviour and inadequate technology use can all be seen as violations of appropriate and safe cybersecurity behaviour. In addition, these violations can be caused through a lack of the aforementioned knowledge and skills [12]. Desolda et al. [4] continue by describing the vulnerability of norms and complacency. Unsafe norms are practices users become accustomed to over time (e.g. not locking the office/computer when leaving the workplace). Complacency is users' self-overestimation of cybersecurity skills, which can in term be related to a lack of knowledge and awareness. Another human vulnerability is lack of policies and compliance, which are predetermined written guidelines which an employee should adhere to [15]. Additionally, Zimmerman and Renaud [15] include the possibility of malicious users, this vulnerability encompasses those who make the “mistakes” without the intent of doing the right thing. Both of the above factors are strengthened by Pollini et al. [12], who mention the lack of adherence to rules as well as the chance of malicious violations.

There are also other approaches towards defining human error, Gillam and Foster [14] used the Human Aspect Information Security Questionnaire (HAIS-Q) to identify vulnerable areas. This questionnaire is the leading holistic method of measuring the human factor in cybersecurity [16]. It differentiates between seven various topics: password management, e-mail use, internet use, social media use, mobile devices, information handling and incident reporting. As becomes clear from the specificity of these subjects is that they are more specialised and application oriented. However, additionally they are vulnerable factors, things humans often do wrong.

2.3 Solutions for the vulnerability of the human factor

After the extensive consideration of the existing human factors in cybersecurity it is beneficial to outline the various solutions addressing this vulnerability. The main solution almost all researchers comply with consists of three elements: knowledge, education and training [4], [11]–[13]. Desolda et al. [4] expand on this by portraying training as key for those with low technology related literacy. Furthermore, these training shouldn’t only explain what to do but expand on the reasoning behind it [13]. In addition, Metalidou et al. [13] propose basic cybersecurity training for everyone and further specified programs based on an employee's function. Nobles et al. [11] expand on this by suggesting to generalise it even further and let all universities teach courses in human factors. Additionally, the training programs should be designed to include gamification, increasing engagement [11]. The second solution consists of improved policies and rules [12], [13]. Metalidou et al. [13] emphasises the importance of adequate distribution and enforcement as these are often only displayed on the company’s website. This way no-one sees it and therefore doesn’t even have the ability to comply with it. Other solutions are more focused on the

organisational level, one of them is the use of existing work and the encouragement of further research on human factors [4], [11]. The last approach towards improvement is focused on the culture of the organisation and the attitude towards cybersecurity [4], [12]. It is crucial to have the right mindset within both the employees as well as the organisation.

All defined solutions focus on protecting humans from making a mistake, literature also defines a different approach. Zimmerman and Renaud [15] propose to see the human as a solution instead of a problem. Hence, they avert from the aforementioned solutions, since the target of these methods is to constrain humans from making the wrong decision. They advocate for enhancing cybersecurity contingent on six principles: focus on success, human as a solution, encouragement of learning, defer to expertise, balance resistance and resilience, collaborate and communicate.

2.4 ISAT

In the former section of this paper, the weakest link in cybersecurity is extensively discussed, humans. To mitigate this risk possible solutions were presented, among which information security awareness training (ISAT). ISAT has various definitions, Wright [17] provides a very simple definition, describing ISAT as a training program to improve awareness. In this paper for a GP report the definition from Tsohou et al. [18] is adopted. They define ISAT as “a process that aims at changing individuals’ perceptions, values, attitudes, behaviour, norms, work habits, and organisational culture and structures with regard to secure information practice”. There are also various synonyms used in scientific literature, information security training and awareness (ISTA), cybersecurity training, and security education, training and awareness (SETA). These terms are used in numerous references, however corresponding findings are addressed under ISAT in this paper.

2.4.1 Reasons for focusing on ISAT

There are multiple reasons for focusing on ISAT for improving human error in information security. Firstly, it is endorsed to be a leading solution for dealing with the human weakness in information security [19]. Eminağaoğlu et al. [20] found that improving employees' knowledge and awareness is the most powerful technique for reducing security risks. It is even being recommended by the ISO/IEC 27002 [21], which presents guidelines on organising information security standards and practices [22]. Furthermore, there are multiple organisations that have regulations and standards in place where companies need to comply with, occasionally including ISAT. For example, when a company handles cardholder data, Payment Card Industry Data Security Standard (PCI-DSS) is in force. It requires policies that define ways of handling information security for all in the organisation [23]. Albrechtsen and Hovden [24] found that ISAT is a highly cost-effective way to deal with security, hence reasonable for companies to implement. Additionally, ISAT can improve one's information security awareness (ISA), a key factor in moderating information security risks [25]. Although ISA is already being seen as an important aspect in cybersecurity, members of organisations still lack this awareness [26]. The European Network and Information Security Agency (ENISA), reported that 90% of cybersecurity experts state they consider their organisation susceptible to insider threats [1]. These shocking numbers, combined with the various advantages and requirements make ISAT an interesting and effective approach, having the potential to induce big improvements.

2.4.2 Content of ISAT program

The first thing to consider when creating an ISAT program is the content, what should most definitely be treated in such a course. To our knowledge no clear picture is given on this topic within the current body of work. This can be due to the rapidly changing topic; cybersecurity and its threats are continuously expanding. To overcome this limitation, information from interviews with cybersecurity experts is combined with non-scientific though credible sources.

Before the interview ethical approval was obtained from the ethical committee (RP 2022-27). The interview was semi-structured, hence, there was a list of predetermined questions. This structure gave the opportunity to ask through on given answers or include new questions as the interview progressed. The interview started by introducing myself and this project after which the information letter and consent forms were handled. The first half of the questions focused on gaining knowledge on the current ways of monitoring, testing and educating cybersecurity. The second half focused on specific mistakes and important topics that should be handled. The full list of asked questions can be found in appendix A. Afterwards the audio recording was processed to usable, anonymous information. The interview included two participants who are both employees in handling cybersecurity at the University of Twente.

Cybersecurity education at the University of Twente (UT) is exceedingly important. For a little over a year the UT invites employees and students to participate in cybersecurity assessments and training programs. A baseline program in 2021 where 47% of UT employees and students participated in, assessed awareness on 7 different topics. These are topics that can be meaningful to include in an ISAT program. The results can be grouped into 3 classes based on average performance (see Table 2). It becomes clear that participants performed worst on protecting mobile devices and information. The secondly worst performed topics are related to phishing, social media and secure data protection and disposal. Results from phishing simulations show that 25% of all clicks by students are within a minute, this is very quick. The cause of this behaviour is not fully clear, possibilities are lack of knowledge or students' lifestyle being fast and quick.

Table 2: baseline cybersecurity training results

Topic	**Average score range performance**
Protecting mobile devices and information	66%
Identifying phishing threats Safe use of social media Secure protection and disposal of data	77%-81%
Own protection against scams Protection against physical risks Safe use of the internet	87%-89%

When asked about the most common human mistakes in cybersecurity, interviewee A1 refers to phishing and maltreatment of privacy sensitive cases. The most dangerous ones are those that include getting a virus on the computer. This can be through opening an email attachment or plugging a found USB with software in the computer. Interviewee A2 generalises this answer by saying that the most dangerous mistakes are those where human weakness is exploited. Mentioned were hack attempts, phishing and social engineering. It also includes the use of personal information from social media (e.g. to answer password reminders or find usernames). Hence, A2's response to topics that should most definitely be treated in an ISAT program are password management: strong passwords, no reuse and multi-factor authentication. Secondly, the importance of thinking before handling, taking a break when things do not seem right. Lastly, learning to recognize social engineering techniques. A1 refers to education on prevention of getting a virus on the computer.

Next to information obtained from the interviews there are also some non-scientific sources that can provide useful information. Usecure [27], a business offering a platform to measure and mitigate human cyber risk has set up a list of essential security awareness topics as well. Similar to the interviewees, phishing, password authentication, social engineering and removable media (e.g. USB) are mentioned. Furthermore, usecure has some similarities to the topics treated in the baseline training: mobile device security, internet and email use, and physical security. Other mentioned subjects not treated yet are working remotely, public Wi-Fi, cloud security, and security at home.

2.4.3 Delivery methods

Next to the content of an ISAT program a delivery method has to be chosen, this defines the way the content is conveyed to the clients. There are various configurations of the different educational methods around in scientific related literature.

2.4.3.1 Interview

Besides information on content, the interviews generated some information on the delivery methods as well. In previous years various delivery methods were used to increase ISA on the UT, examples are a cybersecurity escape room or a real-life Trojan horse. Due to COVID most recent efforts use online training programs, these are being provided by the external supplier Proofpoint [28] after which they are distributed among the public, both students and employees, via email. This delivery method is an online program consisting of videos and questions. Because in the past, no explicit assessment had been performed after ISAT efforts there is no knowledge of the potential ISA improvement. Hence, the different methods can't be compared based on effectiveness.

2.4.3.2 Literature

Scientific literature can provide a broader picture, Chowdhury et al. [29] distinguished between 5 different categories, conventional, online, game-based, video-based and simulation-based. Conventional methods are classroom-based lectures or workshops led by an instructor. They can either be in a physical space or held online [30], hence, group size differs from small workgroups of 5 to lecture-based groups of 200+. Chowdhury et. al. [29] state other disadvantages are the high cost and resource, and the fact that clients often experience the program as boring and monotonous [5], [31]. Furthermore, the effectiveness of the program is highly dependent on the instructor and there is no guarantee of

participation from the client. A commercial example of this method is the program offered by the FOX IT company, it is a classical 4-day training including theory, practical examples and exercises [32].

Online-based methods are very popular nowadays, as the term implies, they are courses on information security held online. A benefit of this method is the possibility for users to learn remotely, it is flexible and self-paced [5] [29] . Furthermore, it is highly cost-effective as it can be purchased once and applied throughout the entire company, surprisingly, some courses are without any cost. Chowdhury, Nabin, e.a. [29] mention that clients may not pay as much attention as they don't feel forced and aren't as motivated. The previously discussed method of the UT by Proofpoint falls within this category. Another example is Awaretrain, it consists of short pieces of theory combined with exercises (e.g. to recognize phishing emails) [33].

The third delivery method is game based, here users learn while playing a game. Just like online-based methods these games are often self-paced, scalable, cost-effective, flexible and remotely accessible. Furthermore they are more engaging for the clients than the aforementioned methods, very interactive and including teamwork [6], [29]. Chowdhury, Nabin, e.a. [29] add that it can be disadvantageous that older employees might not be as competent with this technology and it can be time-consuming. CyberEscape is an example of a game-based ISAT program [34]. The learning objectives are being teached through the form of an escape room, it requires the employees to work together and gain knowledge on the topic. Another very different example is the 'defend the crown game' from CISA (Cybersecurity and Infrastructure Security Agency). The goal is to defend the crown from cyber ninjas by using your cybersecurity knowledge [35].

Video-based delivery methods rely on educational videos to convey their content. They have some similar benefits as discussed before (e.g. self-paced, flexible, cost-efficient). Disadvantages of this method are primarily the lack of interactivity and active participation guarantee [29]. Ej4 is an example of this method, they offer educational videos on different aspects of cybersecurity to enlighten their clients on these topics [36].

The last delivery method is simulation-based, a distinction can be made between simulations that include fake trapping the user or the user knowingly going into the simulation. Advantegeous of this method is the way users are being confronted with a real-life situation and the possibility of teamwork. Furthermore, there are multiple other, earlier mentioned benefits, around, remotely, flexible and easily scalable. Disadvantages are coordination and the requirement of pre-existing knowledge [29]. The AttackSimulator is an example of this simulation-based delivery method where users are being trained using automated phishing simulations [37].

2.4.3.3 Conclusion

From the aforementioned delivery methods, multiple interesting findings can be discussed. Abawajy and Kim [31] found that a combination of different methods can improve the success of an ISAT program and is beneficial in keeping the clients interested. Labib [19] agrees with this and emphasises the importance of focusing on an ISAT more than only once a year. Another approach defined the delivery methods as more broad-ranging and states that training is the most effective method, making conventional methods subordinate [38]. This importance of training is being strengthened by Jin et al. [39], stating that students can learn 90% of practised material, while only 20% when this material is being heard or read. The importance of training is reoccurring, especially game-based methods are found to

be effective [5]. Dodge et al. [40] agrees with this but emphasises on the importance of interactivity in an effective delivery method.

Combining these insights, a combination of a game and simulation-based delivery method can be promising. This would mean a combination of methods is used, which are both highly interactive and relatively easy to check on participation. Furthermore, the game aspect would give the client the intrinsic motivation, while the simulation aspect brings the advantage of looking like a real-life situation.

2.5 Use of Virtual Reality in education

Virtual Reality (VR) can be very shortly defined as a “life-like artificial environment” [41]. More extensively McGovern et al. [42] define VR as “a medium composed of interactive computer simulations that sense the participant’s position and actions and replace or augment the feedback to one or more senses, giving the feeling of being mentally immersed or present in the simulation (a virtual world)”. This is the definition used in this paper. To realise VR, the use of a head-mounted display is necessary, providing a visual of a virtual world. Through moving around and interacting the user can participate in the environment [43]. Feedback can be visual, auditory and occasionally haptic [43], [44]. VR is a relatively new technology and still in its infancy, as of only 2014 it became more open to the public due to reasonably priced headsets and efficiency improvements [44].

VR has already been adopted in various disciplines and the applications are growing [42]. For instance, the medical sector uses VR to educate medical students on different procedures (e.g. intubation or laparoscopy) [42]. The value of VR in education has become clear through various studies. Alhalabi [45] found that students experienced a higher rate of interest and performed better when learning using a head mounted VR system compared to no VR or a Corner Cave System using cameras and glasses. Serin [43] strengthens this statement and found that users do not require a long introduction to have the ability to properly immerse in the VR game. Additionally, VR lets its users more easily understand things than when reading about it. This stems from the fact that VR is based on visualisation, this is related to a lower cognitive load [42]. Next to ease, learning through VR improves users' level of attention with 100% and performance with 30% [44]. McGovern et al. [42] also prove the effectiveness of education through VR, stating “VR can enhance students’ ability to acquire a broader range of skills in nurturing their overall educational experience”.

2.6 Related work: Virtual Reality in cybersecurity education

In this section various projects will be researched. Related projects are limited to those that discuss the combination of virtual reality and cybersecurity.

2.6.1 CiSE-ProS [46]

The CiSE-ProS VR program was created to offer students cybertraining programs. The hardware used in this project was the HTC Vive system which includes the wired headset, two handheld controllers and two motion tracking sensors which should be put around the user. The process of intervention is as follows: in the beginning of the user experience a short VR-based tutorial is shown which teaches the user different controls (see Figure 1). Afterwards, the user was teached how to navigate through the virtual world, teleportation, which was found to be the most user-friendly method. After these things the user had to pick

up a toolbelt with multiple objects, using these objects various tasks could be completed. From these tasks it becomes clear that CiSE-ProS mainly focuses on teaching aspects of physical security within the electrical engineering domain as is displayed in Figure 2 (e.g. replacing hardware or connecting cables). Hence, the program is only useful for a very specific target audience.

2.6.2 CyberVR [47]

CyberVR is a more general project than CiSE-ProS, it focuses on improving user awareness of cybersecurity-related issues. The storyline of the game is as follows; the user is an IT

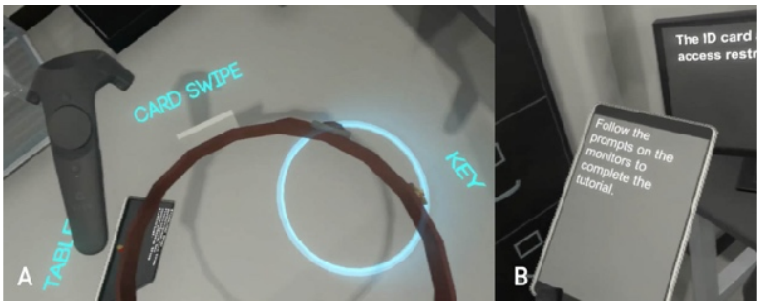


Figure 1: VR tutorial CiSE-ProS [46]

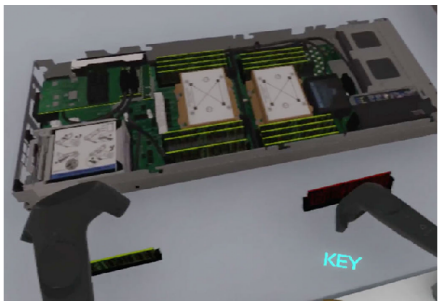


Figure 2: Tasks in the electrical engineering domain [46]

technician exploring a post-apocalyptic world. In this world IT systems are in the form of VR worlds and the user can set these up by playing the game. Progress can be made by completing different tasks in the form of mini games, all covering different topics of importance in cybersecurity (see Figure 3). All tasks contribute to improving a non-secure IT system, with the ultimate goal of creating a secure IT system. Topics handled are information flow, code injection, patch management, dynamic SW analysis, privilege escalation and public-key cryptography. Although these topics are all important regarding cybersecurity, most employees won't encounter them on a daily basis, some are beyond their scope. For example, privilege escalation lets the user scan to find whether the system contains any intruders. For the average employee it would be more helpful to focus on the prevention of letting intruders in the system.

CyberVR was developed using the Unreal Engine 4 and played with an oculus rift and leap motion, enabling interaction using hands. Furthermore, for some of the interactions an xBox controller is necessary. CyberVR was found to be similarly effective but more engaging that standard textbook cybersecurity education.

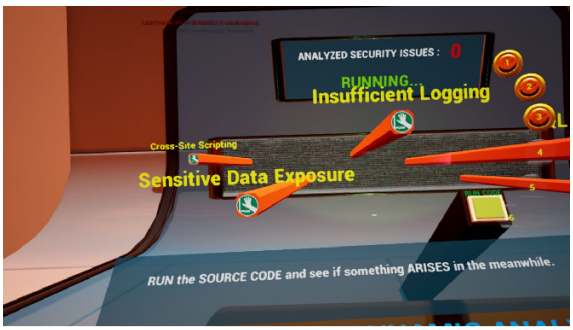


Figure 3: One of the tasks included in the CyberVR program [47]

2.6.3 Immersive Storytelling for Information Security Awareness Training in Virtual Reality [48]

This project did not create a real game but used a VR video to educate the user (see Figure 4). This video did include the user as a person, however no real interaction was possible. This project aimed to research the effect of a VR educational video as opposed to regular online-based training programs. The discussed topic was social engineering. They found

that users in VR gained more knowledge and sustained this knowledge for a longer period of time than when using traditional methods.

Figure 4: Part of the video shown in VR [48]

2.6.4 CyberCOP [49]

CyberCOP aims to create a collaborative, immersive and interactive system. Users connect with the program using Virtual Reality, Windows, Icons, Menu and Pointers (WIMP) or post-WIMP interfaces. Furthermore, the user can have various roles: analyst, coordinator or client. Each role has access to different information and views, by collaborating they can evaluate the security state of the system and keep it safe (see Figure 5).

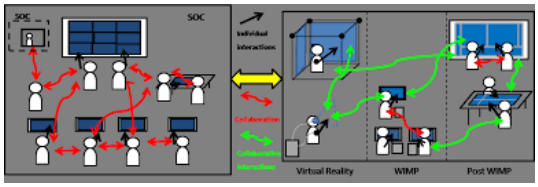


Figure 5: Collaboration in the CyberCOP system [49]

2.6.5 Conclusion

The findings above are summarised in Table 3 and compared to GP goals in Table 4. It becomes clear that none of the related projects have the desired scope of topics. They are all very specific and not of interest for the problems an average employee encounters on a daily basis. Furthermore, all projects take a similar point of view, they let the user be the protector of a system. Regarding interaction possibilities there are some differences, two of the projects use the VR handheld controllers, one even adds a virtual toolbelt to increase interactivity. CyberVR does not use these controllers and lets the user interact through a leap motion controller and occasionally an xbox controller. Immersive storytelling is fully passive and does not include any interactivity at all. Only one of the projects specifically mentioned giving the user a short introduction before the start of the game. When taking a look at Table 4, the differences between the existing programs and the aims of the to-be-developed program become clear. None of the projects have high interaction, a protector point of view and the elemental scope of topics.

Table 3: related work comparison

	Introduction needed	Handled topics	Point of view (protector/ attacker)	Interaction possibilities
CiSE-ProS	On controls and navigation in game	Physical security within electrical engineering	Protector	Highly interactive with 2 handheld controllers and toolbelt (tablet, ID and key)
CyberVR	Unknown	Too specific for average employee	Protector	Interaction through leap motion and xbox.
Immersive storytelling	None	Social engineering	Not applicable	None
CyberCOP	Unknown	Keeping security system safe	Protector	Handheld controllers

Table 4: Comparison related work to GP

	Handles basic topics any average employee encounters	Protector point of view (maintaining safe environment)	High interaction with handheld controllers
CiSE-ProS		✓	✓
CyberVR		✓	
Immersive storytelling			
CyberCOP		✓	✓
GP	✓	✓	✓

3. Creative Technology Design Process

The design method used in this project is the Creative Technology Design Process [50]. This model consists of four iterative phases: ideation, specification, realisation and evaluation, each phase starts divergent and concludes more convergent (see Figure 6). In the ideation the initial concept was ideated and brainstormed to eventually come up with a defined product idea. To do so the checklist method and a mind map were used. The process continues by further specifying this product idea in the specification. This phase made sure all elements were considered, discussed and specified before they were actually created. This section starts by applying a FICS analysis and defining the education method. Subsequently, the system architecture and a typical scenario are described. It concludes by setting up functional and non-functional requirements. The specified product is then actually created in the realisation phase. It discusses the platform and describes the process of creating the various elements of the program. The evaluation is the last phase of the Creative Technology Design Process, it describes the setup of the evaluation and the statistical analysis. It is important to note that this is an iterative process. Whenever, things in one of the phases do not work out it is circled back to one of the previous phases.

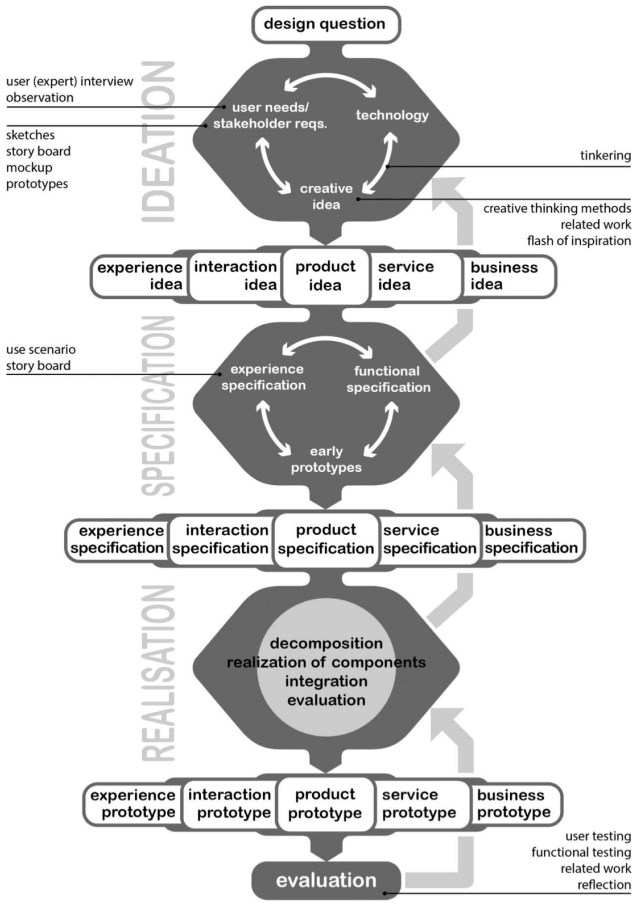


Figure 6: The Creative Technology Design Process [50]

4. Ideation

During the ideation phase the goal was to end up with a defined project idea. This thesis was started with the intention to create a VR-based environment to educate people in cybersecurity. Therefore, the project was already more specific than when starting with just a problem. With this concept in mind the background research was performed to gain knowledge on the state of the art and current ways of handling cybersecurity. Simultaneously the tinkering with the chosen platform started, learning the possibilities and controls of the platform. To start off the ideation the checklist method was used, it consists of asking yourself six questions (why, where, when, who, what and how) [51]. The answers to these questions are displayed in Table 5.

Table 5: Checklist ideation method

Why	Bad ISA among people in a world where cybersecurity is gaining importance.
Where	The game will be played in a VR environment, hence it can be played anywhere where there is a VR set-up. Specifically, this project focuses on enhancing cybersecurity on the UT as a first use case.
When	Multiple times a year to monitor, maintain and educate people on cybersecurity and keep the organisation safe. Furthermore, the program should be included in the onboarding phase of any new employees.
Who	Members of an organisation with bad ISA. Especially those who regularly handle organisational information on- and offline.
What	An interactive and educational VR cybersecurity game which combines the cyber and physical threats into an immersion which simulates a real-life situation.
How	This will be realised by creating the program using neosVR. Afterwards, this program will be evaluated by potential users.

After this method the ideation was further expanded by creating a mind map (see Figure 7). This mind map structures the project by subdividing the program in various parts: for who, values, product, and experience and interaction.

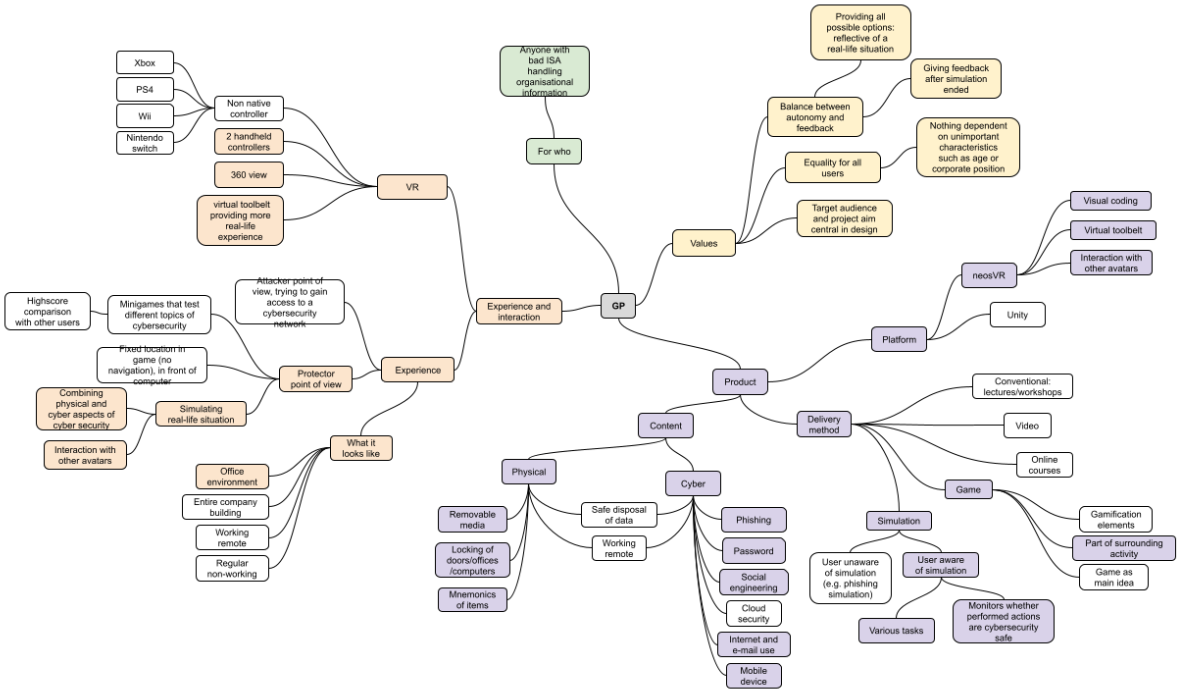


Figure 7: Mind map ideation

4.1 For who

The target audience of the program is quite broad. It aims to help anyone with low ISA who handles organisational information.

4.2 Values

The values are things that should be taken into account when designing the program. One of them is the balance between autonomy and feedback. In the program users should have the autonomy to make their own decisions, the options should be reflective of a real-life situation. Furthermore, they should not be influenced in making these decisions, therefore feedback on their choices should be presented after the simulation ended. The second value focuses on equality for all users. Since the goal of the project is to improve individual and organisational ISA all users should be treated equally. Both the CEO and the administrative assistant should get the same treatment, nothing should be dependent on one's corporate position, age or other unimportant characteristics. Thirdly, in the creation of the program its goals and target audience should be central. Everything should be designed so it can optimally serve the users and improve ISA.

4.3 Product

The product can be subdivided into three elements: content, delivery method and platform. The content describes the topics that should be included, these can be either physical or cyber. As displayed in Figure 7, both classifications include various specific topics. The coloured blocks are mentioned by various sources as important topics to include an ISAT program. The white blocks are only represented by one source. Therefore, only the coloured blocks are included in the program.

Physical security is related to keeping the physical side safe. Removable media are portable objects that can be used to temporarily store information. There are two risks involved. Firstly, losing removable media that contains valuable information. Secondly, the expert interviews showed that they can be left for others to find with malware included. Examples of common removable media are USB sticks, SD cards or smartphones [27]. Next to removable media the locking of doors, offices or computers should be included. This makes sure that all valuable information is safely stored. Lastly, mnemonics of items should be discussed. The expert interviews highlighted the use of sticky notes to remember various passwords.

The cyber part of the content is at least as important, after all it remains cybersecurity. The first topic that should be covered is phishing, as explained in the expert interviews this is the sending of malicious links to gain access to a network or information. Secondly, password security, used passwords should be strong, not reused and multi-factor authentication should be implemented [27]. Social engineering also exploits human weakness by building trust to gain access to valuables. Examples are WhatsApp fraud or posing as a client to gain knowledge [27]. Fourthly, mobile devices, a lot of information is also accessible here, therefore this should be protected as well. Threats are malicious applications or poor protection. Internet and e-mail use includes many aforementioned threats such as phishing and password management. This topic also comprises safe social media use, it can provide hackers with information to gain access. For example, it can provide information for fraud, usernames or passwords. Lastly, there is cloud security, which includes the protection of assets in the cloud. However, because this aspect is not mentioned by multiple sources this will not be included in the program.

There also are some topics that exist in both the physical and cyber domain. Safe disposal of data can be physical (e.g. the use of a paper shredder for disposing valuable information) or cyber (e.g. when deleting a file also deleting it from the recently deleted files). Furthermore, working remotely includes physical and cyber elements as well. A physical aspect is the different environment, a cyber element is the different network used. However, both topics are coloured white, only mentioned by one source. Therefore, they will not be included in the program.

The delivery method consists of five possibilities: conventional, video, online, game and simulation. All are discussed earlier in Section 2.4.3. For this program it is chosen to combine the simulation and game delivery method. Regarding the simulation there were two options, the user can be aware or unaware of being in the simulation. For this program it was chosen to let the user be aware of the simulation, partially because the VR makes an unaware option quite difficult. The simulation will include various tasks and monitor the user’s actions. The game delivery method is part of the surrounding activity. Therefore, it is not actively included for instance through the form of gamification elements. The use of

badges and leader boards seemed unnecessary and potentially leading to social stress or competition, which is not the aim of the program.

Regarding the used platform there were multiple options, the 2 main considerations were neosVR and Unity. For this program it was chosen to develop in neosVR because of multiple reasons, which will be elaborated upon in the realisation section.

4.4 Experience and interaction

The experience of the program can be subdivided into three elements. Firstly, what it looks like, because it will be a simulation the environment should be reflective of a real-life situation. Therefore, it was chosen to use the most common working environment, an office. Secondly, the experience is dependent on the point of view. Although an attacker point of view can be a new approach it does not reflect a real-life situation where users want to keep their information safe. Furthermore, there is an ethical dilemma included, when educating people on things they should improve you simultaneously teach them things they can do to vulnify an organisation. Although this is a side effect of education it seems irresponsible to increase this risk by also designing the game from this point of view. Because of these two reasons it was chosen to take a protector point of view. It optimally simulates a real-life situation. This includes the user having no fixed place in the environment, able to interact with other avatars and the inclusion of both physical and cyber elements. VR is also part of the experience and determines the way of interaction with the program. VR consists of a 360 view which one can interact with by turning around. Furthermore, the VR setup contains 2 handheld controllers which allow the user to interact with objects in the virtual environment. Additionally, a virtual toolbelt will be included that gives the user access to everyday objects such as keys or an access pass. Another option was to provide interaction with non-VR native controllers such as an Xbox controller. This will not be included in the program because the handheld VR controllers provide a more real-life perspective. For example, in real-life the user will open a cabinet with their hands instead of by pushing a button on an Xbox controller. The handheld VR controllers come closer to this experience than any of the non-VR native controllers.

5. Specification

In the specification phase the defined product idea was taken and converged to a specification of the product providing an overview of the functionalities and experience. This product specification is the foundation for the realisation of the program in Section 6. The specification starts by performing a FICS analysis which specifies the various elements of the program. It continues by describing the applied education method. After which the system is visualised using a flow chart in the system architecture. Subsequently, the user experience is elaborated upon in a user scenario. Lastly, requirements are set up which define the things the program shall be able to do.

5.1 FICS analysis

The specification starts by performing a FICS analysis, it provides an insight into the functions of the system categorised in 4 different groups: functions, interaction, content and style.

5.1.1 Functions

The main function of the program is to educate users on cybersecurity. To achieve this the system provides an interactive 3D environment in which the user should perform various tasks. The user's performance is tracked and feedback on choices is presented. To realise this experience the system will have the following functions:

- The system provides an interactive 3D environment.
- Cybersecurity related tasks are presented to the user within the environment.
- User performance on the tasks is kept track of and feedback is presented accordingly.

5.1.2 Interaction

The experience starts by introducing the user to the program. Before entering the simulation, the user is given the following explanation: “You are going in a VR simulation where your cybersecurity skills will be tested. You will get several tasks and should make decisions just like you would do in a real-life situation”. This is followed by a short description of the controls. After this introduction the user can start the program and perform the tasks. Interaction is provided through the VR headset, which enables the 360 view. Furthermore, the user can interact with the environment using the two handheld controllers. They give the opportunity to walk around, grab objects and complete the tasks.

5.1.3 Content

In the ideation the content has been specified into topics that are most important to include. Due to time constraints, it was chosen to shorten this list, it provides certainty that the concept can be realised. Furthermore, this list of handled topics can be expanded when the realisation time is less than expected. The chosen topics are password management and removable media, this way both the cyber and physical domain are represented, which combination is one of the strengths of the program.

Password management is a very important element towards keeping your data safe. ENISA [52] created 10 recommendations to improve password security. One should enable multi factor authentication, not re-use any passwords and use single sign-on functionality. Furthermore, the use of a password manager and appliance of strong and unique passwords are important. Passwords should be changed when appearing in existing data breaches and password reminders should not rely on easy retrievable information. In public spaces one should use a VPN when accessing personal information with the public internet, be aware of surroundings when filling in passwords and not leave devices unlocked. Some of these recommendations are also mentioned in the expert interviews, therefore, these subtopics will be included in the program. These subjects are multi factor authentication, no re-use of passwords and the importance of strong and unique passwords.

The learning objective of this topic is to get to know what good passwords are and the importance of enabling multi factor authentication. This goal will be achieved by letting the user perform tasks which test their knowledge on passwords. An overview of the specific tasks including the potential options are elaborated upon in Table 6. It starts with the user turning on the computers. Secondly, the user should change the password. When this task would let users insert their own password there is the potential that they fill in one of their currently using passwords. Naturally, this is not the aim of the program and ethically irresponsible. In order to simulate this action, but remove the included danger, it was chosen to implement a multiple-choice option. This way the user still has freedom of choice but does not run any risk. The multiple-choice options will include both strong and weak passwords. A strong password contains more than 8 characters including alphanumeric as well as special characters [53]. A password can be weak because of its length, re-use or basicity. The user can choose between eight different passwords, one of which is optimal for cybersecurity (see Table 7). The third task focuses on multi factor authentication, the computer will let the user choose to enable this multi factor authentication.

The second topic is removable media, it is a cybersecurity subject from the physical domain. Removable media are portable objects used to store information. As mentioned in Section 4.3 there are two main risks involved. Firstly, removable media including stored information can be easily lost. Secondly, they can be left for others to find with malware included. Common examples of removable media are USB sticks and SD cards.
Since the first risk is difficult to treat in the intended program because it is based on taking care of your belongings, the focus will be on the second risk.

The learning objective of this topic is to gain knowledge on the dangers of removable media and how to adequately handle them. This learning goal will be achieved by letting the user perform the following task. An unknown character enters the office and notifies the user that a USB found has been found on the floor in one of the hallways and placed in one of the desk drawers. This task is a bit more vague than those previously mentioned, this is because this situation usually does not contain any tasks. In a real-life situation one would accidentally find a USB stick. The character walking in notifies the user of this object and sets the user for a choice on how to handle the USB. The cybersecurity safe choice is going to the IT department and handing in the USB stick. The most cybersecurity unsafe choice is plugging the USB stick in the USB hub next to the computer.

Table 6: Content specification into tasks and options

Content	Situation	Explicit tasks	Options Right Wrong Unclear
Password	Computer is turned off on the desk.	Turn on the computer.	Turning on the computer. Not turning on the computer.
	Computer shows a pop-up screen where the user can change its password.	Computer asks “Your password expires in 1 day, change your password”	Changing password to the optimal option. Changing password to the non-optimal option.
	Computer shows another pop-up screen where the user can choose to enable multi factor authentication.	Computer asks, “Do you want to enable multi factor authentication?”	Not enabling multi factor authentication. Enabling multi factor authentication.
Removable media	Character walking in notifying the user of the found USB.	User has to handle the unknown found USB	Handing USB to the IT department. Plugging USB in the USB hub next to the computer. Picking it up doing none of the above.

Table 7: Multiple choice password options

Basic	Re-used	>8 alphanumeric characters	<8 alphanumeric and special characters	>8 alphanumeric and special characters
Welcome123!	Car00Volkswagen09 (also used for your email account)	2poA30fjv9U8Nh	9i_qH	+1aW_e0-Q8p_2O7t Optimal password
1234567890	Qw0zX-9 (also used for your game account)		p-6fT	

5.1.4 Style

The appearance of the environment is key in providing the wanted experience. The program asks users to enter the simulation making decisions just like they would do in a real-life situation. Therefore, to make the experience as close to a real-life situation as possible, both the environment, building and furniture should be similar to their real-life counterparts. To

define the appearance a mood board was created which is blurred because of copyright (see Figure 8). The three colours in the top right: beige, black and grey, are the key colours used, they are calm and fitting for an office environment. The three materials in the bottom left: concrete, wood and brick, provide warmth and character. Examples of implementations are the images in the middle, they show how a combination of colours, materials and furniture can represent a professional, modern office.

Figure 8: Mood board appearance (blurred because of copyright)

At the foundation of these colours, materials and furniture there is the building and floor plan. Additionally, this floorplan should fit the tasks that have to be completed. Therefore, it should include an office space and a space for an IT department. Furthermore, it has to include a desk and a computer. This floorplan is elaborated in Figure 9. Note that only the large and essential items are placed on this floorplan, decorative items are not included.

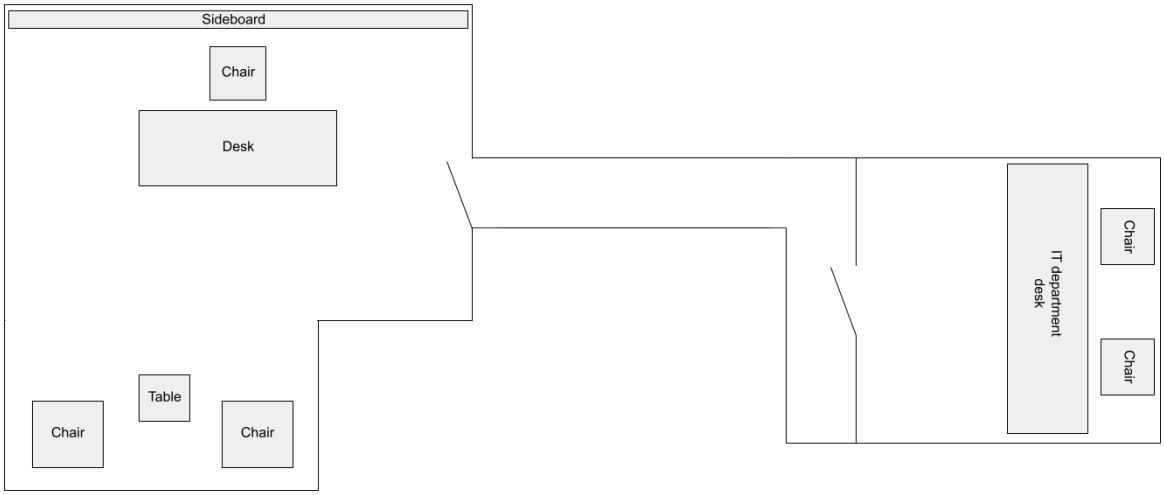


Figure 9: Floor plan including large and essential items

5.2 Education method

Although the defined tasks test one's cybersecurity skills, they do not educate them on these topics. Firstly, instructions can be provided prior to the program so users are educated before they perform the tasks. Secondly, feedback can be provided after they performed a task to gain knowledge on the optimal decision and compare it to their current behaviour. Since the second option allows users to clearly see the difference between their current behaviour and the optimal decision, this is the chosen method. However, it is important here to conform to one of the aforementioned values, balance between autonomy and feedback. The users should have the autonomy to make their own decisions. They should not be influenced in their decision-making process when performing the tasks. Therefore, there are two options for the timing of the feedback. The first option presents the feedback after the tasks of one topic ended and before the next topic starts. The second option is to present feedback regarding all choices after all tasks of all topics are completed. For this program it was chosen to adopt the second option. Temporarily pausing the tasks to give feedback can be interrupting for the user. Furthermore, providing all feedback at the end gives a structured overview of the things the user does well and the areas the user can improve. If in a following phase the other identified topics would also be implemented, increasing the total duration of the program, it may be important to reconsider this decision. The increased duration between the completion of a task and the presentation of feedback may be too long, which can cause insufficient impact on the user behaviour. In the current program the feedback will be provided by displaying the user’s choices next to the optimal choice grouped by topic.

5.3 System architecture

To visualise the specified program a flowchart was created (see Figure 10). From this flowchart it becomes clear how the user is introduced to the concept. Furthermore, it visualises how tasks progress and choices are implemented in the feedback.

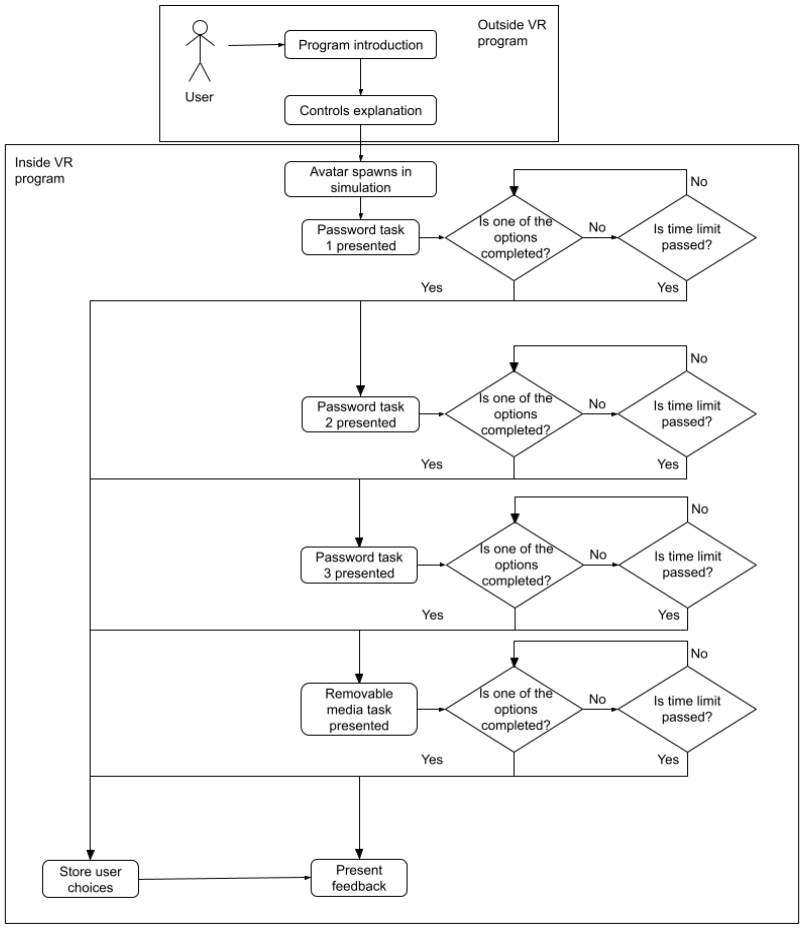


Figure 10: Flowchart specified program

5.4 Scenario

The above flowchart describes the program from a systems point of view. To get a better understanding regarding the user experience a user scenario including a persona has been created.

Name: Tom van Velde
Age: 43
Location: The Hague
Occupation: CEO of a law firm
Family: Married with 2 kids

Tom van Velde is a 43-year-old man living in the Hague with his wife and 2 kids. For 8 years he has been the CEO of one of the biggest law firms of the city. In these 8 years a lot of things have changed, especially regarding technological advancement. When Tom started this position most of the employees mainly used paper to prepare lawsuits and communicate with their customers. Over time this has shifted digitally, currently most employees use computers in their daily work and communicate with their clients by online services. Although this change increases efficiency Tom is aware of the dangers. To decrease the chance of cyber breaches and protect all valuable data Tom wants all employees to follow a training on how to be as cybersafe as possible. When searching on the internet for potential training programs he found this program. He thinks it is a good fit because of the interactivity and

close to real-life experience. After the entire system is realised at the firm's location, Tom asks the employees of one of the departments to participate in the cybersecurity training program.

Name: Mark de Jong
Age: 24
Location: The Hague
Occupation: Intern at the law firm
Study: Last year of law school
Family: Lives with his girlfriend

Mark de Jong started as an intern at the law firm at the beginning this year. He is graduating law school and hopes to become a full-time employee when he finishes his studies. Last week Tom sent Mark's department a message that they were invited to participate in a cybersecurity training. Mark was not really looking forward to having another thing to complete but was willing to participate to improve the organisational cybersecurity. When Mark read on and got to know more about the setup of the program, he became more interested. A week later, in his time slot, Mark went to the location curious about the program and the role of VR. He first got an introduction to the program after which the controls were explained. Mark was excited to use this technology to gain knowledge on the important topic of cybersecurity.

When Mark started the program, he saw he was located in an office, it looked similar to a real-life environment. Then he saw the first task, he had to turn on the computer. Mark looked around and saw a computer sitting on the desk, he used the controller to walk towards it. The computer had a power button on the bottom right, just like his own. He moved his hand to turn it on and it worked, he was amazed by how his real-life movements influenced the virtual environment. The computer showed a message, he had to change his password because it almost expired, there were 8 different options given. Mark looked at the options and laughed when he saw the ‘1234567890’ password option, that would not be a safe decision. With his existing password knowledge, he also eliminated the ‘Welcome123!’ and ‘Car00Volkswagen09’ options. However, he did not know which of the remaining five passwords would be the best. Because of this lack of knowledge Mark just picked one and chose the ‘9i_qH’ password. The computer showed another pop-up, whether he wants to enable multi factor authentication. Mark thinks the multi factor authentication is irritating to use and therefore does not enable it. The computer screen turns off and a character walks in. The person tells Mark that a USB was found on the floor in the hallway, it was thought it might be his, so they put it in one of the desk drawers. Mark moves towards the drawers and finds the USB in the middle drawer. He picks it up and moves towards the computer, but then he stops. He thinks about the task and concludes that it would be unsafe to plug an unknown USB in his personal computer. He continues by thinking of a better way to handle the USB, he concludes he should give the USB to someone with more knowledge. He remembers that the IT department is at the end of the hallway, they would know how to safely handle the USB. He opens the door, walks through the hallway and enters the IT department room. At the desk he sees a box where one can leave potentially cybersecurity dangerous objects; this is where he leaves the USB. Mark walks back to the office when a feedback screen pops up. He sees that his recent decision regarding the USB was optimal, but that he can improve on the password management domain. He learns that a strong password has more than 8 characters which should be a combination of alphanumeric and

special characters. Furthermore, he learns the importance of multi factor authentication. He clicks the button that he has read all feedback and sees that the program has ended. Mark takes off the headset and walks back to his own office, thinking about the things he has learned. In his office he turns on his computer and enables multi factor authentication for his email account. He is happy with improving his and the organisation's cybersecurity.

5.5 Requirements

To conclude the specification, program requirements are set up. These are split up into functional and non-functional requirements.

5.5.1 Functional requirements

Functional requirements define practical functions the program should be able to perform.

1. The program shall use user input from the handheld controllers and/or VR headset to walk and look around and grab things in the virtual environment.
2. The program shall work with the VR hardware of an Oculus Quest 2.
3. The program shall display a virtual environment including various cybersecurity related tasks.
4. The program shall combine the physical and cyber aspects of cybersecurity.
5. The program shall provide feedback on user choices after the last task is completed.

5.5.2 Non-functional requirements

Non-functional requirements define non-functional things the program shall include.

1. The virtual environment shall look like a real-life environment. Participants will be asked to score this on a 1-5 Likert scale, the average score shall be over 3.
2. The program shall educate users on the defined cybersecurity topics. To measure this the participants will complete a questionnaire on the cybersecurity topics before and after the program. Performance shall be increased.
3. The program shall be user friendly therefore scoring an average SUS score of over 68.

6. Realisation

In the following section the realisation of the earlier defined program is described. It starts off by delineating the chosen platform including installation and main controls. It continues by describing the process of realising the program, this is divided into eight aspects: the office building, 3D models, lighting, interaction, guidance, characters, outside environment and sound.

6.1 Platform

There are various platforms which could be used to realise the VRCyberEducation program. The two main competitors were NeosVR and Unity. Eventually, it was chosen to use NeosVR for a variety of reasons. Firstly, NeosVR provides various ways to make objects physically interactable. Secondly, distribution of the created program will be easier. Users only have to download the openly accessible program Steam, after which the VRCyberEducation program can be opened. Unity will require creating a build of the program which should be made accessible somewhere and therefore needs a distribution platform like a website.

NeosVR can be installed on windows and Linux. Since there was only access to Apple MacBooks with IOS, the installation became quite complicated. The full process of installing NeosVR on MacBook is displayed in Appendix B.

NeosVR is a program which allows one to create 3D worlds from an in-game perspective. Through the use of various tooltips, one gets access to various specific functions, they are visualised as thimbles. The most important tooltips are the developers, Logix and material tooltip. The developer's tooltip enables one to scale, rotate and move objects using gizmos (see Figure 11A). Furthermore, one can create new objects and view their properties on an inspector panel. The Logix tooltip gives access to important features of the visual programming system (see Figure 11B). The material tooltip, as the name implies, enables you to add and edit textures and materials of objects (see Figure 11C).

Figure 11A: Developer's tooltip and menu

Figure 11B: Logix tooltip and menu

Figure 11C: Material tooltip and menu

6.2 Process

The process of realising the VRCyberEducation program in neosVR started by learning the controls and possibilities of the program. There are many tutorials online that discuss the various elements of the program. Most watched tutorials are by probableprime, who handles both basic and advanced topics in a clear and understandable way. After learning the elemental information on the program, the realisation was started. However, this is an iterative process, whenever things were unclear, it was circled back to tutorials and the Neos wiki to gain more information on the specific subject.

6.2.1 Office building

The realisation started by creating the environment. After an extended search on two 3D model websites, Turbosquid and Sketchfab, several models were identified which had the potential to be the foundation of the office building. However, during the implementation of these models none proved to be fitting for the goals of the space. Therefore, the choice was made to not use a pre-existing model and create it manually. Since neosVR is not an optimal program for creating 3D models Unity was used instead. The model has been designed based on the aforementioned floor plan in Figure 9 combined with the defined style. The created model (see Figure 12) was then exported to an fbx file, after which it could be imported and textured in neosVR (see Figure 13). Furthermore, a door was added to close off the office from the hallway. A second door was placed at the end of the hallway to prevent the user from leaving the building while maintaining the idea that the space extends beyond the visible rooms.

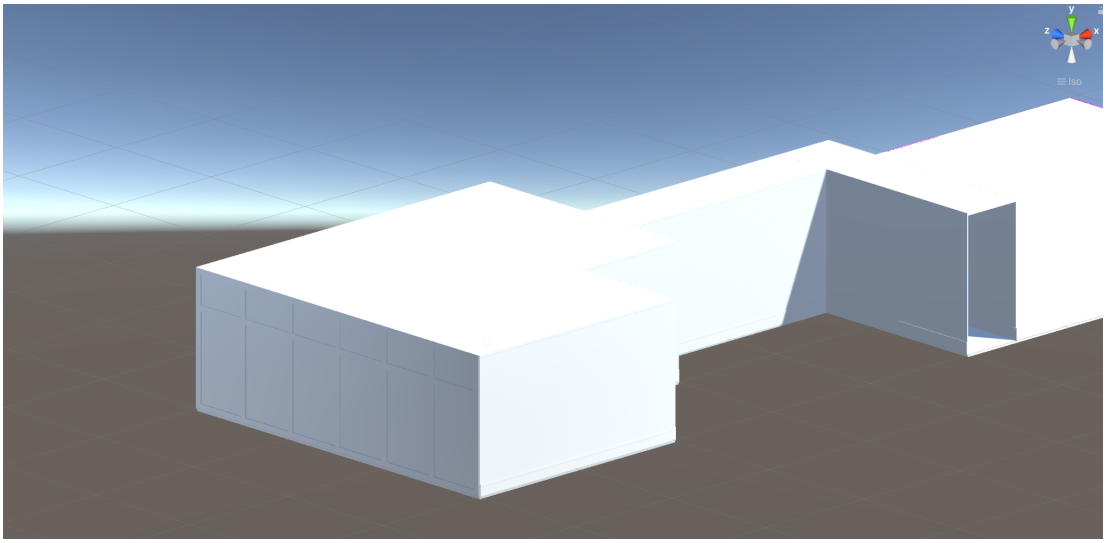


Figure 12: 3D model office building Unity

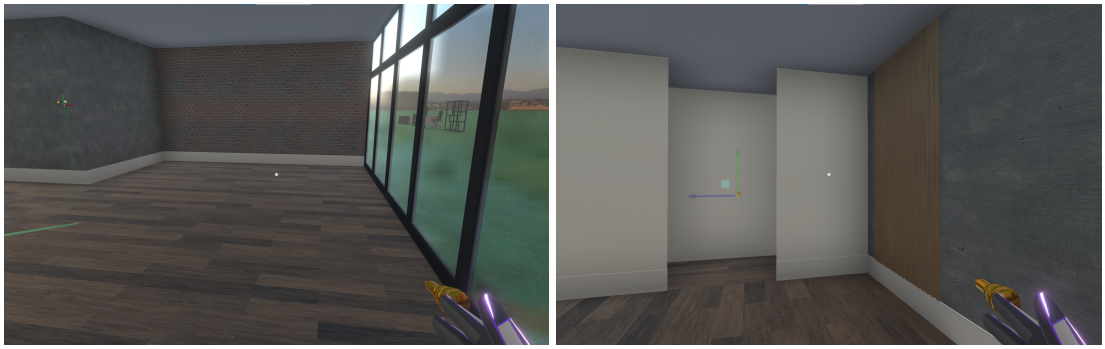


Figure 13: 3D model office building imported and textured in neosVR

6.2.2 3D models

Since the office building was completed, it had to be filled with objects. They could either be decorative or have a clear in-game function. However, it was key that both were as close as possible to their real-life counterparts. There are various objects that have a clear function, they are crucial in the completion of the tasks. Firstly, the computer monitor, which is necessary for the password management subject. For the removable media topic there are four important objects, the USB stick, the USB hub, a box to dispose of the USB stick and a desk to store the USB stick. All functional modes are displayed in Figure 14.

Figure 14A: Monitor Figure 14B: USB Figure 14C: Desk Figure 14D: Cyber unsafe objects

To further decorate the building various other 3D models were included. This includes desk chairs, bookshelves, armchairs, a side table, wall shelves and a second desk. Smaller decorative items are paintings, folders and plants. Lastly, a character collider was added to each object, this made sure that the user cannot walk through the objects (see Figure 15 for the fully decorated space). The handmade 3D models are the removable media disposal box and the paintings. All not handmade 3D models are used according to their licence and referenced in Appendix I.

Figure 15: Environment fully decorated

6.2.3 Lighting

Now that the office building was created and had been fully furnished and textured, lighting is added. Combining the desired style and Neos' lighting possibilities resulted in the following three lights: ceiling spots, desk lights and decorative light bulbs (see Figure 16). The ceiling spots are the main source of light and illuminate the entire space. Furthermore, their minimalistic and modern design fits the space perfectly. The desk lights are for the illumination of specific places and additionally to further decorate the area. This lamp also uses spot lighting since the top of the lamp directs all light downwards. The last source of light is from the light bulb lamp, this lighting has no specific function besides decoration. Furthermore, this is the only lamp that uses 'round' lighting since the glass bulb does not restrict any of the light.

Figure 16A: Ceiling spots *Figure 16B: Desk light* *Figure 16C: Decorative light bulb lamp.*

6.2.4 Interaction

All aforementioned changes created a non-interactable, static environment. However, to monitor and educate one's cybersecurity knowledge and skills, the user should be able to interact with the environment, more specifically, perform the tasks. NeosVR provides multiple ways to include interactable objects. The main way is through Logix, Logix is Neos'

visual programming system. One can equip the Logix tooltip which allows you to create Logix nodes of objects and connect them to others.

The first task regarding password management uses the functional model of a computer monitor. The first sub task asks the user to turn on the computer, therefore there should be a power button, the used model did not include this button, so it was handmade in neosVR and added to the monitor. Furthermore, a static model does not include an interactive screen which can be turned on and off. Therefore, a separate screen was created using a Neos' canvas with a windows background sprite. On this main canvas different images can be placed who each have their own properties and components, representing the various pop-ups.

The first subtask toggles the boolean value 'active' of the screen, turning it on and off. Firstly, a button canvas is created with all alpha values set to 1, being invisible. This canvas is located just above the power button. The button components are extracted to a Logix node, and a buttonEvents node was added. Whenever one presses the button, an impulse will be sent. Secondly, a boolean latch node is added, which toggles the boolean value when this impulse is received. Lastly the main screen node is extracted such that its active component can be influenced. After the screen is turned on the first pop-up should ask whether the user wants to change their password. This requires a screen with two buttons, a 'yes' button to set the password options screen to active and a 'no' button to skip to the multifactor authentication screen. Both buttons are created using a Neos' canvas, under which an image and text are placed. The canvas sets the size of the button and creates a border, the image includes the button component and sets the button colour, the text displays the textual content on the button. Furthermore, the style of the buttons adheres to the style of windows buttons, increasing the feeling of a real-life situation. To make the buttons interactable, the aforementioned Logix approach is used. However, it turns out that this approach does not support multiple buttons directly influencing the same component. For example, all password options should lead to the same screen, setting the multifactor authentication screen to active. More research gave notice that Neos' includes a second way to program simple UI elements. One can add a specific component to the object called a 'buttonvalueset<boolean>', it sets a boolean value to true or false whenever the button is pressed. This method does allow multiple buttons to influence the same object. Therefore, this is the method applied to the buttons on the pop-ups. For example, on the popup asking to change the password, the 'no button' sets the current screen to non-active and sets the multifactor authentication screen to active. All created screens and their relations are displayed in Figure 17 and 18.

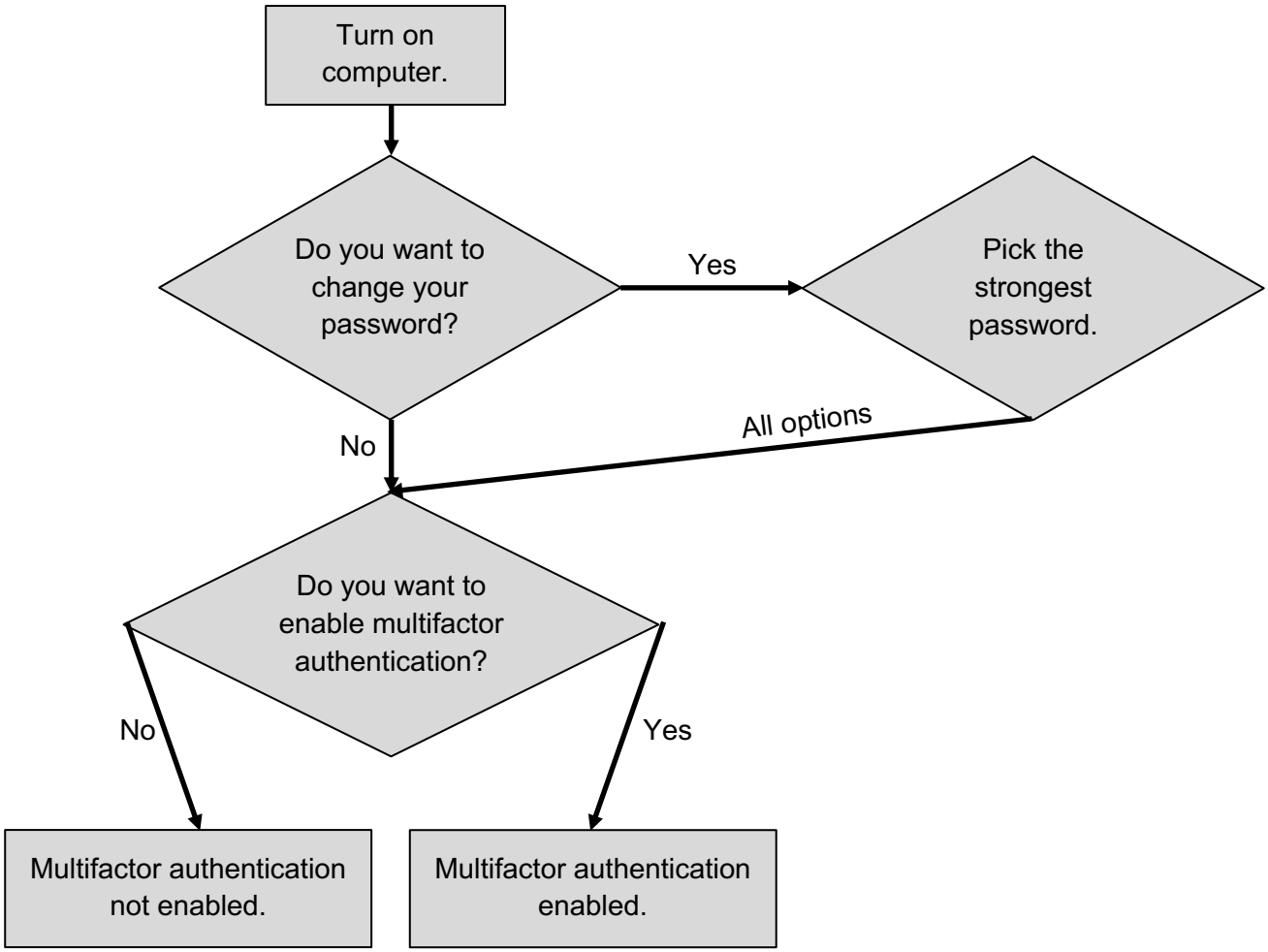


Figure 17: Relations computer screens

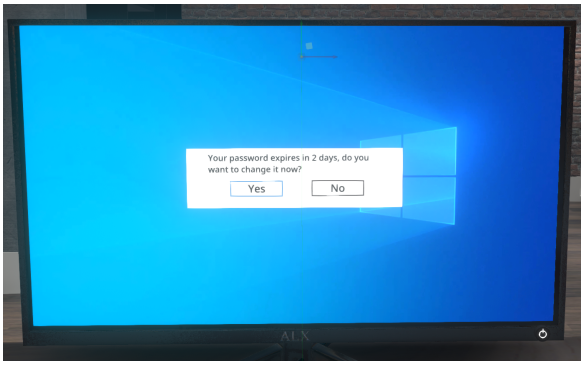


Figure 18A: Choosing new password

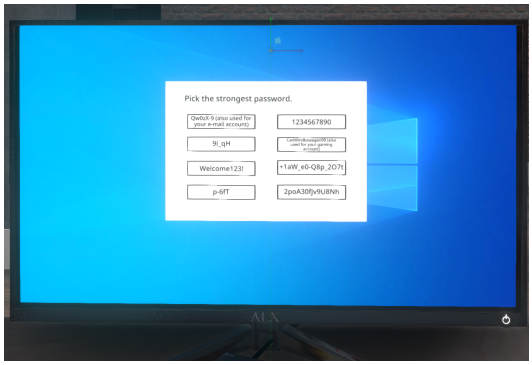


Figure 18B: Options new password

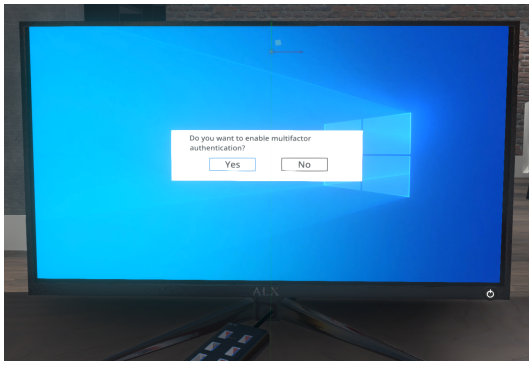


Figure 18C: Multifactor authentication

The second task starts by another character walking in the room, this person lets the user know that they have found a USB on the floor in the hallway and thought it was theirs, so they put it in one of the desk drawers (see Figure 19). This element shows one of the strengths of the program, the combination between the virtual and physical aspects. Furthermore, the person walking in increases the idea of a real-life situation. Normally, one does not find an unknown USB through a specific task either. The character walking in is created through a motion capture tool, this movement is then installed to an avatar whose animation can be turned on and off through a checkbox. The start of the character walking in can be triggered by two things, the user finishes the last password management subtask or the related time limit is reached. Furthermore, the motion capture tool does not include capturing any sound. Although alternatives such as text have been considered, speech is the most natural way of conveying the message. Therefore, a voice generator was used to create speech fitting for the chosen character. This sound file was imported and triggered to start playing when the character walks in the office.

Figure 19: Character walking in

The user will continue by opening the drawers. Therefore, the first thing that should be programmed are the desk drawers. To do so a slider component was added to a drawer, just like the name suggests, it allows an object to slide along a defined range. Since the drawer should only move along its z-axis, all other ranges are set to 0. However, the range allows the drawer to move that distance along the axis on both sides. This is incorrect, the drawer should only move one way, to fix this an offset was added above the drawer. Afterwards, the same method was applied on the other desk drawers.

The task continues by the user finding the USB, picking it up and choosing how to handle it. Since the user is informed about the IT department in the ‘getting started task’ they can bring the USB there. Secondly, they can plug the USB in the USB hub, like one would normally do with their own USB. To program this there should be checked for a collision between the USB and either the USB hub or the removable media disposal box. A box collider was added to all three objects. The collider of the USB was set to active; this means it checks each frame whether it collides with something. The colliders of the IT department box and USB hub were set to static. This combination of collider types makes sure that the collision is detected. For example, two static colliders will not notice when they collide with each other. Secondly, these colliders should be programmed, in Figure 20 the Logix graph is displayed. On the start of a collision, it is checked whether the other collider is the USB hub, if this is the case a boolean value for a piece of text is set to active. This notifies the user that they completed the tasks. Additionally, on collision end, this text is set to inactive again. The Logix graph for the collision between the USB and IT department USB box is the same. The graphs are combined by one node, since this is the last task, the feedback screen should be presented on completion. Therefore, when there is a collision with one of them, this screen is set to active.

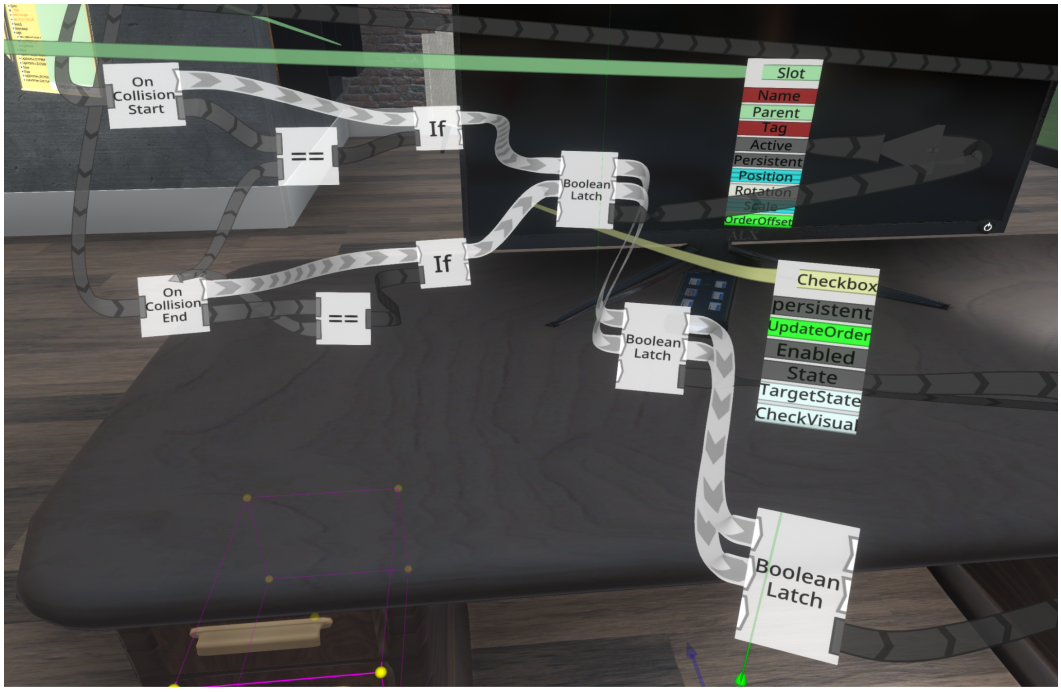


Figure 20: Logix graph USB collision.

When both tasks are finished, the user receives feedback on their performance and coaching on ways to improve. This aspect is key in educating the user on their current mistakes and opportunities to improve. The feedback is presented through a feedback screen, this screen shows the user's choices and explains the optimal choice.

The screen is created using a canvas, just like the computer screen. However, since there is much information which should be clearly ordered, layout elements were implemented. The first horizontal layout component orders the child layout elements in rows. For most results this is sufficient, but the password options need some more organisation. Therefore, one of the rows includes a vertical layout component with two child layout elements, resulting in 2 columns within the row. Within each column another horizontal layout component is added to divide the column into 4 rows. A scheme of the layout is displayed in Figure 21, the resulting screen can be found in Figure 22.

Each task is represented and accompanied by a checkbox. The checkboxes for the password management are programmed using the buttonvalueset<boolean> components. For example, when 'yes' is pressed to enable multi factor authentication this results in progressing to the next screen but also checking the accompanying checkbox. The checkbox for the removable media task is programmed in the existing Logix graph. When the collision with the IT department USB box is true the checkbox is set to active. The checkboxes provide a clear overview of the user's performance. However, to educate the user on the correct behaviour each task includes an explanation section which explains the optimal choices regarding the various subtasks.

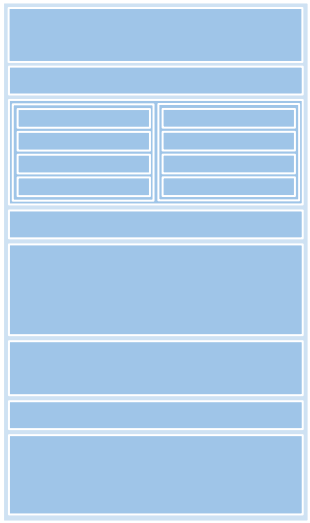


Figure 21: Layout feedback screen

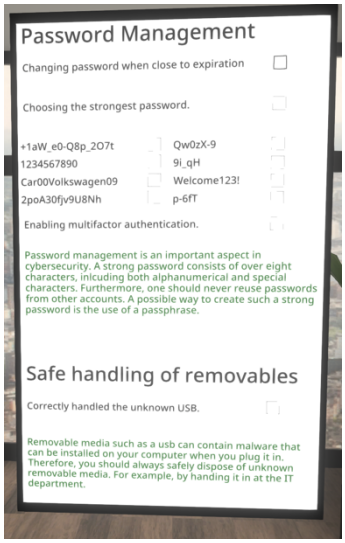


Figure 22: Feedback screen.

As discussed in Section 6.2.1 two doors are added to the model in Neos. They close off the office and building from the rest of the environment. However, one of these doors should be opened by the user to gain access to the IT department room. To achieve this a joint component is added to the door (see Figure 23). The range is set to 90 degrees along the y-axis, this means the door can move 90 degrees back and forth along this axis. However, a door should only open 90 degrees to one side. Therefore, a rotation offset is placed above this object which limits this extra movement. The current advancements lead to a door which can be grabbed and opened one way. However, a real-life door only opens when the handle is pushed down. Since an important aspect of this program is its closeness to a real-life situation this should be included as well. To do so, a similar approach was applied to make the handle rotatable along one axis. Now, the door had to be limited to only open when the handle was down. When the handle is above a certain angle the joint component of the door is set to active which enables the user to move it.

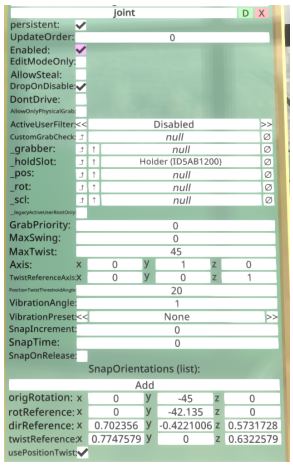


Figure 23: Joint component door

6.2.5 Guidance

The aforementioned interactions are solely for specific tasks or feedback. However, the user also needs some guidance in getting used to the program and advancing to the next task. The main guidance in the program will be provided through a canvas placed on the wall in the office. This screen displays the current task, making sure that the user is always aware of it.

Most users will not have much experience with VR, although controls can be explained outside of the program it is beneficial to check whether the user understands the controls before the tasks are started. Therefore, the program begins with a simple ‘getting used to the program’ task. It asks the user to walk to the IT department and meet Susan. In the IT department room, the user is asked to pick up a plant and whether they understand the controls (see Figure 24). This

Figure 24: Getting started

tests the user on their ability to move around and grab objects, crucial controls in completing the tasks.

To make sure that users do not get stuck on a certain task a timer has been implemented. Whenever the task is not completed before the timer is up, the user is asked to continue to the next task. Since the tasks are quite simple and do not require many steps, both can be completed within a minute. However, to provide the user with some time to think both timers are set to two minutes. When the user does not finish the password management task within 2 minutes the computer screen will display a 'time is up screen' and the character starting the USB task is set to active. Regarding the second task, when 2 minutes have passed, the USB is turned inactive and a text appears for 8 seconds that lets the user know the time is up. Furthermore, since this is the last task, it also turns the feedback screen to active.

The last element of interaction is invisible for the user, but plays a key role in the program, a reset button. When the user interacts with the program they change a lot of things, such as the active computer screen or USB location. The reset button resets all interactable objects to their original state. This way, the program can be easily reset for the following user.

6.2.6 Characters

Since it is a VR program, users will be able to see their own avatar when wearing the headset. It is important that this avatar fits the environment, to enhance the real-life situation of the program. The avatar should represent a businessman or woman. The option to let users choose between these two to further increase the real-life ability was considered. However, the decision has been made to not include this. It may start of the simulation on the wrong foot, inciting the idea of playing like that character instead of making decisions like they would normally do. Furthermore, it would be impossible to create a few avatars to choose from, that many can resonate with. Issuable elements are among others gender, weight, length and clothing style. To not exclude anyone, this would mean there should be many more characters to choose from. However, letting users choose between 10+ avatars distract them from the actual aim of the program. Because of these reasons it was decided to use a universal standard character which fits the environment (see Figure 25). This avatar does not solely represent a specific gender and has an average weight and height. Furthermore, the clothing style fits the office environment while still being casual.

Figure 25: Avatar

Apart from the user's avatar, the current environment does not include any other characters that are constantly around. This is fitting for the individual office but not for the IT department. To increase the feeling of a real-life situation two characters are added in the IT department area. Since it would not be realistic to have two static characters in this room, they are both animated. The woman is animated to look on her computer screen, blink and point to the USB disposal box on the desk whenever the user walks in (see Figure 26). This way, she makes the user aware of this object in a very natural way. The man on the right is animated with an idle movement, he types on the computer, blinks and looks around (see Figure 26). Both characters have an appearance that fits their environment, they look like businessmen/women. The animations were created in Blender before the models were imported in Neos.

Figure 26: Animated character on trigger (left), animated idle character (right)

6.2.7 Outside environment

All previous developments have created a fully functional environment. However, there also are two non-functional elements included. The outside environment is not something the user directly interacts with but does play a key role in setting the right atmosphere. For example, when the user looks through the windows and only sees grey, the standard 3D environment, this would not match the office ambiance set by the inside environment. To come as close as possible to a real-life situation it was chosen to use a skybox. A skybox is a fully surrounding 3D picture that can simulate a specific environment. The chosen skybox displays an urban environment and places the office between various skyscrapers, a fitting location for an office.

6.2.8 Sound

The second non-functional addition is the inclusion of sound. A fully silent environment is not representative of a standard real-life situation. Furthermore, it enables users to hear sounds sourcing from the actual environment which can be distracting. Therefore, it was chosen to include an ambient sound that fits the environment, like background office chatter. However, the environment includes an individual office and an IT department, no communal work areas. Furthermore, it would be weird if the sound from these areas would resound in the individual office. Therefore, it is chosen to not include background chatter in the individual office. However, since the IT department does have two animated characters seated behind a desk, the chatter sound is included in this part of the environment. Secondly, background traffic sounds are added, they are fitting because of the urban environment. Whenever it is silent inside you can always hear sounds from outside such as car horns and engines. This sound is included throughout all areas of the environment. Combined, the two sounds provide an appropriate ambient sound which close the user off from the outside world and further enhance the real-life situation of the environment. These sounds are constantly looped and start from the beginning whenever the reset button is pressed (see Figure 27A for the Logix). Furthermore, after implementation it seemed that the traffic sound was missing something, a siren, a common sound in an urban environment. Since no superior alternatives could be found, a sound effect was added, which plays every 30 seconds (see Figure 27B for the Logix).

Figure 27A: Logix ambient sound

Figure 27B: Logix added sound effect

7. Evaluation

To find out what the effect of the created program has on one's cybersecurity knowledge and awareness an evaluation is set up. The impact is measured by capturing one's cybersecurity knowledge before and after being exposed to the VRCyberEducation program (the full procedure is explained below in Section 7.3). Cybersecurity knowledge and awareness is measured by the validated HAIS-Q. Since the VRCyberEducation program is limited to two topics, questions related to these subjects are extracted from the questionnaire. Furthermore, the evaluation researches the usability of the created program. The potential of large-scale application combined with short user interaction with the program increases the importance of high usability. This will be measured using the SUS questionnaire and is therefore included in the questionnaire after exposure to the program. The research is approved by the EEMCS ethical committee under RP 2022-117.

7.1 Participants

To evaluate the created VRCyberEducation program participants are recruited. Each participant has to conform to the following inclusion criteria. The participant must speak and understand English since this is the language used in the program. Secondly, based on the research performed by Bullee et al. [54] it has been decided to include years of service in the inclusion criteria. Bullee et al. [54] found that fewer years of service leads to a higher compliance in phishing, therefore performing worse at cybersecurity. Since the main goal of this evaluation is to find out what the effect of the program is on one's cybersecurity performance, it has been decided to include participants that generally perform worse. This makes sure the average participant has room for improvement and the true effect of the program can be measured. The specific accompanying inclusion criterion is that each participant should be in service of an organisation for less than two years. Since recruitment was quite complicated regarding this criterion, not all participants are fully compliant of it. However, all easily fit the shortest years of service category defined by Bullee et al. [54] of less than 7 years. Furthermore, there is an exclusion criterion applied, VR can cause motion sickness, similar to motion sickness in vehicles. Anyone prone to motion sickness in any context is excluded from the research. The participants are not compensated in any way for their participation and are recruited in various ways. UT employees are contacted directly through email by one of their colleagues. UT students are recruited similarly but through a different platform, they are contacted through the program specific contact groups. Lastly, acquaintances are recruited directly.

The total sample size of the research is 16. Furthermore, the sample consists of an equal division between male and female participants. There are four separate age groups included, as is displayed in Figure 28. The sample represents various highest levels of completed education and areas of expertise (see Figure 29 and 30).

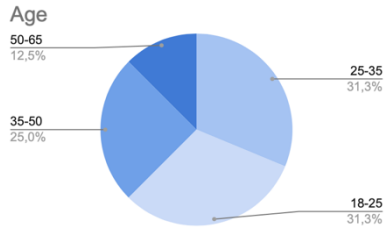


Figure 30: Age participants

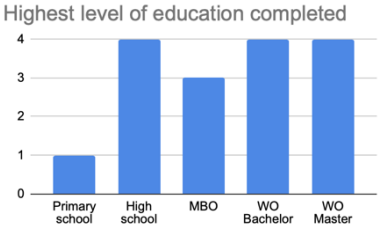


Figure 29: Education level

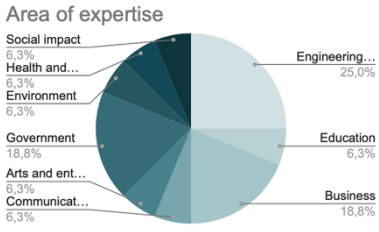


Figure 28: Area of expertise

7.2 Materials

The evaluation with each participant needs to be as similar as possible, therefore the same setup is used every time. The equipment consists of a laptop and an Oculus Quest 2 Business Edition. The laptop is a Lenovo legion 5 pro with a NVIDIA GeForce RTX 3050 graphics card. These specifications are sufficient to run the highly intensive program for the Oculus headset. The laptop runs on the operating system of Windows 10. In addition, there are various programs crucial to run NeosVR on Oculus. Firstly, NeosVR and SteamVR which can both be downloaded through Steam. Furthermore, the Oculus headset requires the Oculus pc program to link with the laptop. Since the latest update does not support the business edition headset, an extra software update provided by Oculus support is required. The Oculus Quest 2 Business Edition headset runs on the latest software version 37.0. The Oculus headset is connected to the laptop using the airlink or a long USB c cable dependent on the Oculus headset's battery. The described set-up is displayed in Figure 31.

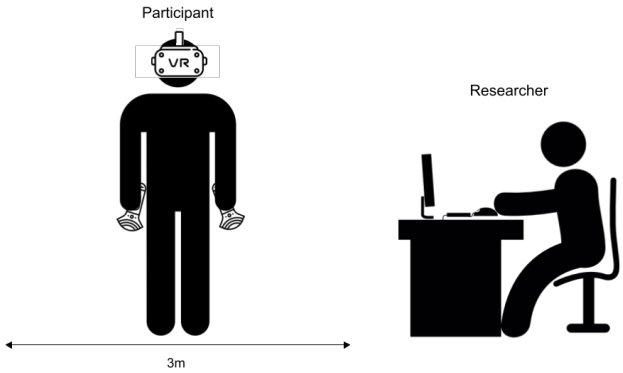


Figure 31: Experimental set-up

7.3 Procedure

Before the research, ethical approval is obtained from the EEMCS ethical committee under RP 2022-117. The procedure of the research starts when the participants are recruited, prior to their arrival the information letter and consent form are provided (see Appendix C). This enables them to read it all through calmly without feeling rushed or pressured. When they arrive, they are asked whether they have any questions and the consent form is signed. Firstly, the participant is asked to fill in a short anonymous demographics questionnaire which can be found in Appendix F. Subsequently, they are asked to fill in the questionnaire on cybersecurity displayed in Appendix D. This questionnaire contains 12 statements extracted from the HAIS-Q handling topics included in the program. An example of a statement is: “A mixture of letters and numbers is necessary for work passwords”. The research continues with a short explanation of the controls for the VRCyberEducation program as well as the mention of the possibility to stop at any point in time. “When you put on your headset you will be in a virtual environment. With the handheld controllers you can move around and interact. At the wall there is a screen that displays your tasks. With the buttons on your middle finger you can grab objects. Using the button at your index finger you can activate a laser, which you can use to grab objects from further away. Use the left joystick to walk around. Please make decisions like you would normally do and remember you can stop or take a break at any point in time by asking for assistance or taking off the headset.” After this explanation the participant performs the tasks presented in the virtual environment. Upon completion the participant leaves VR and is asked to fill in a questionnaire on cybersecurity and user friendliness which can be found in Appendix E. Subsequently, the participant is asked some of the qualitative questions displayed in Appendix G, the answers are noted by the researcher. This last task finishes off the research and starts the debriefing, the participant is thanked for their participation. It is made clear that it is a virtually simulated environment and none of the actions are real. Furthermore, it is

mentioned that any bad performance is an opportunity to improve, one should not be sad about it. Additionally, each participant is made aware about the UT's existing cybersecurity e-learning programs. Subsequently, it is mentioned that the researcher's contact details are provided on the previously given information letter, this way they can ask for more information if they would like to know more. Furthermore, it is mentioned that the final report can be found on the UT's bachelor thesis site, which is also included on the information letter.

7.4 Statistical design

The cybersecurity questions extracted from the HAIS-Q firstly need to be scored, where a high score is good performance. When the statement is negative, strongly disagree is assigned a score of 5 and strongly agree a 1. When the statement is positive, strongly disagree is assigned a 1 and strongly agree a score of 5. After the answers are scored, the differences between the before and after scores are calculated. Subsequently, normality is tested using the skewness and kurtosis values. The data has both a skewness and a kurtosis of -0.562, although this does indicate a slightly left skewed distribution the deviation is too small to reject a normal distribution. Secondly, normality is checked by using Shapiro Wilk's test, testing H0: sample has a normal distribution against H1: sample has non normal distribution. At a 5% significance level the data did not provide evidence to reject the assumption of a normal distribution, W(16)=0.936 p=0.318. Subsequently, the sample is checked for outliers using a boxplot. As can be seen in Figure 32, the data does not include any outliers. Since the differences X1… X16 can be assumed to be independent, normally distributed and not inclusive of any outliers, a paired samples test is applied. It tests H0: μ=0 against H1: μ>0 with α=5%. Furthermore, to check the degree to which the cybersecurity questions measure the single construct of cybersecurity Cronbach's alpha is applied. The data shows a Cronbach's alpha value of 0.712. Literature shows various ways and ranges of interpreting Cronbach's alpha, this is displayed in Figure 33. A value of 0.712 can therefore be classified as acceptable, satisfactory, sufficient, high, good, reasonable, adequate or relatively high.

The System Usability Scale (SUS) questionnaire, part of the last questionnaire, also needs to be scored before statistical analysis can take place. Strongly disagree is scored a 1, strongly agree is assigned a 5. For each odd statement, 1 will be subtracted from the user's response. For the even statements the following mathematical equation is applied: 6 - user's response. Subsequently, the converted score per user will be added and multiplied by 2.5, this creates a score between 0-100. From these individual SUS scores the mean will be calculated and interpreted using the two highly popular methods of conversion to percentile rankings [56] and assignment of grading scores [57].

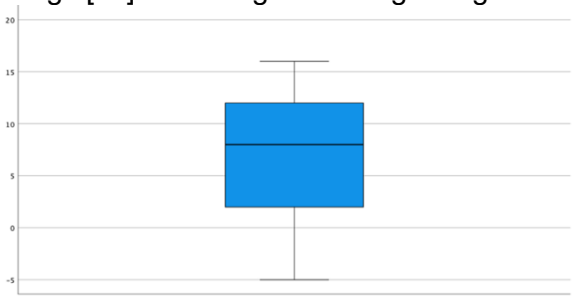


Figure 33: Boxplot of cybersecurity score differences

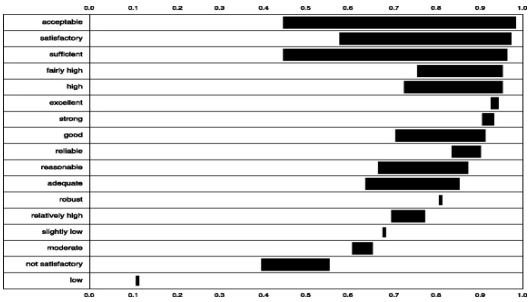


Figure 32: Interpretation of Cronbach's alpha [55]

8. Results

The VRCyberEducation program aims to address the role of human error in cybersecurity, decreasing the mistakes made by humans through an educational VR program. In the evaluations participants performed the tasks in the program as described in the previous section. All participants chose to change their password, however various passwords were chosen. Furthermore, none of the participants chose one of the re-used passwords. Regarding multifactor authentication three participants chose to enable multifactor authentication just after they said that they consider it to be very annoying. During the second task, three of the participants plugged the USB in the computer but did not think it had any effect since nothing happened.

As aforementioned the main goal of the evaluation was to research the effect of the program on one's cybersecurity knowledge. Since the cybersecurity score differences can be assumed to be independent, normally distributed and not inclusive of any outliers, a paired samples test is applied. It tests H0: $\mu=0$ against H1: $\mu>0$ with $\alpha=5\%$. The data shows at a 5% significance level that the cybersecurity score on average is increased after being exposed to the VRCyberEducation program, $T(15)=4.7$, $p<0.001$.

Secondly, the SUS scores are calculated and converted to 0-100 range as described Section 7.4. The data has a mean SUS score of 72.5 with a standard deviation of 8.37. When interpreted using percentile rankings, a SUS score of 68 is considered average, this is related to a 50% percentile ranking (see Figure 34). The mean SUS score of 72.5 surpasses this average and can be interpreted as a percentile ranking of 65%. When applying the assignment of grades, as displayed in Figure 34, the mean score can be classified as a high C or low B.

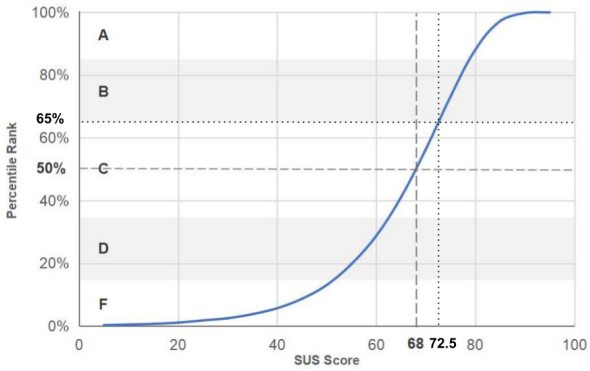


Figure 34: Rankings SUS score [58]

In addition to the quantitative data, the qualitative questions, asked at the end of the research, generated results on how participants perceived the environment. The character walking in was regularly described as convincing to be a regular colleague. Furthermore, although participants mentioned that he was resembling a real-life character they did not think of him as non-virtual. When delineating the process they just experienced, the method of movement was described as walking. Furthermore, participants used a first-person perspective in their description. For example, “After I had picked up the USB, I walked through the hallway to hand in the object at the IT department”. Additionally, participants were asked what they learned about removable media and how they obtained this knowledge. Answers described that they first handled the USB themselves and got feedback on their decision and the optimal way of handling it afterwards through the screen. This information was easy to put into context as they just experienced it, making either the cybersafe or cyber unsafe decision. Furthermore, it made them aware of their current behaviour. However, most participants did find the screen to be weirdly positioned which led to some noticing it very late. Furthermore, it can be made clearer that it completes the program.

9. Discussion

The significant positive results regarding the cybersecurity score show the intervention does improve cybersecurity performance. Therefore, both the second non-functional requirement of increased cybersecurity performance and SQ 6 are fulfilled. The quantitative results can be combined with the aggregated information from the qualitative questions. This displays participants experience the avatar as themselves, mainly due to using a first-person perspective in their description and specifying the movement as walking. This experience increases the chance of making decisions like one would normally do, which is key in getting correct results. Furthermore, when asked about the learning process, participants highlighted that the program made them aware of their current cybersecurity behaviour. In addition, the most cyber safe choice was easy to put into context as they just experienced it or already performed it correctly. This information indicates that VR is key in the program to obtain the aggregated significant results. VR enables the user to perform the task which enables the monitoring of current cybersecurity behaviour and the possibility to make them aware of this behaviour. Furthermore, VR is also the element that makes the feedback easy to understand since it allows the user to experience it. The result regarding the positive effect of VR complies with findings on the use of VR in the medical field. In surgical training it has shown to improve outcome, decrease injury and increase speed [59]. This finding is interesting for the educational field of cybersecurity. It provides a new method towards effective cybersecurity training handling the basic topics anyone should know, improving personal and organisational cybersecurity.

However, the cybersecurity scores also include some surprising data. Two samples of the aggregated data show a decreased cybersecurity score after exposure to the program. Potential causes are misinterpretation of the feedback or misreading of the questionnaire. The second cause seems most likely since the questions are both positively and negatively formulated and therefore require precise reading. When misreading one of the questions this can lead to a 4-point difference in scores which can have a big impact on the final score. Furthermore, some participants described the character walking in as both real-life and virtual, which is contradictory. This can be because the model used for this character is very resemblant of a real person. However, one can differentiate between the character and a real person, which may lead to one describing it as virtual and real-life simultaneously.

The SUS scores show an above average usability; therefore, the third non-functional requirement is fulfilled. It indicates a good usability which is crucial for large scale application. Especially since many new users will use the program for a relatively short period of time, high ease of use is important. However, the qualitative questions also generated information on ways to improve. The location and activation of the feedback screen can be improved to make it more noticeable and easier to understand the content. Furthermore, from the observation during the evaluation it became clear that the completion of the removable media should have a clear consequence that lets the user know they have completed the task. For example, a screen popping up on the computer when plugging in the USB.

The study also includes some clear limitations. Firstly, the created program remains a prototype, showing the possibilities and potential applications. Therefore, it does not include all important topics specified in Section 4. Another limitation is the inclusion criterion of years of service, due to recruitment complexities some of the participants are in service of an organisation for a little longer than 2 years.

This study proves the potential of the VRCyberEducation program, showing how it improves one's cybersecurity performance. To start addressing the role of human error in cybersecurity and make a real impact, the program will have to be implemented in organisations, similar to the way the current baseline program is implemented at the UT as described in Section 2.4.2. Therefore, one of the next steps should include completion of the program. Including all defined cybersecurity topics to transform the prototype into a complete education program. Secondly, this study researched the effect of the VRCyberEducation program on basic cybersecurity knowledge. Future work could build on these findings and research the potential of personalisation. Some fields require specific cybersecurity knowledge and skills which could be included in a similar program. Another way to include personalisation could be to make the current program adapt to user needs. For example, when someone performs well on the topic of removable media but needs more training on social engineering, the program should adapt the handled topics next time this user immerses in the program. Another interesting direction for future work is to research the potential of VR in other educational domains. For example, how VR can assist in remote learning.

10. Conclusion

As technology advances and digitization continues, cyber breaches increase and cybersecurity is gaining importance. 95% of all cyber incidents source from some form of human error, making this an area with substantial room for improvement. This project aimed to address this problem by creating a program to monitor, maintain and practise one's cybersecurity knowledge and skills. Background research highlighted the consensus on lack of human cybersecurity knowledge and awareness, accompanied by the general solution consisting of knowledge, education and training. Furthermore, it discussed the content and delivery method of an ISAT program. The ideation, specification and realisation described the process towards achieving the created program. The evaluation describes the way the data is collected and statistically analysed. The results display a significant increase in average cybersecurity performance after exposure to the program. This is accompanied by a mean SUS score of 72.5, conforming to a percentile ranking of 65%. These results show the possibilities and potential impact of the VRCyberEducation program. Creating a new method towards effective education of basic subjects in the increasingly important and growing field of cybersecurity. Future work should include completion and implementation to enable the VRCyberEducation program to have a real impact.

Appendix

Appendix A: Expert interview questions

- Which audience performs the worst in your cybersecurity testing and who performs the best? Do you have any idea why this is the case?
- How do you test employees on their cybersecurity knowledge? Has it proven to be effective?
- What are your current ways of educating employees on cybersecurity?
- What are the most often made mistakes in cybersecurity that you encounter?
- What are the mistakes made that are the most dangerous or cost the most money?
- What are the topics that in your opinion should most definitely be treated in a cyber/ information security awareness training?

Appendix B: Installing NeosVR on MacBook.

One starts with either a windows or Linux operating system (OS), on which Steam can be downloaded which is the foundation of neosVR. Steam can be used to launch and download neosVR. The first try consisted of installing a virtual machine called VirtualBox. On this VirtualBox windows was installed after which steam was downloaded. However, whenever NeosVR was started the program showed an error. The second try used the same virtual machine but used a different OS, Linux Ubuntu. NeosVR got further in the start up procedure but still showed an error before entering the program. Since, using a different virtual machine was even more complicated and using Linux did have some improvements as opposed to windows, a third try was performed with a different version of Linux. However, the same aforementioned error popped up. Therefore, it was chosen to continue with a very different, but also more complicated virtual machine, Bootcamp. The difference between bootcamp and VirtualBox is that VirtualBox opens a windows/Linux window within the IOS OS. Therefore, one can still use and access the programs and documents on one's computer. Bootcamp restarts the computer in the other OS and allocates all data on a separate disk partition. Therefore, one cannot access any of the information on the other OS. Furthermore, one should restart the computer in the other OS whenever the accompanying programs have to be opened. To download windows using bootcamp a >16GB USB is needed to temporarily store the windows install ISO. It will copy the windows ISO and install it on the allocated disk partition. On the first try, bootcamp froze when copying the windows files. After 48 hours, only very little progress was made. Therefore, it was chosen to quit and restart the installation, it continued by presenting an error regarding reading the USB. Erasing all content on the USB was not possible either, eventually this was achieved on another computer. The third try on installing windows through bootcamp succeeded, both Steam and NeosVR could be successfully downloaded.

Appendix C: Information letter and consent form

Information Letter

In this research I will evaluate my created VRCyberEducation program for my bachelor's thesis. You are free to participate in this research which starts by filling in a anonomous demographics questionnaire and continues with a questionnaire on your current cybersecurity knowledge. Subsequently you get an introduction to the program after which you immerse in the VR environment to test and educate your cybersecurity skills. You will be asked to perform various in-program tasks and make decisions just like you would normally do. After completion, you fill in a second questionnaire on your cybersecurity knowledge. Combined it will take a maximum of 30 minutes.

When immersing in VR using a VR headset there always is the possibility of motion sickness, similar to motion sickness in vehicles. Therefore, I advise you to not participate when you are prone to motion sickness in any other context. Furthermore, you are free to withdraw from this research at any point in time up to and including 48 hours after the research to remove your data from the study. When you want to withdraw during the immersion in VR you can always take off the headset or ask for assistance from the researcher.

Apart from the consent form no personal information will be collected, both the demographics and cybersecurity questionnaires will be filled in anonymously. The consent forms will be stored in a secluded google drive using a university-based account and deleted right after the project (08-07-2022). The participant has the right to request access to and rectification or erasure of personal data. The aggregated results will be published in the researcher's bachelor thesis, which can be found on essay.utwente.nl. If the results and study are worthwile, the aggregated results will be included in a research proposal and/or papers.

Researcher
Lara Klooster
l.klooster-1@student.utwente.nl

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) This committee consists of independent knowledgeable researchers from the university and is available for questions and complaints surrounding the research.

31-05-2022

Consent form

	Yes	No
I have read and understood the study information dated [31/05/2022], 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 withdraw from the study at any time, without having to give a reason.	☐	☐
I understand that taking part in the study involves fulling in two questionnaires and participating in a VR program on cybersecurity.	☐	☐
I understand that taking part in the study involves the following risks: the possibility of getting motion sickness. I understand that if this is the case I can take a break or withdraw at any time by taking of the VR headset.	☐	☐
I understand that information I provide will be used for the evaluation of the VRCyberEducation program and included in the researcher's bachelor thesis. I understand that if the results and study are worthwhile, the aggregated results will be included in a research proposal and/or papers.	☐	☐
I understand that personal information collected about me that can identify me, such as [e.g. my name], will not be shared beyond the study team.	☐	☐
Signed by name ----------		q

Appendix D: Participant questionnaire before VRCyberEducation program

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
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
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 password, even if a colleague asks for it.						
Strongly disagree	1	2	3	4	5	Strongly agree
It's safe to have a work password with just letters.						
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
I use a different password for my social media and work accounts.						
Strongly disagree	1	2	3	4	5	Strongly agree
I share my work passwords with colleagues.						
Strongly disagree	1	2	3	4	5	Strongly agree
I use a combination of letters, numbers and symbols in my work passwords.						
Strongly disagree	1	2	3	4	5	Strongly agree
I wouldn't plug a USB stick found in a public place into my work computer.						
Strongly disagree	1	2	3	4	5	Strongly agree

Appendix E: Participant questionnaire after VRCyberEducation program

The questionnaire includes the same as the before questionnaire but is extended with the following questions.

The virtual environment looks like a real-life situation.						
Strongly disagree	1	2	3	4	5	Strongly agree
I think that I would like to use this system frequently.						
Strongly disagree	1	2	3	4	5	Strongly agree
I found the system unnecessarily complex.						
Strongly disagree	1	2	3	4	5	Strongly agree
I thought the system was easy to use.						
Strongly disagree	1	2	3	4	5	Strongly agree
I think that I would need the support of a technical person to use this system.						
Strongly disagree	1	2	3	4	5	Strongly agree
I found the various function in this system were well integrated.						
Strongly disagree	1	2	3	4	5	Strongly agree
I thought there was too much inconsistency in this system.						
Strongly disagree	1	2	3	4	5	Strongly agree
I would imagine that most people would learn to use this system very quickly.						
Strongly disagree	1	2	3	4	5	Strongly agree
I found the system very cumbersome to use.						
Strongly disagree	1	2	3	4	5	Strongly agree
I felt very confident using the system.						
Strongly disagree	1	2	3	4	5	Strongly agree
I needed to learn a lot of things before I could get going with this system.						
Strongly disagree	1	2	3	4	5	Strongly agree

Appendix F: Demographics questionnaire

What gender do you identify as?

Male	Female	Non-binary	Prefer not to say	Other
☐	☐	☐	☐	----------

What is your age?

18-25	25-35	35-50	50-65	>65
☐	☐	☐	☐	☐

What is the highest level of education you have completed?

Primary school	High school	MBO	WO Bachelor	WO Master
☐	☐	☐	☐	☐

What is your area of expertise?

Architecture	Arts and entertainment	Business	Communications	Education
☐	☐	☐	☐	☐

Engineering and computer science	Environment	Government	Health and Medicine	International
☐	☐	☐	☐	☐

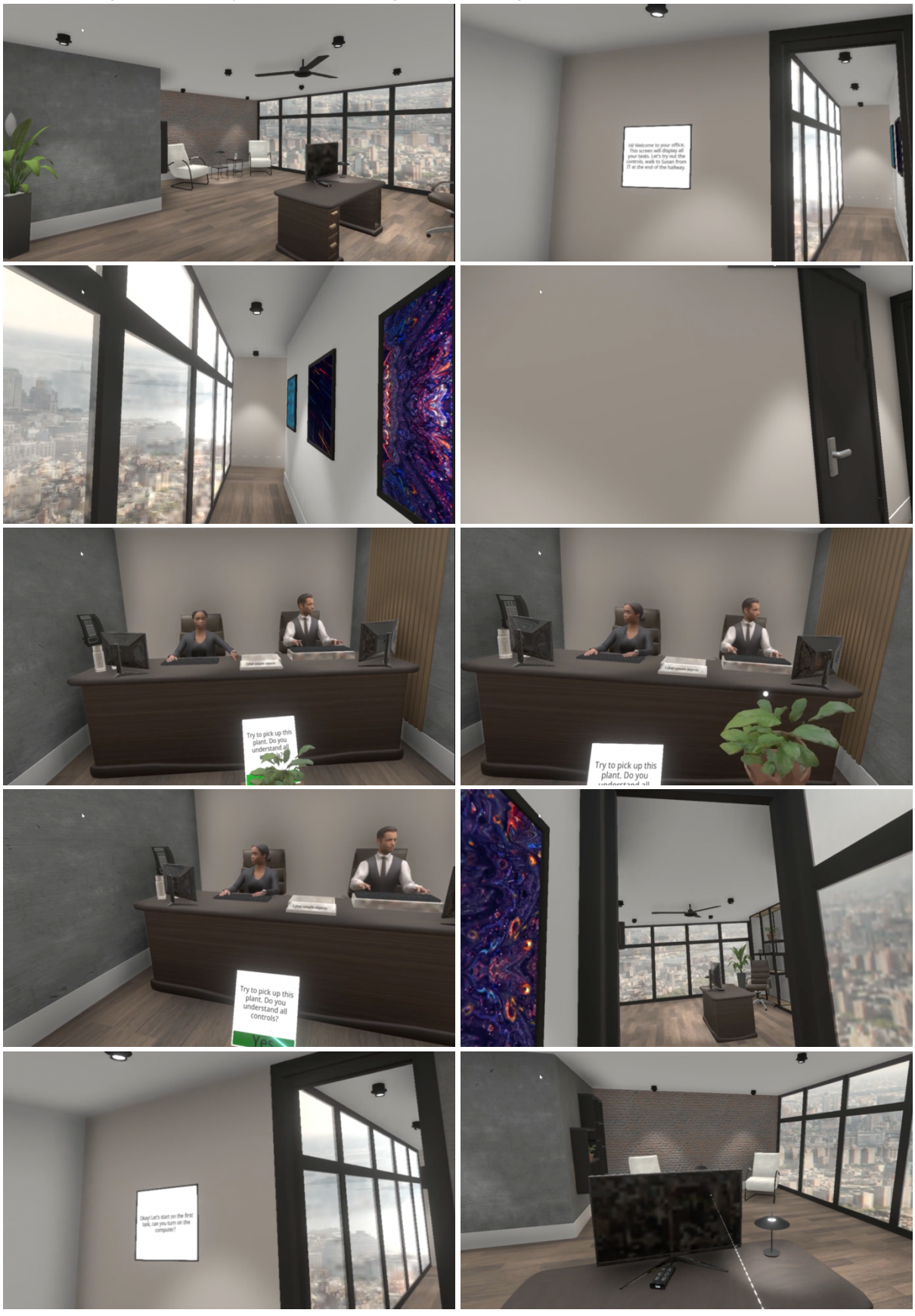
Law and public policy	Sciences	Social impact
☐	☐	☐

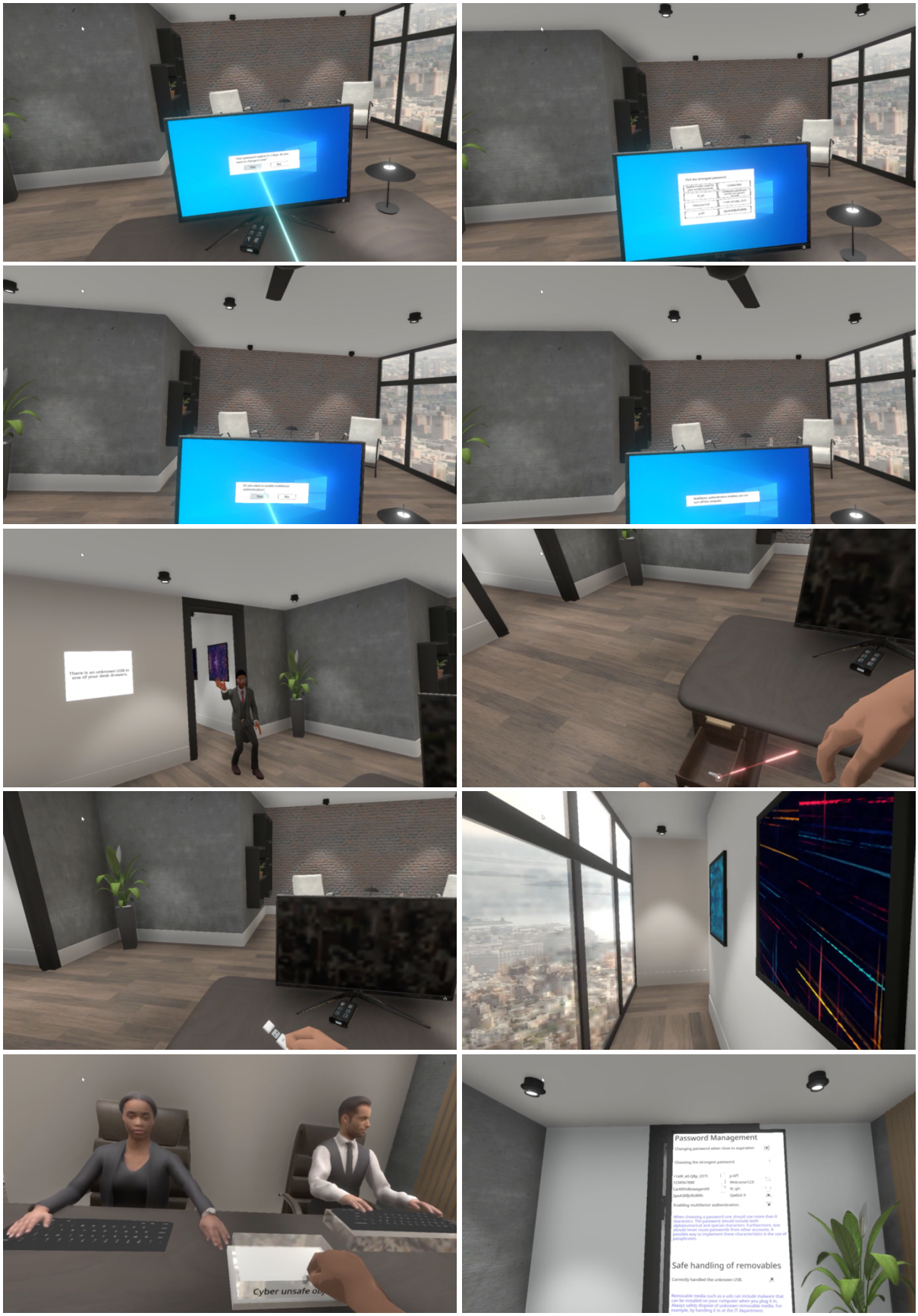
Appendix G: Qualitative questions evaluation

- What have you done in the VR program?
- What did you think of the person coming into the room?
    - Did you think of him as virtual?
    - Did you think of him as convincing?
    - Did you think of him as trustworthy?
- What have you learned about removable media?
    - How have you learned this?

Appendix H: First person perspective experience

These images show a typical walkthrough of the program from a first-person perspective.




There is an unknown USB in one of your desk drawers.
Password Management
Safe handling of removables

Appendix I: References 3D models

Door: https://sketchfab.com/3d-models/door-2738468b94d74c5f827e7e5df7be8359
Created by DJMaesen under CC Attribution license.
Modifications: different texture applied and change in door handle.

Usb hub: https://sketchfab.com/3d-models/usb-hub-ca45e5fa0fcc42a7a4894810fd456900
Created by YinRebuffReality under CC Attribution license.
No modifications.

Monitor: https://sketchfab.com/3d-models/monitor-0f3d348a29c14242bf79d0560f027af1
Created by valeriydeyneca under CC Attribution license.
No modifications.

Desk (Bank Teller): https://sketchfab.com/3d-models/desk-bank-teller-a5c7f6dfcea747c38f59ba7746d06209
Created by abdillaamy under CC Attribution license.
No modifications.

Collection of lamps ANI (BOSMA): https://www.turbosquid.com/3d-models/ani-bosma-lamp-3ds-free/886648
Created by bosma lighting under a 3D Model License limited to editorial use.
Not permitted in an open MMO virtual world-type.

dIX-Book Shelf(Manhattan Beach): https://sketchfab.com/3d-models/dlx-book-shelfmanhattan-beach-f8ce190335134b20b57bbe4bea07e3ec
Created by d-luX under CC Attribution license.
Modifications: vertically scaled the bookshelf.

Wardrobe: https://www.turbosquid.com/3d-models/free-obj-mode-modern-wardrobe/736200
Created by og1oc under a 3D Model License.

Lider Comfort Office Chair Black - 205315: https://sketchfab.com/3d-models/lider-comfort-office-chair-black-205315-10b0bcc04d174b14bde0ab9ac6f227da
Created by Zuo Modern under a Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0) license.

Flash Drive: https://www.turbosquid.com/3d-models/3d-model-flash-drive/715870
Created by marcis3D under a 3D Model License.

Modern chair 3 3D: https://www.turbosquid.com/3d-models/modern-chair-3d-1683202
Created by David Crupp under a 3D Model License.
Modifications: applied a different texture.

Mayfair 5505 Table Lamp by Vibia: https://www.turbosquid.com/3d-models/3d-mayfair-5505-table-lamp-model-1308641
Created by Designconnected under a 3D Model License limited to editorial use.

Liam Side Table by Minotti 3D: https://www.turbosquid.com/3d-models/liam-side-table-by-minotti-3d-1740932#
Created by Toss90 under a 3D Model License limited to editorial use.

Peace Lily 3D:
https://www.turbosquid.com/3d-models/peace-lily-3d-1770446#
Created by SPACESCAN under a 3D Model License.

Folders:
https://sketchfab.com/3d-models/folders-ca754d09e0ae42fdaf21b7c185f3a8cc
Created by valeriydeyneca under CC Attribution License.
No modifications.

Plants are nice:
https://sketchfab.com/3d-models/plants-are-nice-52704c1bafd44bfd9e98538276ad5614
Created by Manuagc under CC Attribution License.
Modifications: vertically scaled the model.

Water Carafe & Glass 3D:
https://www.turbosquid.com/3d-models/water-carafe-glass-3d-1504351#
Created by cgcentury under a 3D Model License.

Phone:
https://www.turbosquid.com/3d-models/free-phone-3d-model/444414
Created by TripRay company under a 3D Model License.

A compact keyboard(US-layout):
https://www.turbosquid.com/3d-models/us-layout-keyboards-obj-free/713305
Created by Nyanko556 under a 3D Model License.

Carla Rigged 001 3D:
https://www.turbosquid.com/3d-models/photorealistic-human-rig-3d-1422548
Created by Renderpeople under a 3D Model License.

Eric Rigged 001 3D:
https://www.turbosquid.com/3d-models/photorealistic-human-rig-3d-1422553
Created by Renderpeople under a 3D Model License.

References

[1] K. Khando, S. Gao, S. M. Islam, and A. Salman, “Enhancing employees information security awareness in private and public organisations: A systematic literature review,” *Computers & Security*, vol. 106, p. 102267, Jul. 2021, doi: 10.1016/j.cose.2021.102267.

[2] J. Hawdon, “Cybercrime: victimization, perpetration, and techniques,” *Am. J. Crim. Just.*, vol. 46, no. 6, pp. 837–842, Dec. 2021, doi: 10.1007/s12103-021-09652-7.

[3] “IBM Security Services 2014 Cyber Security Intelligence Index.”

[4] G. Desolda, L. S. Ferro, A. Marrella, T. Catarci, and M. F. Costabile, “Human factors in phishing attacks: A systematic literature review,” *ACM Comput. Surv.*, vol. 54, no. 8, pp. 1–35, Nov. 2022, doi: 10.1145/3469886.

[5] J. Abawajy, “User preference of cyber security awareness delivery methods,” *Behav. Inf. Technol.*, vol. 33, no. 3, pp. 237–248, Mar. 2014, doi: 10.1080/0144929X.2012.708787.

[6] K. F. Tschakert and S. Ngamsuriyaroj, “Effectiveness of and user preferences for security awareness training methodologies.,” *Heliyon*, vol. 5, no. 6, p. e02010, Jun. 2019, doi: 10.1016/j.heliyon.2019.e02010.

[7] “virtual-reality noun - Definition, pictures, pronunciation and usage notes | Oxford Advanced Learner’s Dictionary at OxfordLearnersDictionaries.com.” https://www.oxfordlearnersdictionaries.com/definition/english/virtual-reality (accessed Mar. 16, 2022).

[8] G. N. Samy, R. Ahmad, and Z. Ismail, “Security threats categories in healthcare information systems.,” *Health Informatics J.*, vol. 16, no. 3, pp. 201–209, Sep. 2010, doi: 10.1177/1460458210377468.

[9] D.-L. Huang, P.-L. P. Rau, and G. Salvendy, “Perception of information security,” *Behav. Inf. Technol.*, vol. 29, no. 3, pp. 221–232, May 2010, doi: 10.1080/01449290701679361.

[10] N. Badie and A. H. Lashkari, “A new Evaluation Criteria for Effective Security Awareness in Computer Risk Management based on AHP,” Jan. 2012.

[11] C. Nobles, “Botching human factors in cybersecurity in business organizations,” *HOLISTICA – Journal of Business and Public Administration*, vol. 9, no. 3, pp. 71–88, Dec. 2018, doi: 10.2478/hjbpa-2018-0024.

[12] A. Pollini *et al.*, “Leveraging human factors in cybersecurity: an integrated methodological approach.,” *Cogn. Technol. Work*, pp. 1–20, Jun. 2021, doi: 10.1007/s10111-021-00683-y.

[13] E. Metalidou, C. Marinagi, P. Trivellas, N. Eberhagen, G. Giannakopoulos, and C. Skourlas, “Human factor and information security in higher education,” *J of Systems and Info Tech*, vol. 16, no. 3, pp. 210–221, Aug. 2014, doi: 10.1108/JSIT-01-2014-0007.

[14] A. R. Gillam and W. T. Foster, “Factors affecting risky cybersecurity behaviors by U.S. workers: An exploratory study,” *Comput. Human Behav.*, vol. 108, p. 106319, Jul. 2020, doi: 10.1016/j.chb.2020.106319.

[15] V. Zimmermann and K. Renaud, “Moving from a ‘human-as-problem” to a ‘human-as-solution” cybersecurity mindset,” *Int. J. Hum. Comput. Stud.*, May 2019, doi: 10.1016/j.ijhcs.2019.05.005.

[16] K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac, and T. Zwaans, “The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation

studies," *Computers & Security*, vol. 66, pp. 40–51, May 2017, doi: 10.1016/j.cose.2017.01.004.
[17] *The IT regulatory and standards compliance handbook*. Elsevier, 2008.
[18] A. Tsohou, M. Karyda, S. Kokolakis, and E. Kiountouzis, "Managing the introduction of information security awareness programmes in organisations," *European Journal of Information Systems*, vol. 24, no. 1, pp. 38–58, Jan. 2015, doi: 10.1057/ejis.2013.27.
[19] F. Labib, "Qualities of Impactful Cyber Security Awareness Qualities of Impactful Cyber Security Awareness Training Training."
[20] M. Eminağaoğlu, E. Uçar, and Ş. Eren, "The positive outcomes of information security awareness training in companies – A case study," *Information Security Technical Report*, vol. 14, no. 4, pp. 223–229, Nov. 2009, doi: 10.1016/j.istr.2010.05.002.
[21] Introduction, "An Exploratory Study of Current Information Security Training and Awareness Practices in Organizations."
[22] "ISO - ISO/IEC 27002:2013 - Information technology — Security techniques — Code of practice for information security controls." https://www.iso.org/standard/54533.html (accessed Mar. 16, 2022).
[23] "Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards." https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss (accessed Mar. 16, 2022).
[24] E. Albrechtsen and J. Hovden, "Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study," *Computers & Security*, vol. 29, no. 4, pp. 432–445, Jun. 2010, doi: 10.1016/j.cose.2009.12.005.
[25] E. A. Irunokhai, A. M. Nuhu, and E. E. Daniel, "(PDF) Information Security Awareness, a Tool to Mitigate Information Security Risk: a Literature Review," Jun. 2021.
[26] J. S. Lim, A. Ahmad, S. Chang, and S. B. Maynard, "Embedding Information Security Culture Emerging Concerns and Challenges.," Jan. 2010.
[27] "12 Essential Security Awareness Training Topics for 2022." https://blog.usecure.io/12-security-awareness-topics-you-need-to-know-in-2020#removable (accessed Mar. 16, 2022).
[28] "Enterprise Cybersecurity Solutions, Services & Training | Proofpoint US." https://www.proofpoint.com/us (accessed Apr. 01, 2022).
[29] N. Chowdhury, S. Katsikas, and V. Gkioulos, "Modeling effective cybersecurity training frameworks: A delphi method-based study," *Computers & Security*, vol. 113, p. 102551, Feb. 2022, doi: 10.1016/j.cose.2021.102551.
[30] "'Qualities of Impactful Cyber Security Awareness Training' by Fadi Labib." https://pdxscholar.library.pdx.edu/honorstheses/682/ (accessed Mar. 16, 2022).
[31] J. Abawajy and T. Kim, "Performance analysis of cyber security awareness delivery methods," in *Security technology, disaster recovery and business continuity*, vol. 122, T. Kim, W. Fang, M. K. Khan, K. P. Arnett, H. Kang, and D. Ślęzak, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 142–148.
[32] "Fox - Attack and Defend Professional." https://cybersecurity.fox-it.com/attack-and-defend-fundamentals (accessed Mar. 16, 2022).
[33] "Alles om security awareness te creëren | Awaretrain." https://awaretrain.com/nl-nl/?utm_term=security%20awareness%20training%20for%20employees&utm_campaign=Awaretrain+NL&utm_source=adwords&utm_medium=ppc&hsa_acc=2695654975&hsa_cam=253307091&hsa_grp=99585170814&hsa_ad=434711003198&hsa_src=g

&hsa_tgt=kwd-296275846930&hsa_kw=security%20awareness%20training%20for%20employees&hsa_mt=e&hsa_net=adwords&hsa_ver=3&gclid=Cj0KCQiAjc2QBhDgARIsAMc3SqQ--fC_FSjSx7nOCMPAkB4mWfshLHHdezKMbgZr1o68d8g6ijhV6_gaAmw2EALw_wcB (accessed Mar. 16, 2022).

[34] "Living Security Teams: CyberEscape Online." https://www.livingsecurity.com/cyberescape-online (accessed Mar. 16, 2022).

[35] "Cyber Games | CISA." https://www.cisa.gov/cybergames (accessed Mar. 16, 2022).

[36] "Cybersecurity Training Videos - HSI." https://hsi.com/solutions/employee-training-and-development/cybersecurity-training-videos (accessed Mar. 16, 2022).

[37] "Cyber Security Awareness Training with Phishing Simulations - ATTACK Simulator." https://attacksimulator.com/ (accessed Mar. 16, 2022).

[38] K. H. Sharif and S. Y. Ameen, "A review of security awareness approaches with special emphasis on gamification," in *2020 International Conference on Advanced Science and Engineering (ICOASE)*, Dec. 2020, pp. 151–156, doi: 10.1109/ICOASE51841.2020.9436595.

[39] G. Jin, M. Tu, T.-H. Kim, J. Heffron, and J. White, "Game based Cybersecurity Training for High School Students," in *Proceedings of the 49th ACM Technical Symposium on Computer Science Education - SIGCSE '18*, New York, New York, USA, Feb. 2018, pp. 68–73, doi: 10.1145/3159450.3159591.

[40] R. C. Dodge, C. Carver, and A. J. Ferguson, "Phishing for user security awareness," *Computers & Security*, vol. 26, no. 1, pp. 73–80, Feb. 2007, doi: 10.1016/j.cose.2006.10.009.

[41] "Virtual reality - Oxford Reference." https://www.oxfordreference.com/view/10.1093/oi/authority.20110803120011837 (accessed Apr. 05, 2022).

[42] E. McGovern, G. Moreira, and C. Luna-Nevarez, "An application of virtual reality in education: Can this technology enhance the quality of students' learning experience?," *Journal of Education for Business*, vol. 95, no. 7, pp. 490–496, Oct. 2020, doi: 10.1080/08832323.2019.1703096.

[43] "View of Virtual Reality in Education from the Perspective of Teachers." https://amazoniainvestiga.info/index.php/amazonia/article/view/915/1047 (accessed Mar. 16, 2022).

[44] N. Elmqaddem, "Augmented reality and virtual reality in education. myth or reality?," *Int. J. Emerg. Technol. Learn.*, vol. 14, no. 03, p. 234, Feb. 2019, doi: 10.3991/ijet.v14i03.9289.

[45] W. S. Alhalabi, "Virtual reality systems enhance students' achievements in engineering education," *Behav. Inf. Technol.*, vol. 35, no. 11, pp. 919–925, Nov. 2016, doi: 10.1080/0144929X.2016.1212931.

[46] J. H. Seo, M. Bruner, A. Payne, N. Gober, D. "Rick" McMullen, and D. K. Chakravorty, "Using virtual reality to enforce principles of cybersecurity," *JOCSE*, vol. 10, no. 1, pp. 81–87, Jan. 2019, doi: 10.22369/issn.2153-4136/10/1/13.

[47] S. V. Veneruso, L. S. Ferro, A. Marrella, M. Mecella, and T. Catarci, "Cybervr: an interactive learning experience in virtual reality for cybersecurity related issues," in *Proceedings of the International Conference on Advanced Visual Interfaces*, New York, NY, USA, Sep. 2020, pp. 1–8, doi: 10.1145/3399715.3399860.

[48] P. Ulsamer, A. Schütz, T. Fertig, and L. Keller, "Immersive storytelling for information security awareness training in virtual reality," presented at the Hawaii International

Conference on System Sciences, 2021, doi: 10.24251/HICSS.2021.861.
[49] A. Kabil, T. Duval, N. Cuppens, G. Le Comte, Y. Halgand, and C. Ponchel, “3D cybercop: A collaborative platform for cybersecurity data analysis and training,” in *Cooperative design, visualization, and engineering: 15th international conference, CDVE 2018, hangzhou, china, october 21–24, 2018, proceedings*, vol. 11151, Y. Luo, Ed. Cham: Springer International Publishing, 2018, pp. 176–183.
[50] A. H. Mader and W. Eggink, “A Design Process for Creative Technology,” Sep. 2014.
[51] M. Tassoul, *Creative Facilitation*, 3rd ed. Vssd, 2009.
[52] “Tips for secure user authentication — ENISA.” https://www.enisa.europa.eu/news/enisa-news/tips-for-secure-user-authentication (accessed Apr. 25, 2022).
[53] E. Users, “Basic security practices regarding passwords and online identities.”
[54] J.-W. Bullee, L. Montoya, M. Junger, and P. Hartel, “Spear phishing in organisations explained,” *Info and Computer Security*, vol. 25, no. 5, pp. 593–613, Nov. 2017, doi: 10.1108/ICS-03-2017-0009.
[55] K. S. Taber, “The use of cronbach’s alpha when developing and reporting research instruments in science education,” *Res. Sci. Educ.*, vol. 48, no. 6, pp. 1–24, Jun. 2017, doi: 10.1007/s11165-016-9602-2.
[56] J. Sauro, *A Practical Guide to the System Usability Scale: Background, Benchmarks & Best Practices*. Denver: Measuring Usability LLC, 2011.
[57] A. Bangor, P. T. Kortum, and J. T. Miller, “Determining what individual SUS scores mean: adding an adjective rating scale,” *Journal of Usability Studies*, no. 4(3), pp. 114–123, 2009.
[58] “5 Ways to Interpret a SUS Score – MeasuringU.” https://measuringu.com/interpret-sus-score/ (accessed Jun. 29, 2022).
[59] J. D. Bric, D. C. Lumbard, M. J. Frelich, and J. C. Gould, “Current state of virtual reality simulation in robotic surgery training: a review.,” *Surg. Endosc.*, vol. 30, no. 6, pp. 2169–2178, Jun. 2016, doi: 10.1007/s00464-015-4517-y.