

Immersive Virtual Reality and Cybersecurity: Combatting Social Engineering in a Healthcare Context

by Sem Bakker

Supervisor: Dr. ir. R.W. van Delden, Critical observer: Dr. J.H. Bullee

Graduation Project for Creative Technology

University of Twente, Enschede

July 5, 2024

Abstract

This report details the process of the design and creation of a high fidelity prototype of an immersive virtual reality serious game which educates the player about two social engineering cybersecurity threats in a healthcare context. The first social engineering threat the game teaches about is email phishing. During the game the player learns how to recognise phishing emails based on five main signs. In addition, the game also teaches about a second social engineering threat through a surprise voice call. This voice call teaches the player about vishing, not lending out two-factor authentication, and reporting cybersecurity incidents. The design was based on background research, expert interviews, low fidelity prototype testing, and was validated in a hi-fi user study with students of health related studies. From this user study it was found that the designed intervention was successful in teaching the participants about three of the five main signs of phishing emails in the game, while the other two main phishing signs in the game could not be investigated, as those were already known by the participants before having played the game. In addition, it was found that participants scored better on the Human Aspects of Information Security Questionnaire (HAIS-Q) after having played the game. These findings give a potential indication that the designed prototype is successful at teaching the player about the two social engineering threats in the game. Finally, useful feedback was obtained from participants to make the scenarios in the game more relevant and believable regarding a healthcare context. In this way this project has contributed to the development of immersive VR cybersecurity games for a healthcare setting.

Acknowledgement

First of all, I want to thank my supervisor Robby van Delden and critical observer Jan-Willem Bullee for providing me with much useful feedback and insight during the many meetings we had during the months of this process.

I want to thank Sven Sonneveld for his collaboration on the expert interviews, recruiting participants during hi-fi prototyping and the ethics requests. In addition, I also want to thank him for giving me a heads up on the article about the deepfake meeting which was used in the introduction, for his feedback during our individual meetings, and also for the 3D models that he made which I could also use in my project.

I also want to thank the two anonymous cybersecurity experts who were kind to let me interview them and for sharing their knowledge with me.

Finally, I want to thank all the kind people who participated in the lo-fi and hi-fi testing of the game, your contribution means a lot.

Table of figures

1	Images of Lara Klooster’s GP [21]	16
2	Infosecure security awareness VR game [16]	17
3	An example of phishing in OneBonsai VR cybersecurity training trailer [25]	17
4	Creative matrix, the vertical axis consists of social engineering methods, whereas the horizontal axis consists of VR technology interactions.	22
5	Physicalised email phishing idea sketch	24
6	Removable media in-person persuasion idea sketch	24
7	CEO fraud idea sketch	24
8	Lo-fi instruction screen, text version	25
9	Lo-fi instruction screen, visual version	25
10	An overview of the lo-fi setup during the first session.	26
11	Low fidelity version of two factor authentication screen for 2FA vishing mini-game	27
12	New additions to the second session: a Bluetooth speaker for the 2FA vishing mini-game (top right) and a company contacts book (on the left)	27
13	Recruitment poster for lo-fi prototyping	28
14	Overview of the desk environment in the hi-fi prototype	35
15	Instructions displayed on the monitor in the hi-fi prototype	35
16	Demonstration of stamps on an email	37
17	ProtoFlux code of stamp number 1	37
18	ProtoFlux code which resets the emails in the game	38
19	Demographics of participant group	41
20	Background of participant group	42
21	A top down diagram of the experiment setup during the hi-fi prototyping sessions	43
22	Box-plot of HAIS-Q score differences / improvements	46
23	Overview of counted phishing signs in the open question ‘Please list all signs you can think of that would indicate an email is a phishing email’, before and after having played the game	47
24	Package email, first email asked in the questionnaire	49
25	Patient phishing email	50
26	Reimbursement legitimate email	50
27	Answers to how believable the 2FA voice call was considering a healthcare context	51
28	Answers to how relevant the 2FA voice call was regarding a healthcare context	51
29	Questionnaire answers to how believable the scenarios were in the game as a whole in a healthcare context	52
30	Questionnaire answers to how relevant the scenarios were in the game as a whole	52

Table of abbreviations and glossary

0.1 Table of abbreviations

The following are recurring abbreviations used in this thesis and their respective meanings:

GP - Graduation Project

SQ - Sub-question

VR - Virtual Reality

TG - Technische Geneeskunde, a health related study at the University of Twente which educates to become a technical doctor

BMT - Biomedische Technologie, a health related study at the University of Twente which educates to become a medical engineer

2FA - Two factor authentication

HAIIS-Q - Human Aspects of Information Security Questionnaire

0.2 Glossary of key concepts

The most important concepts for this graduation project will be explained in the glossary below. These key concepts will also be explained in the text, however the reader can use this glossary to become more familiar with terminology used in this graduation project, or to get a refresher.

Immersive Virtual Reality - Virtual reality in the broad sense refers to a digital or virtual world using 3D graphics, some video games and interactive experiences are an example of virtual reality. In this GP report, the focus will be on *immersive* virtual reality. Immersive virtual reality refers to the user being able to immerse themselves in this digital world using a VR headset or head-mounted display.

Social engineering - Social engineering is to a type of cyber-attack where the attacker tries to persuade the victim to do an action that is of the benefit to the attacker.

Phishing - Phishing is a type of social engineering attack where the goal of the attacker is to obtain sensitive data such as login information. A common type of phishing is through email, however other methods also exist.

Vishing - Vishing is a term for phishing done specifically through voice calls.

Contents

0.1	Table of abbreviations	4
0.2	Glossary of key concepts	4
1	Introduction	7
2	Background	9
2.1	Literature review cybersecurity threats	9
2.1.1	Types of threats in cybersecurity	10
2.1.2	Weaknesses in cybersecurity	11
2.1.3	Discouraged and recommended behaviour around cybersecurity	11
2.1.4	Discussion and conclusion	12
2.2	Non-academic sources on cybersecurity threats	13
2.3	Expert interviews	13
2.4	Shape and structure of the intervention	14
2.5	Academic related work	15
2.6	Commercial related work	16
2.7	Takeaways of background research	18
3	Design process	19
4	Ideation	20
4.1	Initial exploration	20
4.2	Initial concepts	21
4.3	Three main concepts	22
4.4	Paper low fidelity prototyping	25
4.5	Results of low fidelity prototyping	29
5	Specification	30
5.1	Requirements based on lo-fi prototyping	30
5.2	General requirements	31
5.3	Educational requirements	32
5.4	Ethical requirements	33
6	Realisation	34
6.1	Overview of designed hi-fi prototype	34
6.2	Functionality of stamps and emails	36
6.3	Processing emails	37
6.4	Resetting the world	38
6.5	Introduction screens	38
6.6	Aesthetics of the game	39
6.7	Trade-offs in the realisation process	39

7	Evaluation method	40
7.1	Participants	40
7.2	Experiment setup	43
7.3	Procedure	43
7.4	Design and analysis	44
8	Evaluation results	46
8.1	Results HAIS-Q score	46
8.2	Results phishing signs	46
8.3	Results questions about emails in the game	49
8.4	Results 2FA voice call	51
8.5	Results general questions	52
8.6	Results from observation of game-play footage	53
9	Discussion	55
9.1	Implications & limitations	55
9.2	Future work	56
10	Conclusion	58
A	Expert interview questions	62
B	Mock emails used in lo-fi paper prototyping	64
C	Lo-fi interview questions	67
D	Consent form and information letter user study	68
E	Walk-through screenshots of the game	70
F	Recruitment flyer	73
G	Researcher checklist during hi-fi prototyping	74
H	Pre-play-test questionnaire questions	75
I	Post-play-test questionnaire questions	78
J	Attribution of used assets final prototype	83
J.1	Sound effects	83
J.2	Voice fragments for 2FA request	83
J.3	3D models	83
J.4	Graphics on recruitment flyers	83

1 Introduction

Social engineering increasingly is a relevant threat. Social engineering refers to a type of cyber-attack where the attacker tries to persuade the victim to do an action that is of the benefit to the attacker. This can be in the form of providing login credentials, downloading malware or sharing sensitive data for example. As technology improves, so do the tactics used by cyber criminals. Just this year, 2024 at the time of writing, there was news of cyber criminals using deepfakes, using AI to replicate real persons in video, to fake an online meeting [5]. Through this method of social engineering the criminals were successful in convincing the targeted finance worker to transfer money to them.

The threat of social engineering is even more critical in a hospital context, where one wrong click can mean patient data being leaked to malicious actors. In fact, this was the case in 2019, where patient records with sensitive data of 68.000 patients were leaked as a result of two employees having clicked on a link in a phishing email [10], [29]. In addition, there have been multiple examples of patient data being held for ransom just alone this year of 2024, indicating how cyber-attackers want to get their hands on patient data for malicious purposes [4], [22]. These examples highlight the importance of people being educated about the different social engineering methods employed by cyber criminals.

As this importance of cybersecurity education is increasingly being recognised in our modern world, there are already quite a few different interventions with the goal of educating about cybersecurity. Newer technology such as immersive virtual reality (VR), which is the use of a head-mounted display to immerse the player in a virtual reality, shows potential for education. However, there are not many cybersecurity education interventions that make use of immersive virtual reality. Furthermore there are very few [16], [20], [25] immersive VR interventions that specialise in educating about social engineering.

This is where this graduation project (GP) comes in, by trying to answer the following main research question: *How can an immersive VR serious game be designed that successfully educates the user about how to recognise two social engineering cybersecurity threats in a healthcare setting?*

There were several steps to answer this question and create the final design. Starting off, background information was gathered to inform the design. This was done through a literature review, conducting expert interviews and searching the internet for related work. Once the solution was designed, it was validated through user testing. To validate the final design in the user testing, the following six sub-questions were formulated:

1. **SQ 1:** To what extent does the designed intervention influence the score on the Human Aspects of Information Security Questionnaire?
2. **SQ 2:** How well do the participants remember the intended learning goals of the designed game?

3. **SQ 3:** To what extent are the scenarios in the game deemed relevant for a healthcare setting?
4. **SQ 4:** To what extent are the scenarios in the game deemed believable for a healthcare setting?
5. **SQ 5:** How could the scenarios in the designed game be made more relevant to a healthcare setting?
6. **SQ 6:** How could the scenarios in the designed game be made more believable regarding a healthcare setting?

In the process of designing this immersive VR serious game there were some notable findings. First of all, it was found that participants remember three of the five phishing signs taught in the game, while the other two signs could not be investigated as those were already known by the participants. In addition, it was found that HAIS-Q scores of all participants improved after having played the game, and that there is a potential indication the scenarios in the game are relevant and believable regarding a healthcare context. Finally, there were great suggestions from healthcare students on how to create an immersive VR cybersecurity game specifically for a healthcare context.

The structure of the thesis is as follows: the thesis starts off with chapter 2, in which background information on the graduation project will be given through a literature review on cybersecurity threats, findings from expert interviews and an overview of already existing (VR) cybersecurity education solutions. Chapter 3 will go into the choice of design process. Chapter 4 will go into ideation, and paper prototype testing that was done. Chapter 5 continues by establishing specific requirements that the design of the final game needs to comply with, based on the findings in the background chapter. Chapter 6 will discuss the final design and the details on how it was realised. Chapter 7 and 8 are about conducting a user test on the designed VR serious game, and the results of this user test, respectively. Finally, Chapter 9 discusses implications, limitations and directions for future work and Chapter 10 presents the conclusion of the thesis.

2 Background

This background chapter serves as a basis for the ideation process and for choices made in the design process of this GP. The first part is a literature review on cybersecurity threats. After the literature review part, non-academic sources are discussed. The chapter then continues by analysing the findings of the expert interviews that were conducted to get insight into concrete cybersecurity situations in different organisations. Based on these interviews, a discussion will be done on whether the intervention should be a serious game or simulation. Next, academic and commercial related work relevant to this project is discussed. The background chapter is concluded with a section summarising the most important takeaways.

2.1 Literature review cybersecurity threats

In order to design the VR application, more needs to be known about cybersecurity threats¹. These cybersecurity threats can then be put in a creative matrix on one axis together with different VR technologies on the other axis. This allows ideation to be done in a structured manner by creating ideas for every combination of cybersecurity threat and VR technology. Towards that purpose, the goal of this literature review part will be to give an overview of cybersecurity threats that immersive virtual reality can help educate about. To answer this question, five sub-questions regarding cybersecurity threats were formulated:

1. *What are threats in cybersecurity in general according to literature?*
2. *What kind of social engineering methods are employed by offenders according to the literature?*
3. *What are common weaknesses in cybersecurity according to literature?*
4. *What is discouraged behaviour around cybersecurity and social engineering according to literature?*
5. *What is recommended behaviour around cybersecurity according to literature?*

The literature review consists of four main sections. The first part consists of paragraphs one and two, which respectively discuss sub-questions one and two. This is done by establishing current cybersecurity threats in general and then zooming in on social engineering threats. The second part has the goal of discovering weaknesses in cybersecurity, so that these can be improved with the VR intervention and is discussed in the third paragraph. The third part is about recommended and discouraged behaviour around cybersecurity and answers sub-question four and five, respectively. The fourth and final part consists of a critical discussion and conclusion which conclude the literature review.

¹Sections 2.1.x are based on my literature review assignment for Academic Writing [3]

2.1.1 Types of threats in cybersecurity

There are many different types of cybersecurity threats, however there might be a common factor in most of them. Multiple papers state that most cybersecurity threats involve some form of malware [2], [6], [19], [30]. Malware is a broad category of software that can be used to cause harm to the system running it or cause other malicious effects which is of some benefit for the attacker [19]. It makes sense that from the papers we can conclude that most cybersecurity threats involve malware, as the nature of cyberattacks is usually digital, and the software used is malicious. The different types of malware mentioned by [19] are: viruses, worms, trojans, rogware, spyware, and bot executables. However, [19] is from 2014, therefore it could exclude newer threats that have emerged in the last 10 years after the paper was published. In fact, a study from 2021 [24], mentions ransomware, which is a type of malware which has become more prominent in recent years. It is clear from this that as time goes on, more ways of conducting cyberattacks pop up. There are various ways attackers spread malware, among them are spam, social engineering (specifically the sub-type of phishing), and drive-by downloads [6], [19]. In addition, cybersecurity threats mentioned by [24], [30] are: DDoS attacks, Man in the Middle attacks, SQL injection, and password attacks. It is clear that there are many types of cybersecurity threats, but there is a logical pattern in the sense that most of them involve some form of malware. One of these aforementioned types of cybersecurity threats, social engineering will be explained and discussed in more detail in the next paragraph.

Zooming in on social engineering, there are different social engineering methods employed by offenders, however there is one specific category of social engineering that stands out as being dominant. Social engineering is defined by Aldawood and Skinner [1] as "manipulating and persuading people to disclose sensitive information or grant access to restricted areas or systems." [1, p. 63]. By far the most common social engineering threat seen in the papers seems to be that of phishing [1], [2], [6], [11], [19], [24], [30]. Phishing is a type of social engineering attack where the offender tries to steal a person's credentials or login info by pretending to be a trustworthy entity [1]. Phishing can be done through multiple methods, in the papers email, SMS, VoIP/telephone, phishing websites, and social media are mentioned as mediums used for phishing attacks [19]. This shows that phishing is common and can be done in multiple ways, what seems to unify these phishing methods is that they use the same underlying technique of exploiting the victim's trust. However, according to Gupta et al. [13], [14] not all phishing attacks are the same as they can be classified in two types: social engineering and malware attacks. The social engineering type is done through fake emails or websites, whereas the malware type does not involve the user handing over their data voluntarily [14]. Still, even in the case of a malware type phishing attack the victim is being persuaded to click on the link, therefore it could be argued that this type of attack is also a form of social engineering. Using phishing as a method to deploy malware is mentioned in multiple studies [2], [11], [13], [14], [19], [24]. From this it can be gathered that phishing is an important

method of spreading malware and therefore seems an important to educate about. The next section discusses what the weaknesses to cybersecurity threats are to answer sub-question three.

2.1.2 Weaknesses in cybersecurity

Weaknesses to cybersecurity threats can be grouped into two categories of technical weaknesses and social engineering weaknesses, although social engineering is the most important of these two. Technical weaknesses mostly lie in emerging technologies as attackers try look for flaws in them or abuse them for malicious goals [19]. As [19] is a bit older, we should apply this to our current day. A relevant emerging technology to keep in mind could be generative AI, as generative AI is a new and developing technology. In fact, Z-Cert, a cybersecurity foundation focusing on the Dutch healthcare sector, included generative AI in their threat overview of 2023 [31, pp. 33-35], where they mention generative AI will make cyber offenders' phishing emails more difficult to recognise. Besides this they mention that generative AI helps make video and audio fraud possible through deepfake technology. Weaknesses to social engineering attacks are a lack of information security awareness [1], [14], and being too trusting of strangers [1]. This makes sense as social engineering attacks actively exploit the naivety of the victim. An interesting point is that [1], [2], [11], [14] all express a sentiment in some form which states that technical defences can be nullified by a social engineering attack. From this we can conclude that social engineering weaknesses are more important than technical weaknesses.

2.1.3 Discouraged and recommended behaviour around cybersecurity

The discouraged behaviour around cybersecurity likely falls prey to the weaknesses and threats discussed in the previous paragraph. This could be things like filling in your login info in a phishing email, which could have been prevented if the victim had paid more attention to small cues that would have given away the in-authenticity of the message as mentioned in two papers [2], [13]. Two examples of discouraged behaviour are mentioned by [19], the first being downloading an unknown file from someone the victim befriended on social media, and the second example being clicking on an image file in a spam email [19]. Indeed, the findings in this paragraph are in line with falling prey to the weakness of lacking information security awareness and being too trusting of strangers found in the previous section.

On the other hand, the recommended behaviour around cybersecurity likely defends against the weaknesses mentioned in section two. That would mean that the recommended behaviour around cybersecurity tackles technical and/or human weaknesses. Regarding defending against social engineering weaknesses, Baillon et al. [2] found that providing information and simulating a phishing attack help to decrease the likelihood of employees giving their password away. Actively educating yourself and colleagues about cybersecurity is the most mentioned advice in the papers that provide suggestions on recommended cybersecurity behaviour [2], [6],

[13], [30]. This helps reinforce the need for educational methods such as the one in the GP. A suggestion regarding phishing is to set up an anti-spam filter or email classification based on various heuristics [13]. Some more recommended cybersecurity behaviour includes having strong passwords, using two factor authentication (2FA), keeping devices updated, securing the Wi-Fi network, staying away from public Wi-Fi, and securing social media profiles, according to [18], [30]. The takeaway from these recommendations seems to be that recommended behaviour protects the person or organisation from multiple types of attacks by implementing defences to reduce different weaknesses.

2.1.4 Discussion and conclusion

Before concluding this literature review part, there are two main points which are important to discuss. First of all, studies [14] and [13] have one author in common, therefore it makes sense if they express similar sentiments as a result of that. A second point of discussion is that it was difficult to find many sources that cover the same exact scope of cybersecurity threats. For instance, [24] focuses on cybersecurity threats in the healthcare sector. These points should be kept in mind when drawing conclusions from this literature review.

To conclude this literature review part, we will return to the main question by putting together the findings to the five sub-questions (SQs) that were the topic of research. Starting off, there are many cybersecurity threats (SQ1), and even though there are so many different threats, there is a common trend in that most threats involve some form of malware. By zooming in on social engineering threats (SQ2), it was found that most social engineering threats employ a form of phishing, through different types of media such email, SMS, telephone or others. Regarding weaknesses to cybersecurity threats (SQ3), it was found that weaknesses can be categorised in either technical or social engineering weaknesses, and that social engineering is the more important one of the two. Regarding discouraged behaviour (SQ4) it was found that most discouraged behaviour falls victim to weaknesses by not having enough knowledge or awareness of cybersecurity threats. On the other hand, recommendations on recommended behaviour (SQ5) are to educate yourself and others about cybersecurity threats such as phishing, and in addition setting strong passwords, thus negating social engineering and technical weaknesses.

Putting all of this together, these findings will help design the VR intervention for the GP as it is now known what threats and weaknesses there are and what the recommended and discouraged practices on the topic of cybersecurity are. The GP should focus specifically on the category of social engineering weaknesses, as it was established to be more important than technical weaknesses. Within the category of social engineering, the different types of phishing are interesting to explore further in the GP. This is because many studies mention phishing, thus deeming it a relevant threat, and because multiple papers mentioned that social engineering threats can nullify technical defences. The next steps in the GP would be to do ideation using

the creative matrix mentioned in the introduction to generate ideas for interventions that can teach about these social engineering threats.

2.2 Non-academic sources on cybersecurity threats

In addition to academic sources discussed in the literature review, there are also non-academic sources, such as the ENISA threat landscape [9]. ENISA is an organisation of the EU which tries to improve the state of cybersecurity in the EU. Regarding cybersecurity threats, the ENISA threat landscape 2023 mentions the most important threats to be: ransomware, malware, social engineering, threats against data, denial of service, internet threats, information manipulation and interference, supply chain attacks [9, pp. 6-7]. Zooming in on social engineering attacks, the ENISA report mentions phishing, spear-phishing, whaling, smishing, vishing, watering hole attack, baiting, pretexting, quid pro quo, honeytraps and scareware [9, p. 7] as the main types of social engineering. This lines up with what was found in the literature research, but also adds on to it through watering hole attacks, quid pro quo, honeytraps and scareware, which were not mentioned in the literature. ENISA also backs up that the emerging technology of AI is helping attackers in conducting social engineering attacks and that phishing still remains the most common form of social engineering [9, p. 4].

There are also commercial sources which report on cybersecurity threats, such as Verizon's 2023 data breach report [15]. The Verizon data breach report also backs up that social engineering and the human element is important, as they mention that: "74% of all breaches include the human element, with people being involved either via Error, Privilege Misuse, Use of stolen credentials or Social Engineering. " [15, p. 8]. In this case 'all breaches' meaning all breaches detected by them within the period 2022-2023 [15, p. 5]. In addition, they also mention that business email compromise has doubled [15, p. 8], this is a social engineering attack where the attacker already has access to the victim's email inbox, and then can use that information and redirect threads in the inbox to manipulate the victim [15, p. 32]. A critical note on this source is that it is from a commercial source, so the validity and integrity should be questioned, as Verizon can be considered to have a conflict of interest as they provide security services.

2.3 Expert interviews

In order to get more insight into concrete examples of cybersecurity at organisations, interviews with two cybersecurity experts at different organisations have been conducted. Interviews were done in a semi-structured manner, the list of questions asked to the experts can be found in Appendix A. Beforehand, an ethical application was filled in (application number 240143), and these interviews were approved by the Ethics Committee Computer & Information Sciences of the University of Twente. Before the interview the interviewee was orally briefed and given a copy of the infor-

mation letter and after everything was clear to them they were asked to fill in the consent form.

There were some interesting findings in these interviews. First of all, regarding what threats to focus on, one of the experts mentioned that there is no clear cyber threat that should be the main focus of an intervention. This is because cybersecurity is about having a broad defence against many types of potential threats.

Second, considering social engineering threats, both experts backed up that phishing is a common social engineering method, which is in line with the literature research that was done. They also both mentioned that phishing is prevented most of the time, but incidents can still happen sometimes. Spear-phishing is also not commonly seen, however it is difficult to detect when it happens as it is very personalised. In addition to phishing, one expert mentioned that CEO fraud and gift-card scams are also relevant social engineering threats. Gift-card scams were not found in the papers of the literature research, so this was an interesting find. Interesting to note is that CEO-fraud and gift-card scams also commonly make use of email as the medium to conduct these attacks.

Third, an interesting point that was brought up during the interviews was that cybersecurity awareness is something that people need to be constantly reminded of. It is not sufficient to only train people once, as the awareness declines after a couple of months.

Besides these three main points, there were also some other findings. One was that there is an ISO standard for cybersecurity, ISO27001 [17]. This standard could be used as a requirement, or source of inspiration for the design of the intervention. Besides this there was also an important takeaway that the intervention should be positive, forgiving, and encourage the person to report cyber threats. It should mention that becoming a victim to a cyber-attack can happen to anyone. These expert interview findings will help in the formulation of specific design requirements discussed in Chapter 5 about specification.

2.4 Shape and structure of the intervention

The proposed cybersecurity intervention can have different shapes, an important choice to make is whether to create a simulation or a serious game. *Should the intervention be a simulation or a serious game?* A simulation would try to recreate real life as closely as possible, while a serious game would be less realistic and more game like through while still teaching the user the same lessons.

The advantage of a serious game approach would be that it is expected to simplify reality a little bit, making it possible to emphasise the elements important to the learning intervention and giving more room for creative freedom. Serious game elements could also help in increasing the engagement and how memorable the intervention is.

A simulation approach on the other hand would have the benefit of translating more clearly and directly onto real life situations. However, creating a simulation also

requires more development time to be spent on details to make the simulation seem convincing.

To get some more perspective on the choice of simulation or serious game, experts were also asked about this in the expert interviews. One experts' opinion on this was that both are viable options, they did not have a preference on which would be best. Another expert preferred a serious game approach with the reason of it being more light-hearted and more memorable.

It seems best to me to use some hybrid form of a simulation and a serious game. What I mean with this is that the environment should still somewhat resemble a real office environment, as I hypothesise that this would help in the user recognising threats in real life. On the other hand, this office environment does not have to be a one to one recreation of a realistic office environment, only the most important elements need to be there. I think in this way it is possible to maximise the benefits that the intervention will have.

As briefly mentioned during the previous section, during the expert interviews, experts also gave insight into current cybersecurity interventions and the proposed structure of the intervention. They mentioned that current interventions are effective at first, and a clear increase in cyberthreat reports is observed. However, after a couple of months this security awareness diminishes. Therefore, the intervention should have a structure which promotes doing the intervention multiple times over a longer time span, in this way keeping the security awareness high.

2.5 Academic related work

There are some examples of cybersecurity training interventions related to what I am trying to achieve with this GP. The most closely related work to this project is Lara Klooster's Creative Technology graduation project [21]. They designed a VR simulation that teaches the user about three different cybersecurity weaknesses/threats: weak passwords, not having multi factor authentication, and plugging in unknown removable media (in this case a USB). The user could choose what to do for these three topics: choose a password, choose to enable multi factor authentication or not and plug in the unknown USB or not. They found that users on average perform better with cybersecurity after having completed the VR training [21]. Images of the VR program can be seen in Fig. 1 below.

What is different about this GP is that it specifically will focus on social engineering threats, whereas Klooster focused more on the technical weaknesses. In addition, this graduation project will focus on creating an intervention for a healthcare context specifically. An interesting idea I had regarding the example of unknown removable media in Klooster's program was that it could also be used as a lesson on social engineering. In Klooster's program the USB is left behind in a desk drawer by a character who says that they found it and thought it belonged to the user. It is not explicitly stated if that person is the cyber-attacker or just a co-worker with good intentions. So, it could have been a lesson on social engineering in its current form,



Figure 1: Images of Lara Klooster’s GP [21]

but the focus seemed to be more on the risk of getting malware. In contrast, my VR program in this example could focus more on the social engineering aspect through having a simulation of a person with malicious intent trying to actively persuade you to plug it in, and afterwards it is revealed that they were trying to social engineer you.

A second interesting related work is that of the cybertruck mentioned in an article on the University of Twente website [8]. The cybertruck is a mobile escape-room done in collaboration with University of Twente and Acute Zorg Euregio. The cybertruck teaches about cybersecurity through the process of stopping a fictitious hacker. In this case the target users which tried the cybertruck were healthcare workers. The methods used by the cybertruck also include an example of an unknown USB stick which was not supposed to be plugged in, just like Klooster [21] did. The other cyberthreats the cybertruck educates about are unknown as the paper of the study is not published yet. The news article mentions that initial results from the study show an improvement in cybersecurity awareness [8]. This project is also an intervention for cybersecurity in the healthcare sector, where my project will differ is that it will make use of an immersive virtual reality simulation/game, instead of an escape-room.

2.6 Commercial related work

Regarding commercial work, I found two main VR programs which mention that they train social engineering. The first of these is a security awareness game by Infosecure [16]. I was not able to find footage of this game, however from the images and description on the site it appears to be a serious game which is set in a futuristic setting. An image of the security awareness game can be seen in Fig. 2. The goal of the game is to stop a social engineer from controlling the servers. It is unclear what

social engineering threat is employed by the attacker, therefore what type of social engineering is trained for.

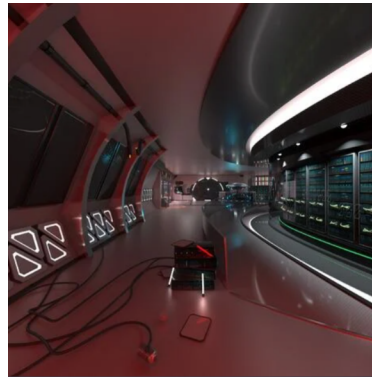


Figure 2: Infosecure security awareness VR game [16]

The second commercial VR program that teaches about social engineering that I found was a cybersecurity training by OneBonsai [25]. This intervention consists of an office environment in immersive VR, where the user can encounter various cyberthreats. The user also is equipped with a tablet, which is used to detect various cyberthreats and weaknesses. The tablet then mentions what is discouraged and what is recommended behaviour around that threat. Regarding social engineering, this program teaches about phishing emails / messages. An example of this can be seen in the video, where the user gets a message that pretends to be a logistics and shipping company, stating that they need the users login info to give them their package. This example from the video can also be seen in Fig. 3. The duration of the intervention is 15 minutes according to the website.



Figure 3: An example of phishing in OneBonsai VR cybersecurity training trailer [25]

2.7 Takeaways of background research

The following are the most important takeaways of this background chapter. Starting off, weaknesses in cybersecurity can mostly be split up into technical or human weaknesses. It was made clear by multiple papers that human weaknesses are quite important as they can bypass technical defences. Therefore, the focus of this project will be on improving human weaknesses through educating about social engineering attacks. In that regard, it was found that there are different social engineering attacks, where the most common seems to be various types of phishing. Phishing can be done through multiple methods such as email, SMS and telephone phishing. Through expert interviews, it was also discovered that gift card scams and CEO fraud are also social engineering threats. There were also some good examples of related work, two commercial VR interventions that tackle social engineering were found, however there does not seem to be any academic VR interventions specifically targeting social engineering. The best shape of the intervention seems to be a program that combines simulation and serious game elements. It seems best to design the intervention in a way that it can be replayed over a longer time period. This could be done through randomising the order of the tasks and mini-games in the intervention, so that every play-through is slightly different, this also prevents the person from just memorising when different threats pop up. In this way the intervention can help keep up the security awareness, preventing the cybersecurity awareness from decreasing.

With the background information that was gathered in this chapter, the design and ideation steps of the project can be done. The next chapter will discuss the design process that will be used to design the intervention.

3 Design process

The design process used in this GP is Mader & Eggink's design process for CreaTe [23]. The reason for choosing this design process is because it is the design process I am made familiar with in my study and it allows room for revisiting earlier design stages if needed. It suggests using an iterative approach with three clear logical stages: Ideation, Specification and Realisation. It is certain that as I go further in the design, I will need to refer back to the previous stages and change things with the new information and feedback that I get. The advantage of an iterative approach is that through each iteration the design will be more polished as a result of incorporating this new knowledge and feedback. For those reasons, this iterative approach is relevant.

Ideation will be done through tinkering with a VR headset and a VR platform which allows one to build VR experiences. Ideas will be gathered in a structured manner through a creative matrix. This creative matrix will consist of two axes, on the one axis will be VR elements found in the VR exploration, with the other axis being the cybersecurity threats found in the background chapter. Then once these axes are created, ideas will be generated for every combination of VR element and cybersecurity threat. In addition to this structured approach, ideation will also be done in an unstructured manner through following flashes of inspiration when they occur. These will be recorded in notes on a smartphone, and the source of inspiration will also be written down if the source is clear.

Specification will consist of creating a list of requirements based on the findings of the background research and expert interviews. The rationale behind all of these design requirements will be explained in the specification chapter. In addition through creating low fidelity prototypes, getting feedback on those prototypes, additional requirements will be formulated. This will be done by reformulating specifications or adding on to existing specifications.

Realisation is the creation of a final prototype based on the ideation and specification that was done. The realisation chapter will describe this iterative design process, in addition to the limitations of the final system. Besides that, the realisation chapter also includes all the technical details of how the system operates, as well as the choices that were made regarding aesthetics.

The next three chapters, Chapter 4, 5 and 6 will discuss ideation, specification and realisation respectively in more detail.

4 Ideation

4.1 Initial exploration

In order to do ideation for this GP project I started by doing an initial VR exploration to see first-hand what experiences have already been made in VR. To do this I borrowed a Meta Quest 2 VR headset from the University of Twente Interaction Lab. I then installed Resonite [28], which is a social VR platform, that allows for collaborative real time editing of worlds. Resonite was chosen as it allows for easy joining of different worlds, which could be used to get additional feedback from other Resonite users. In addition, Resonite also has its own visual programming language which makes it easy to create interactions. The Meta Quest 2 was connected through a link cable to a laptop running Resonite.

This VR exploration consisted of two phases: getting familiar with Resonite, and then joining different worlds. To get familiar with Resonite first I would follow the tutorial to see what the controls are and what features Resonite has to offer. After having done the tutorial, the exploration would be done through joining different worlds and keeping a logbook on what worlds I would join and what elements were interesting about them.

From the exploration, it seemed like Resonite was a viable platform to realise the GP. The Resonite tutorial was reasonably straightforward, and after having done it, I understood Resonite's main mechanics. I thought it was great how it is possible to edit many things about the world while simultaneously still being inside of Resonite. The world exploration ended up being done in two sessions of roughly 2 hours on two different days. Inside of Resonite's world explorer I discovered that there is a filter to only show educational worlds. As that seemed to be the most relevant type of world to this GP, I decided to use this filter to only show educational worlds. During the exploration I discovered multiple worlds that were educational or could be considered serious games and were interesting for this GP. In the end I joined 11 educational worlds. A particularly interesting world was 'Debug Warrior', which was a VR serious game that teaches the player about low level computer programming. An aspect of this game I liked was how they created a whole story around the goal of the game. In the game you need to modify an input of numbers by doing operations on a stack to get a specific output in order to destroy 'bugs' that are attacking your command centre. It also featured a tutorial non-player character (NPC), which was there to guide you through the experience, which was an element I appreciated. Another aspect of the experience that I appreciated was the option to speed up the operations done by your program, this was a nice quality of life feature for when I already understood how the main mechanics worked.

4.2 Initial concepts

After having done this initial VR Resonite exploration, I continued by creating a creative matrix in Miro, which is an online visual workspace tool. A creative matrix works by putting two factors on two axes and then creating ideas for different combinations of these factors. In this case two axes I used were: VR interaction elements on the one axis and social engineering threats on the other. In the creative matrix I thought of and wrote down some ideas on how different VR elements can be used to design educational exercises for each social engineering threat. Multiple of these ideas can be combined to create the VR intervention, as all these ideas are just parts that can be used together to teach about social engineering. This creative matrix can be found below in Fig. 4.

	VR Tech / interaction	holding items / item actions through context menu	NPC character	floating menus (sliders, buttons, text input)	Objects emitting audio	Moving / rearranging objects
SMSishing	hold a smartphone where you get different sms texts	Normal co-worker NPC letting you know you they SMS'ed you, leading you to also find other SMS's to review	Big hologram projection of SMS menu instead of on a small phone	SMS phone can emit notification sound	Rearranging SMS messages from least to most suspicious	
e-mail phishing	use a laser gun to destroy different e-mails that pop up in the sky	NPC saying they were trying to reach out to you through e-mail, prompting you to check your e-mails	sliders and buttons to navigate and read e-mails	e-mail notification sound from laptop	process physicalized e-mail envelopes by putting choosing to put them into the trash or not	
voicecall / telephone phishing	you get 3 different phonecalls and you pick up the phone and put it down when you think it's a social engineer	assistant NPC letting you know there is a call for you	big floating conference call / smartphone call screen	telephone/ VoIP meeting sounds	picking up putting away phone to interact	
social media phishing	Holding smartphone and having to choose which friends or messages to accept. Context is given on how you know them or not	Coworker NPC who notifies you of someone who has sent you a message on social media	inspect social media profile page. click on button to block user on social media	voice messages to listen to, notification audio	switch from smartphone to laptop social media	
website phishing	move a mouse object to navigate a browser	NPC prompting you to check out a website	user can find different urls and type them on the laptop on their desk or not.	website pop up sound	moving browser windows, max / min	
Removable media persuasion	Either grab the USB from the person or not	NPC who tries to get you to plug in USB / their smartphone /	floating arrow highlighting the removable media	Removable media that makes a sound, such as a smartphone	Connect unknown smartphone to charge it through cable to laptop or not	
Other in-person persuasion	Use item you got from the NPC w/ context menu or not	NPC asking to use your laptop / phone	social engineer trying to get you to click a button	NPC can talk	NPC holding out an item you can either take or not	

Figure 4: Creative matrix, the vertical axis consists of social engineering methods, whereas the horizontal axis consists of VR technology interactions.

4.3 Three main concepts

The idea for the final intervention is to tackle multiple social engineering threats, as it was made clear in the expert interviews that cybersecurity benefits from a broad

defence against different attack angles. Therefore, the goal for the intervention is to train against three different social engineering threats. Based on three ideas from the creative matrix, I worked out three interesting cybersecurity threat intervention tasks. The threats that these intervention sub-tasks educate about are: (email) phishing, in-person removable media persuasion and CEO fraud. Explanations of these ideas can be found below:

1. Desk setup with physicalised emails that the person can hold. The person needs to look through 10 emails and sort out the suspicious ones in the trash. On the screen are instructions with how to detect whether an email is phishing or legitimate. In addition, the screen can be used to open the links/URLs in the emails to get feedback on what could happen if they click the link. They could get a call shortly after they click a bad link from either an IT person or a manager to emphasise the potential consequences.
2. A non-player character (NPC) walks up to your desk and tries to persuade you to plug in their smartphone in your laptop under the excuse that its battery is almost empty. However, the smartphone will infect your laptop if you do this. This task aims to educate the user about in-person persuasion social engineering, with a specific focus on removable media. On the other hand, it would also be good to have some red herring NPCs, as it is not always clear in real life whether there is a real danger or if everything is actually okay.
3. CEO fraud task. Here there is a person trying to pretend to be a CEO or higher up in your company. The medium for this could be a social media app/website recreated in the intervention. There will be context provided on how to detect when CEO fraud happens. This could be done through another route from the other two tasks, such as through getting a phone call.

The idea is that all three of these tasks can all be done sitting at the virtual desk, as this removes the need to walk around, making the game more accessible to new players. In addition, it also reduces likelihood of motion sickness and streamlines the experience. After these three initial ideas were generated, I then created sketches of them, which can be seen below in Figs. 5 to 7.

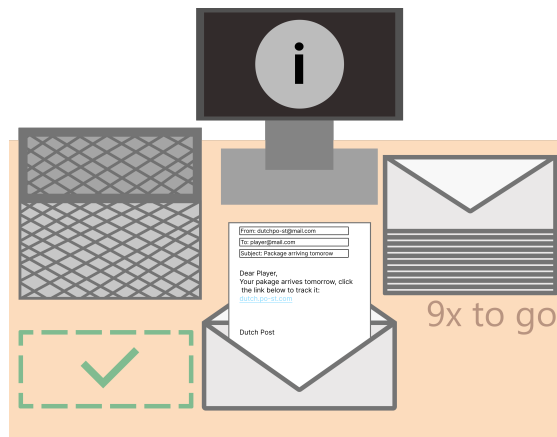


Figure 5: Physicalised email phishing idea sketch

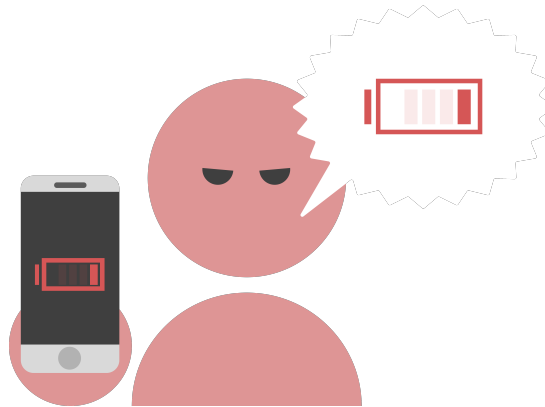


Figure 6: Removable media in-person persuasion idea sketch

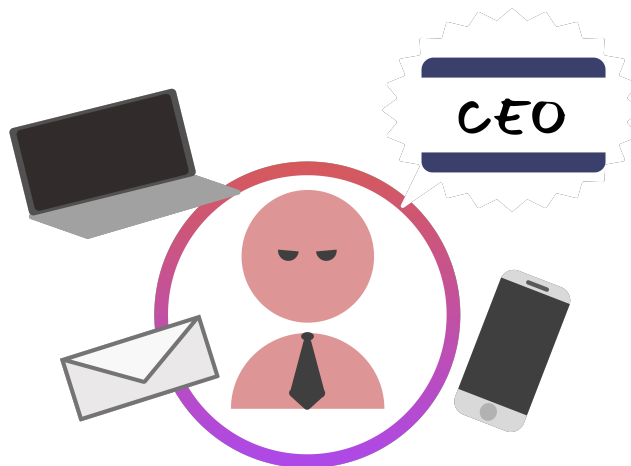


Figure 7: CEO fraud idea sketch

4.4 Paper low fidelity prototyping

To get initial feedback on these initial ideas that were generated in the ideation phase, paper prototyping was done. The goal of the paper prototyping sessions was to test multiple versions of the email phishing mini-game, test out the 2 factor authentication vishing interaction and find out what can be improved about the idea in general.

The email phishing game from the ideation chapter was worked out more for these prototyping sessions. First, the instructions screen was made. For the low fidelity testing, two versions of the instructions screen were made, the first version is more text-based while the second uses icons. Pictures of these two instruction screens can be found in Figs. 8 and 9 below.

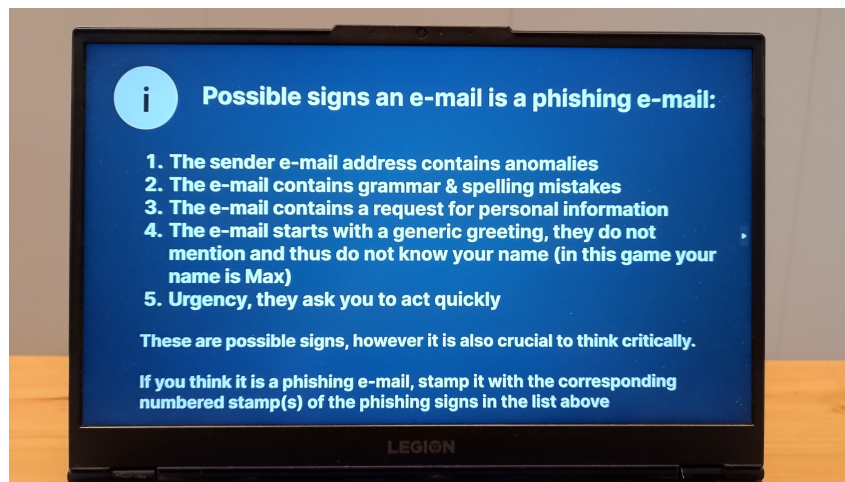


Figure 8: Lo-fi instruction screen, text version

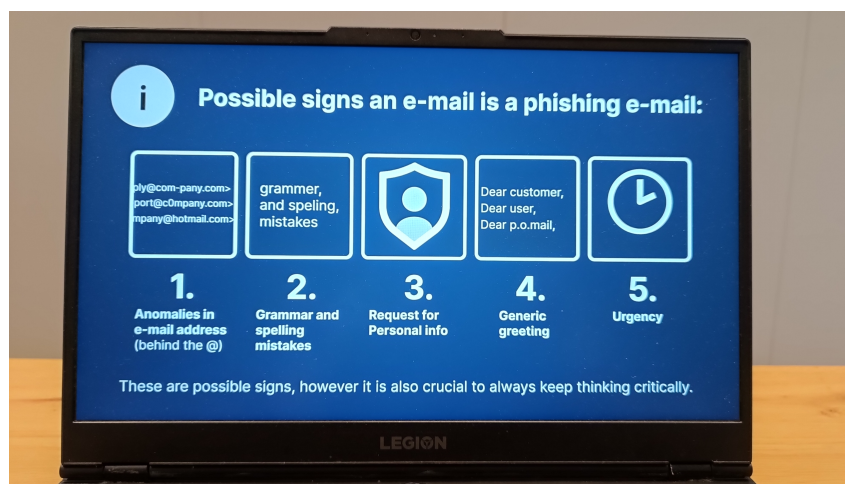


Figure 9: Lo-fi instruction screen, visual version

A new addition to the email phishing game was to have the player mark what signs they believe the email to be phishing based on five key signs that are on the instruction screen. The reasoning for this is that the player needs to be more aware of why they think a mail is a phishing email and is encouraged to look beyond the first sign of phishing that they see. Because otherwise, if the player is only asked to approve or deny the email they can just spot one sign that it is phishing and put it in the phishing bin, but that would mean they can ignore the other signs. Six mock emails were made in total for the paper prototype: four with different combinations of signs of phishing and two which are legitimate. The six mock emails used in the paper prototyping can be found in Appendix B. Once the participant placed the stamps on the email they could flip over the envelope to find out the correct solution, as a way to provide feedback. In the emails, it was chosen to give player character a name, as it serves as an indicator whether it is a generic greeting or if the sender of the email might know you. For this, the name Max was chosen as it is a gender neutral name, so that people of all genders can identify with it. An overview image of the setup of the first paper prototyping session can be seen in Fig. 10. On the left are the places to sort the emails, in the centre are six mock emails, on the top is a laptop which has an instructions with five signs of phishing, and on the right there are five stamps with the corresponding numbers of phishing signs used to mark the emails.

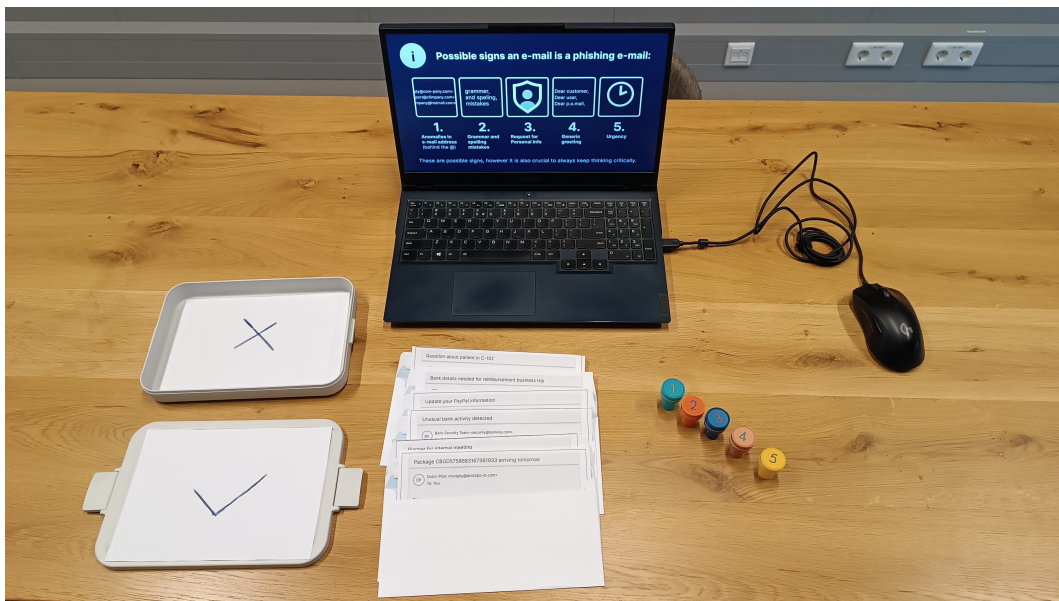


Figure 10: An overview of the lo-fi setup during the first session.

Besides the email phishing task, a low fidelity version of the two factor authentication (2FA) fraud task was also tested. This was based on the CEO fraud concept in the ideation phase, where the player gets called by a social engineer. The offender is pretending to be a higher up and trying to get you to approve a 2FA request for the patient database on the screen. However, as the goal of the offender is not to get the player to transfer money, it cannot be categorised as CEO fraud, instead it is more accurate to refer to this threat as 2FA vishing. The 2FA vishing threat was simulated through playing a text to speech voice on a Bluetooth speaker using Google Translate. The voice pretended to be a higher up who needs the player to approve a two factor authentication request 'to update the patient database'. After the participant was done with the email phishing task, this text to speech fragment started and a paper with the two factor authentication request was then put in front of the participant, which they could either accept or deny. The 2FA screen can be seen in Fig. 11. The additions to the second paper prototyping session can be seen in Fig. 12.

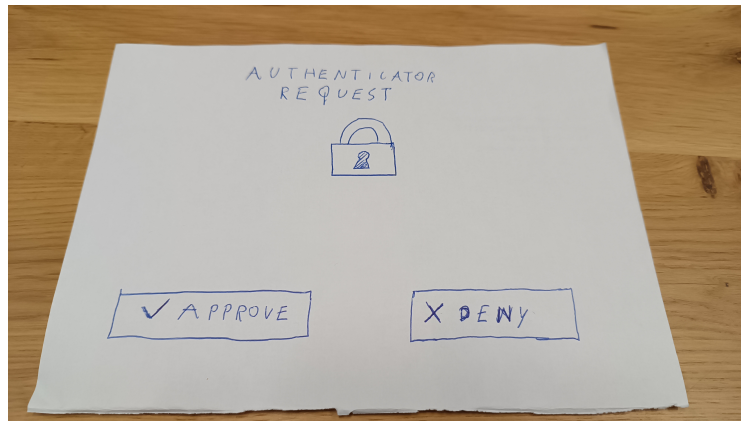


Figure 11: Low fidelity version of two factor authentication screen for 2FA vishing mini-game



Figure 12: New additions to the second session: a Bluetooth speaker for the 2FA vishing mini-game (top right) and a company contacts book (on the left)

Testing of the lo-fi prototype was done through recruiting students at the Technohal building of the University of Twente in two sessions on two different days. Before doing the lo-fi testing, ethical approval was requested from the Ethics Committee Computer & Information Sciences (application number 240361) and permission was granted. Recruitment was done by walking around and asking students, asking at the association room of the TG/BMT studies and through a poster on the door of the room that was booked, which can be seen in Fig. 13. A total of five participants were successfully recruited across the two sessions. At the start of the prototyping session, participants were briefed orally on the goal of the session. During the briefing it was made clear that the session was about the design of the prototype, not about how good the person is at recognising phishing emails. They were then asked to read the information letter and ask any questions if they had them. If everything was clear they could sign the consent form, after which the session would start. At the start of the session the participant was asked to do the phishing email task, which was followed up by the 2FA vishing task for the second session. During the tasks, notes were written down if there were interesting observations. After participants were done with these tasks, they were interviewed using a pre-defined list of questions, which can be found in Appendix C, and their answers were written down.



Figure 13: Recruitment poster for lo-fi prototyping

4.5 Results of low fidelity prototyping

There were multiple points of improvement found during these paper prototyping sessions. During the first day of play-testing with two participants, it was found out that one of the phishing signs was incorrectly added to the answers on the back of the envelope. One of the participants also mentioned that it is difficult to know whether you know someone is in your organisation or not, especially regarding the spear phishing email, as you are not the person in the game and do not have the context. The other participant, when asked about extra functionality wanted to be able to click on the sender in the emails to get more information. Based on this feedback, the organisation contacts book was added as a tool that the player can use to check whether a person is in their organisation for the second play-testing session.

During the second day of play-testing, three more participants tried the lo-fi prototype, with the 2FA vishing mini-game and an organisation contacts book as new additions, see Fig. 12. If the participant wanted to use the contacts book, I would say: "You look in the book and find out that X is (indeed in your organisation/not known within your organisation)". The new participants all intuitively tried to use the company contacts book whenever they did not know when someone was in their organisation or not, for the email phishing mini-game as well as the 2FA vishing voice message. One of the participants had dyslexia, which made the 'errors in spelling and grammar' phishing sign difficult to recognise for that person. As a result, the spelling and grammar phishing sign needed to be made more obvious. Considering things that were unclear, one participant mentioned that the check-mark and cross symbols could be confusing, as the check-mark could also mean 'yes, it is phishing'. Therefore, the phishing and normal emails should be labelled besides having the check-mark and cross symbols. When asked about extra functionality that they would like to be able to do, a point that was mentioned was that it would be nice if you could actually swing by Jolene Frogsworth's office, which is mentioned in one of the emails, see Appendix B. Another point of improvement mentioned was that the 2FA vishing voice seemed suspicious from the start as it made use of robotic sounding text-to-speech, therefore the final prototype should not use text to speech unless it sounds organic.

The main recurring point of feedback from both sessions seemed to be to provide context about things such as which people and companies Max (the player character) knows. Regarding the two versions of the instruction screen, there was a preference for the more visual version by all five participants. The main reason for the preference for the visual version was that it showed examples of what to look for in the emails. When asked about how realistic the interface and contents of the emails were, the designs of the emails and the contents of the emails were considered to reflect that of real emails by all participants. There were two emails which were designed to be more difficult to correctly categorise by using red-herrings, however more than half of the participants categorised them correctly. Considering usability, none of the participants mentioned that they were frustrated by interacting with the prototype.

5 Specification

This chapter distils the findings of the literature review, expert interviews, and paper prototyping into concrete requirements. The chapter then continues by formulating additional requirements based on ethical considerations.

5.1 Requirements based on lo-fi prototyping

To summarise the findings of the lo-fi prototyping, the following requirements were created:

- There should be a context screen at the start of the game, which explains the context and setting of the game.
- There should be a method of checking whether someone is actually in the player's organisation in the game, as context is key in judging whether an email or call is from someone the player 'knows'. This could be done through a company contacts book, which was added in the second lo-fi prototyping session.
- The phishing mini-game should use an instructions screen that uses visuals rather than text, as all five participants had a preference for the visual version of the screen.
- The phishing mini-game should mark whether the drop of place is for phishing or regular emails besides having the check-mark and cross symbols. This is because one of the participants mentioned the symbols could be interpreted the other way around otherwise.
- It should be possible to visit your co-worker, as it is mentioned in one of the emails. Or it should be removed from the email if it is not possible to visit the co-worker in the game.
- The spelling and grammar signs in the phishing email should be made clearer for someone with dyslexia.
- The 2FA vishing voice should sound organic, to not arouse suspicion from the start.

5.2 General requirements

Based on expert interviews and background research, the following requirements were formulated:

- The intervention should teach about multiple types of social engineering, with a target goal of teaching about three types of social engineering threats. This is because one of the experts mentioned that cybersecurity is about having a broad defence against many types of potential threats.
 - One of the threats should be (email) phishing, as both the literature review as well as the expert interviews made clear that this is the most common form of social engineering.
- Ideally the phishing emails should be randomised to allow for replay-ability and to require the user to pay attention instead of memorising order.
- The intervention should take into account the ISO standard for cybersecurity information protection, ISO27001 [17]. This standard was brought up by one of the experts in the expert interviews. It is out of scope for this report to describe all the requirements to comply with ISO27001 standard. In addition, the ISO27001 standard is made with organisations and their information security management systems in mind, however it can still be a good source of inspiration. For this project, the most important takeaway from the ISO27001 is that the program should try to minimise personally identifiable information that is collected, and if it is collected, it should be stored securely. In addition to trying to minimise any security risks or weaknesses in the program.
 - The game will also be run on a server which is only accessible for University of Twente students, researchers and employees, to further secure the data and defend against any potential security risks.
- The intervention should be positive and forgiving of making mistakes, and encourage the person to report cyber threats. It should mention that becoming a victim to a cyber-attack can happen to anyone. This was reinforced by one of the interviewed experts.
- Regarding a serious game versus a simulation approach, there should be some hybrid form, combining the engaging and light-hearted elements of a serious game while still resembling the real life situation somewhat. However, it will be more a serious game than a simulation.
- Regarding email phishing, a requirement is that no existing brands are used in the emails. This is to prevent brand identity playing a role in the classification of whether an email is phishing or not. This was a good point brought up in a meeting with my graduation project supervisors.

5.3 Educational requirements

The goals for the system are to educate the user about what the recommended and discouraged actions are around different social engineering techniques used by offenders. Specifically, the learning goals of the program are:

- Recognising different types of social engineering in a healthcare context:
 - How to recognise a phishing email from a normal email based on 5 potential signs:
 1. Anomalies in email address
 2. Grammar and spelling mistakes
 3. A request for personal information
 4. A generic greeting
 5. A request which is urgent
 - Learning about vishing through a voice message and a two factor authentication request, and learning about not letting someone else use your two factor authentication request.
 - Reporting an incident to the IT department if it happens.

In order to facilitate these learning goals, the following requirements were formulated:

- The first requirement is to have a debrief built into the serious game, letting the person know how they did, giving more information on social engineering and what they can learn from this experience. This helps to connect the takeaways from the serious game that they experienced to real life.
- The game should give feedback on how well the player is doing when they perform an action, such as when the player marks an email as phishing or not or sets a stamp. This facilitates the player to learn from the results.
- To recognise phishing in emails and transfer the knowledge to real life, it is important that the emails in the serious game should resemble that of the most popular email clients. This was already incorporated and tested in the lo-fi prototype.
- If an attack occurs the program should let the user report it to the IT department.

5.4 Ethical requirements

As part of a reflection on potential ethical issues raised by the graduation project, the following requirements were formulated:

- The VR experience should not cause harm, physically nor psychologically.
- The program could be misused by people with bad intentions. Therefore the intervention should try to avoid being an instruction on how to make social engineering more difficult to recognise.
- The design should avoid executives from using the program as a test to fire employees who perform poorly at detecting social engineering threats. Therefore elements which could be used to test, such as a score should not be included in the game.
- The program should clearly communicate its scope and its limitations. In other words it should be clear what it does and does not teach about. It should make clear that there are other types of social engineering than the ones in the program. This can be done through a disclaimer screen at the start of the game.
- The player should be informed that the program involves deception. However, as this is a necessary part of the game, it should be done in the debrief after the game.

6 Realisation

This chapter first gives an overview of the designed hi-fi prototype game, and then continues by explaining how the game works, how the game was created and how certain design choices were made.

6.1 Overview of designed hi-fi prototype

Realisation was done in the platform Resonite, using Resonite's programming language called ProtoFlux. The development of the Resonite world was mostly done using Resonite's PC mode, while sometimes checking what it looked like in VR. The game was ran on a special server which is only accessible for University of Twente students, researchers and employees, to defend against any potential security risks from outsiders.

The main goal of the program is to teach about recognising phishing emails through 5 main signs. To do this, the player needs to look at six different emails, and sort them into either the normal or phishing section. If they player thinks an email is a phishing email, they need to stamp the mail with stamps of the five respective signs which indicate the email is a phishing email. The six phishing emails in the final game were based on the six phishing emails used in the lo-fi prototyping session, but altered based on the feedback that was received.

An overview of the desk environment in the final game can be seen on the next page in Fig. 14. On the left of the desk a company contacts list, which can be grabbed. On the monitor in the middle of the desk are instructions with 5 signs which indicate an email could be a phishing email, which can be seen in more detail in Fig. 15. In front of the screen are two places to put the emails, where they are then processed. Finally, on the right of the desk are five stamps, which can be used to mark the emails with the 5 respective signs of phishing of the instructions screen on the monitor.

Besides the phishing email game, there is also a voice call phishing activity, which is triggered three minutes after the player has read through all introduction screens. This voice call is from someone pretending to work at the health organisation of the player, who is 'updating patient information in the patient database', and thus trying to get access to the patient database by getting the player to accept the 2FA request. The 2FA vishing call makes uses of an organic sounding voice generated using ElevenLabs [7]. In addition, a female voice saying 'incoming message' was also generated using ElevenLabs and added to prepare the player for listening to the voice call. After the message has stopped playing, the 2FA screen pops up, where the player has the choice of either accepting or denying the request.

There are three learning goals for this voice call. First, it teaches the player about vishing, which is phishing done through a voice call. Second, it teaches the player not to let others make use of their two factor authentication. Third, it teaches the player to report incidents if they happen.

A video play-through of the hi-fi prototype game was recorded and uploaded to YouTube, which can be accessed through the footnotes of this page². In addition, screenshots of a walk-through of the game are provided in Appendix E, with a note that not all six individual emails are featured in the screenshots.

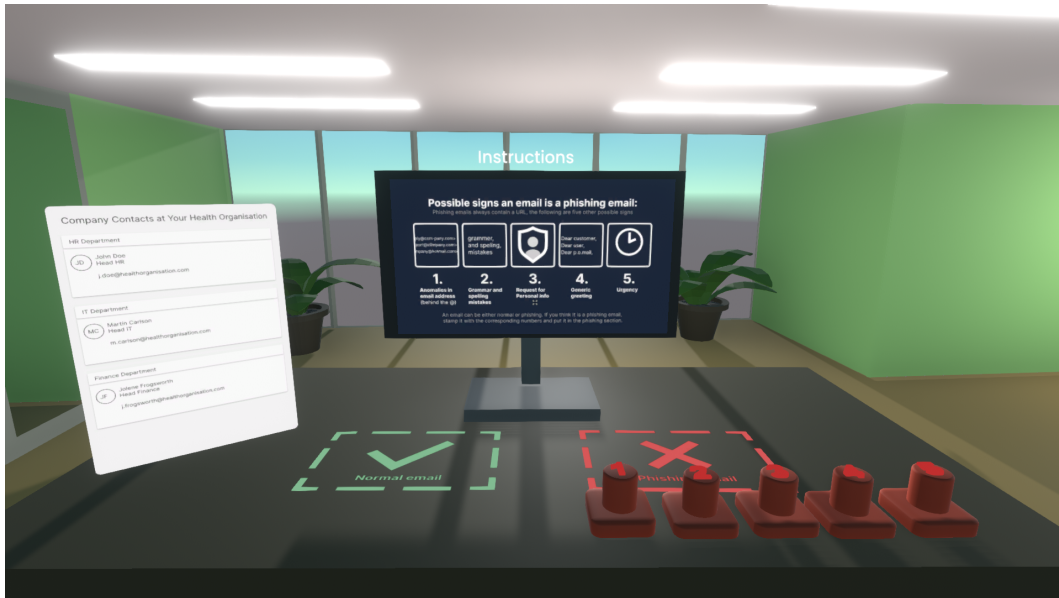


Figure 14: Overview of the desk environment in the hi-fi prototype



Figure 15: Instructions displayed on the monitor in the hi-fi prototype

²<https://youtu.be/ME5CDHQI0ow>

6.2 Functionality of stamps and emails

The main part of the system are the stamps and emails, which is also the most complicated part. Stamps and emails interact and communicate with each other through colliders and tags. The first working version of the email system checked whether an email is normal or phishing using collision detection and then by checking the tag of the email, which was either `isPhishing` or `isNotPhishing`.

Later this tag system was expanded to include the correct stamp solution and the submitted stamp solution on the email. A tag on an email looks like `isPhishing135-` for example. When a stamp collides with the email, it adds its own tag to the end of the email tag. The `-` sign is there to clearly separate the correct stamp numbers from the submitted stamp numbers and in order to apply string operations to the tag. For example, stamp number 3 colliding with the email would result in the tag `isPhishing135-3` on the email. In addition, when a stamp collides with an email, it also duplicates the 3D model of the number on its stamp cushion, to visually show that the email has been stamped by that number, which can be seen in Fig. 16. This number is parented to the email, so that the stamped number moves when the email moves. A stamp can only add its own tag and stamp once, which is achieved by checking whether the email already has a child with the same tag as the stamp attached to it.

When a stamp is added, the code checks whether it is correct by checking whether the tag of the stamp occurs more than once in the resulting string. The example of `isPhishing135-3` shows that 3 occurs more than once, which means the stamp number three is included in the correct answer. If the stamp is correct, it makes a ding sound and the resulting stamp keeps its red colour. If the stamp is incorrect, it makes a buzzer sound and the resulting stamps' material is set to a grey material. This material swapping is done using a `MaterialSet` component, where the material index number is either 0 or 1 depending on whether the stamp number is correct or not. A demonstration of the stamp system in use can be seen below in Fig. 16. In the example in Fig. 16, the email contains phishing signs 1 and 3, which indicate an anomaly in the email address and a request for personal information, respectively. Stamps 2, 4, and 5 were applied but are greyed out to indicate that they are wrong. The code that was described in this paragraph can be seen in Fig. 17.



Figure 16: Demonstration of stamps on an email

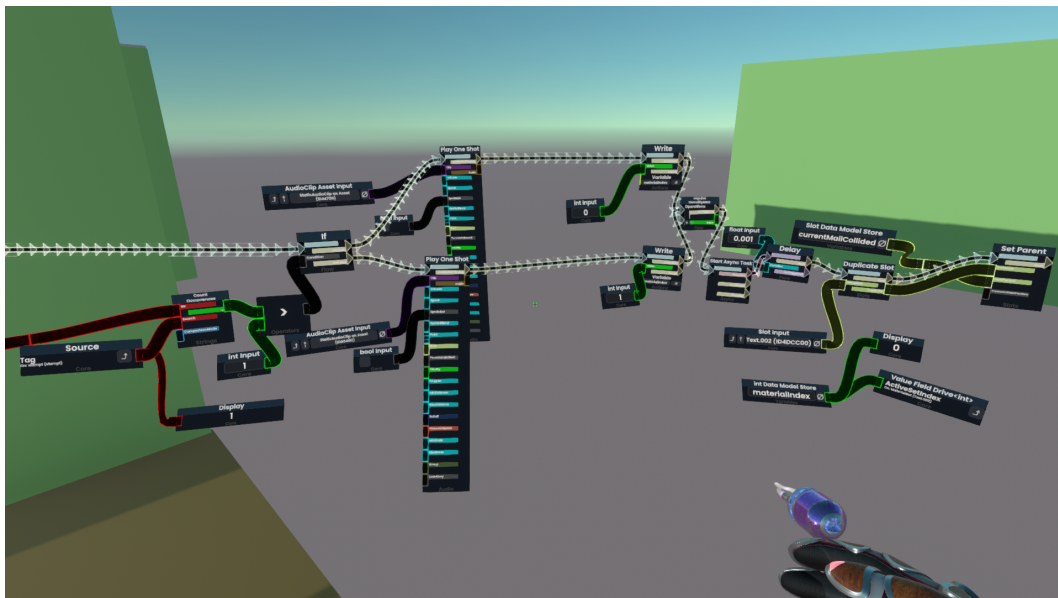


Figure 17: ProtoFlux code of stamp number 1

6.3 Processing emails

If an email is put in either the normal or phishing section, the system first checks whether it is correct. If the email is correct, it plays a ding sound and disables the email, making it disappear. If the email is put in the wrong section instead, it plays a buzzer sound and rejects the email. The reasoning behind this design is so that the player has a chance to look at the email again and learn from the feedback and then process it correctly, as the goal of the program is to teach, not to test the player.

6.4 Resetting the world

Another important component to the program is code that resets the whole scene so that the world is brand new for a new player. This was done by having an onStart event node trigger code that resets everything that needs to be reset when the world is started up. First this code makes sure the end screen is inactive, makes sure the introduction screens are active again, and the second part of the code resets all emails, which can be seen in Fig. 18. The resetting of the emails is done by going through all the emails within the 'ContainerForAllMails' using a for loop, and deleting all the children on the individual emails, which are the stamp numbers which were attached to the emails. Once the stamps are removed, the tag of the email should also be reset, in order to not have the tags that were added from previous stamp use. To do this, the code looks for the '-' character in every email's tag, and all characters behind the '-' character are removed from the tag. Finally, the emails are put back into their proper starting position, and all emails are set to inactive.

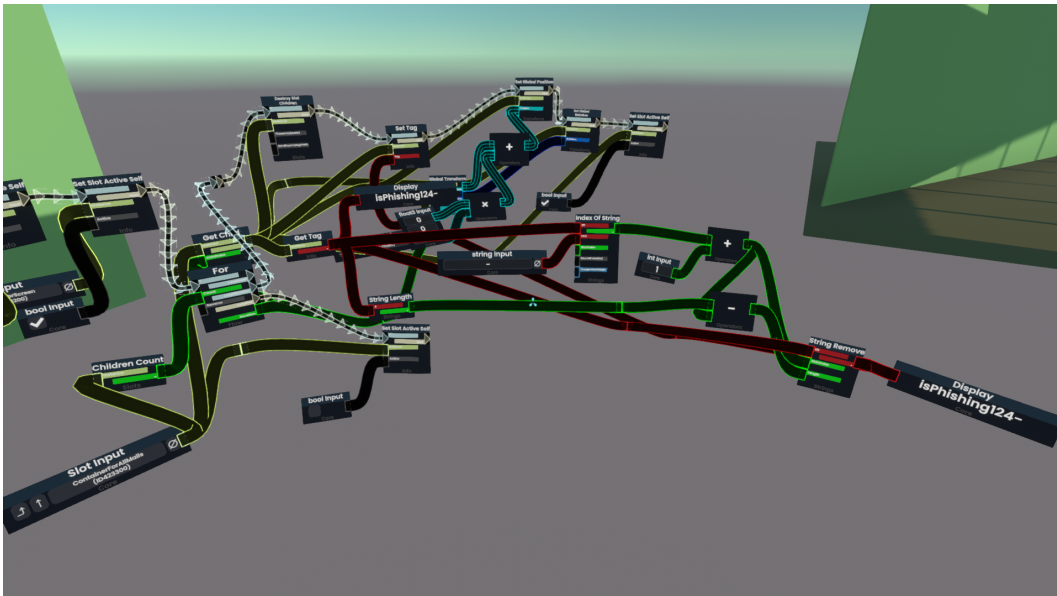


Figure 18: ProtoFlux code which resets the emails in the game

6.5 Introduction screens

At the start of the game, the player reads through the controls, disclaimer and context screens, which can be seen in the walk-through screenshots, see Appendix E. The emails and stamps are only set active once the player has finished clicking through the introduction screens, which was designed this way so that the player has to read the controls, disclaimer and context screens before being able to do anything in the game. In addition, this also resets and then starts a stopwatch node which functions as a three minute timer to activate the 2FA vishing call.

6.6 Aesthetics of the game

The art-style of the game is quite simple, which is intentional. Simple materials were chosen to make the game less realistic, as complete realism was not the goal. The idea is that the simple style makes the game feel more light-hearted, and does not distract the player. In addition, the simple style also has the benefit of making the game run as smoothly as possible and cutting development time spent on materials.

3D modelling was split up with another student doing a similar graduation project. For this I 3D modelled the office environment with all the floors, walls and windows. In addition, 3D models were created by me for the five stamps. The remaining models in the game were created by Sven Sonneveld, which are the monitor, table, and plants.

All 2D assets were made in Figma, this includes the emails, email sorting areas, the instructions screen with 5 main phishing signs, the disclaimer screen and the two 2FA result screens. The only exception being the controls and context screens, which were created using the UI canvas in Resonite.

6.7 Trade-offs in the realisation process

During the ideation phase I came up with the idea of creating an in-person physical media persuasion mini-game, where an attacker would walk up to your desk and try to get you to plug in a smartphone under the excuse that its battery was almost empty. The idea was good considering how it is a mini-game that would make good use of the characteristics of VR. However, it was deemed too ambitious to execute to a satisfactory degree within the scope of this graduation project as it would cost a lot of development time and resources to make and program a convincing humanoid NPC. Therefore, it was chosen to put the focus of the intervention on the phishing email and 2FA vishing tasks. Another aspect that was scrapped was where the player would be able to visit the office of a co-worker if they did not trust that the email was legitimate, due to similar reasons.

7 Evaluation method

To validate the final design, a final user study was done with two main goals. The first of these goals was to get an indication of whether the VR intervention helps in educating about social engineering cybersecurity threats. The second of these goals was to find out whether the serious game contains relevant and believable scenarios regarding a healthcare context. Before the hi-fi prototype evaluation sessions, an application was done in the ethical review portal (application number 240530) and ethical approval was granted through the ethical review committee of Computer & Information Sciences.

7.1 Participants

Participants were students recruited from health related studies at the University of Twente. The inclusion criteria was whether the participant was a student of one of the following studies: Technische Geneeskunde (TG), Biomedische Technologie (BMT) or Gezondheidswetenschappen. The names of these studies in English, respectively are: Technical Medicine, Biomedical Technology, and Health Sciences. In addition, there was an exclusion criteria for people who are known to have motion sickness, as VR is known to possibly trigger motion sickness. Recruitment was done through asking people in-person, asking acquaintances, and by sending a message with information and a date planner in the group chat with students of the studies BMT and TG. Additionally, flyers were created together with a fellow student doing the same graduation project assignment, and were spread around the Technohal building, which is the main building where most health related students are. Flyers were also spread at the association rooms of the studies BMT and TG and of Health Sciences. The design of the flyers can be seen in Appendix F. In total around 100 flyers were handed out or spread around the building. Through all these methods combined, a total of five participants were recruited. Participants were not compensated for participating, except for snacks set up in bowls at the end of the session.

Regarding the questionnaire demographics, it was chosen to ask for the participant's age range instead of their specific age, to maximise the participants' anonymity, as the data collected could be considered sensitive.

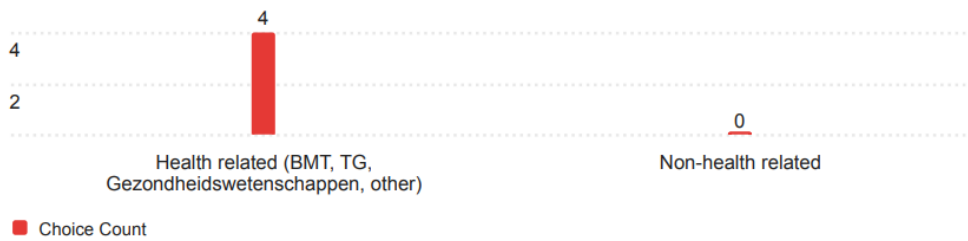
Although five participants participated in total ($N=5$), one of the participants did not consent to having the answers they provided in the questionnaire to be archived in the University of Twente thesis repository, therefore the answers to the questionnaire of this participant will be excluded from analysis in this report, however findings from their game-play, and notes taken during the session can still be discussed.

The characteristics of the remaining participant group can be seen in Figs. 19 and 20. The participant group of the questionnaire consisted of four female students, all aged 18-24, and all studying a health related study.

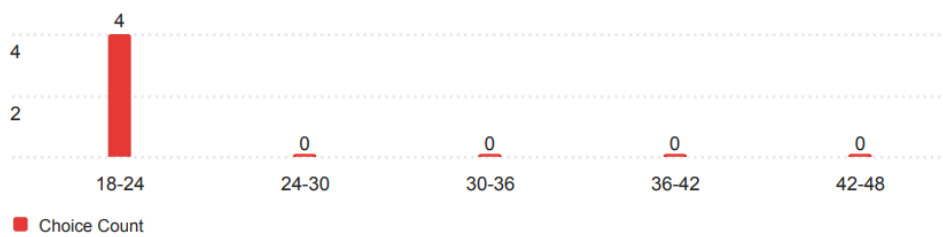
In addition, considering the participants' background experience, all four participants in the questionnaire had tried VR 1-3 times before doing the study. The familiarity of the participants with social engineering and phishing emails differed

between participants: all four participants had different answers to the 'I am familiar with the concept of social engineering' question. Interesting to note here is that all four participants answered either 'somewhat agree' or 'strongly agree' to the statement 'I am familiar with phishing emails'. This is interesting, as phishing emails are a form of social engineering. This difference could be because of multiple reasons. One reason for this difference could be that they are familiar with email phishing, but they are not familiar with what other types of social engineering there are. Another reason could be that participants were familiar with the concept of social engineering, but that they have not heard the specific term for it. However, participants not being familiar with the term social engineering should be negated by the short description of social engineering that was provided before this question was asked in the questionnaire. All participants were at least somewhat familiar with phishing emails before the study.

What type of study are you studying?



Q17 - What is your age range?



What is your gender?

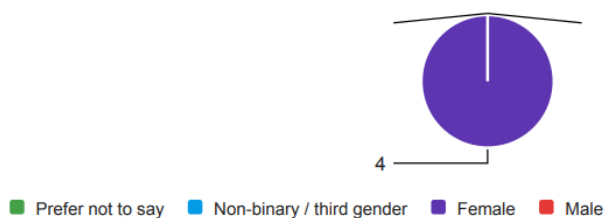
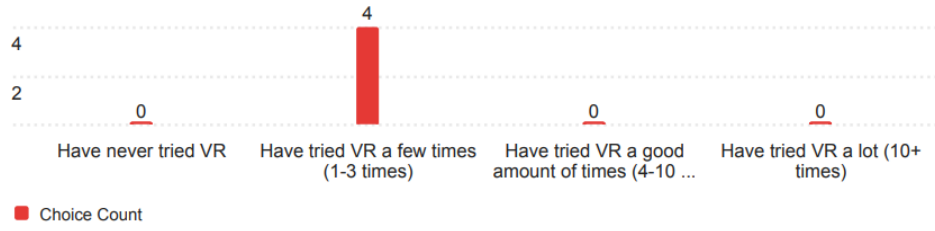
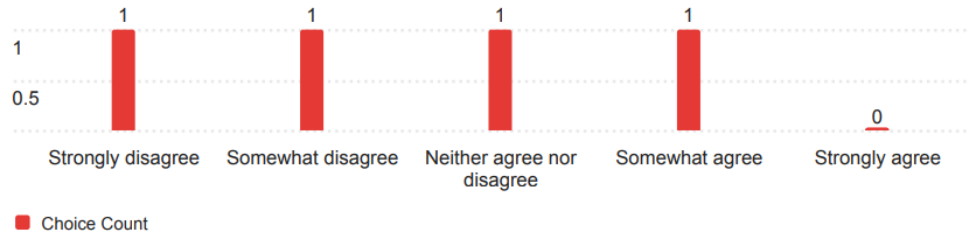


Figure 19: Demographics of participant group

How familiar are you with VR?



I am familiar with the concept of social engineering



I am familiar with phishing emails

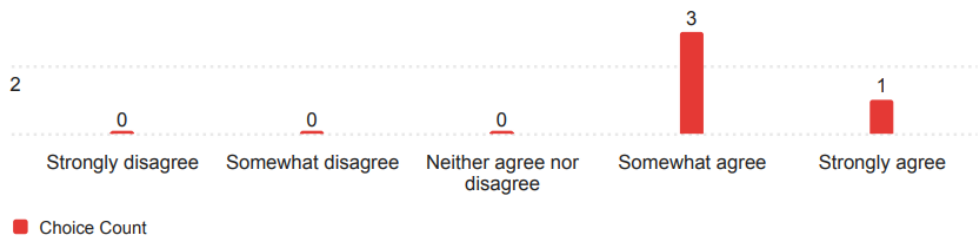


Figure 20: Background of participant group

7.2 Experiment setup

The game was ran on a Lenovo Legion 5 laptop with a RTX 3060 GPU running Resonite on Windows 10. A Meta Quest 2 Business headset was connected to the researcher's laptop using a USB-C link cable. For the experiment, a room was booked for six days in the University of Twente's Interaction Lab to conduct the hi-fi prototype play-testing. This room had the dimensions of roughly 2 by 4 meters, with the playable area in VR being of roughly 2 by 2,70 meters. A top down diagram of the room and the playable space can be seen below in Fig. 21. The beginning and end sections of the session were done at the desk, with P in the diagram indicating the place where the participant sat, and R indicating the place behind the desk where the researcher sat.

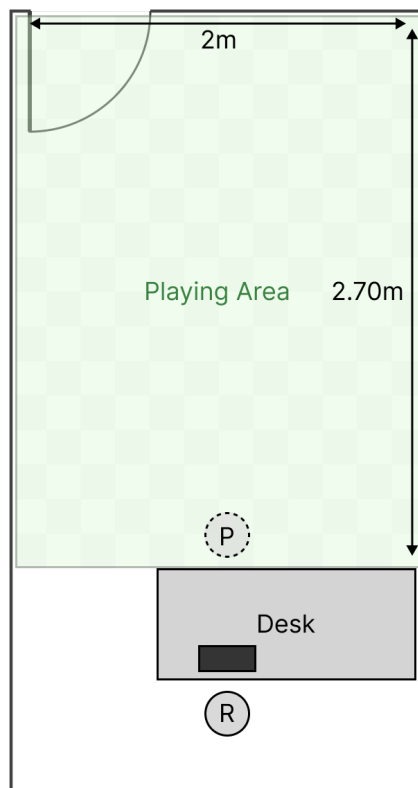


Figure 21: A top down diagram of the experiment setup during the hi-fi prototyping sessions

7.3 Procedure

The user study consisted of three parts: a pre-play-test questionnaire, playing the serious game in immersive VR, and a post-play-test questionnaire. The procedure was aided by a checklist to make sure all necessary steps are taken every play-test session, the researcher checklist can be seen in Appendix G.

In the pre-questionnaire before play-testing the VR game, participants were asked about their demographics, and their familiarity with the topic. In addition, to check

the knowledge, attitude and behaviour of participants regarding cybersecurity topics, the 'Human Aspects of Information Security Questionnaire' [26], or HAIS-Q for short, was applied. The HAIS-Q is a validated tool to get insight into human aspects of cybersecurity [26], and has been shown to be a good indicator of performance in a phishing experiment [26]. For this project questions from the HAIS-Q categories of email use and incident reporting were used, as those are the main topics discussed in the game. The questionnaire was made in Qualtrics [27], which is an online tool which can create and analyse surveys. The pre-play-test questionnaire questions can be found in Appendix H. At the start of the questionnaire, the participant is asked to fill in a participant number, which is randomly generated. This number was a number between 100-999, and generated using the website calculator.net. This participant number allows the questionnaire to be filled in anonymously, while still making it possible to connect which pre- and post-questionnaires are made by the same participant.

After the pre-play-test questionnaire, the participant was guided into the VR game. First, the participant was instructed on how to wear and adjust the VR headset in a way such that it is comfortable for them and that they can read text in game well. After the headset was successfully set-up, the participant was instructed on the controls of the game. The controls of the game were also displayed on the computer screen at the start of the game. After they pressed next on this screen, they would encounter a disclaimer screen.

After the VR section, the participant is instructed to complete a follow-up questionnaire. In the follow-up questionnaire participants were asked to rate the relevance and believability of different scenarios in the game. In addition, three of the six emails from the game were shown in the questionnaire and participants were asked to rate statements regarding the scenario of receiving the three emails. Aspects that were rated were how believable and how relevant the individual emails were for a healthcare setting. Besides the questions about the specific components of the game, participants were also asked about general points of improvement. The post-play-test questionnaire questions can be found in Appendix I

7.4 Design and analysis

The design of the study is a within-subjects design, with a pre-test post-test. Ideally there would be two groups, where participants get randomly assigned to either the group which tries the serious game and where the other group would be instructed to do nothing, so that there is also a control group. Instead, there was only one group, where the participants do a pre-test, then the intervention, followed by a post-test. The pre and post questionnaires both contain 15 questions from the HAIS-Q in total, 9 which are about mails, and 6 which are about incident reporting. The answers to these statements can be scored depending on whether 'Strongly disagree' or 'Strongly agree' was the best / 'correct' answer, with a score of 1 through 5, respective of the answer on the 5-point Likert scale that was used if agreeing with the statement was

correct, while it was assigned the other way around if agreeing with the statement was the worst answer. By adding up all these scores to the different HAIS-Q questions, a total HAIS-Q score can be calculated for every participant both before and after having played the intervention game. These two groups of HAIS-Q scores can then be analysed using a one tailed paired samples t-test.

In this case, the null hypothesis H_0 is as follows: 'There is no difference between the mean HAIS-Q scores of participants before and after playing the VR intervention (i.e. $\mu_0 = \mu_1$)', while H_1 is: 'The mean HAIS-Q scores of participants are higher after having played the game (i.e. $\mu_0 < \mu_1$)'. We can reject H_0 if $\alpha < 0.05$. To do this test, we assume that the responses of different participants are independent, the population data is normally distributed, and there are no extreme outliers.

8 Evaluation results

8.1 Results HAIS-Q score

Unfortunately, despite all the efforts made to recruit as many students as possible, only 5 participants participated which makes it difficult to make statistically significant claims about the HAIS-Q score, and relevance and believability scores. A calculation will still be done, but is not likely to be accurate.

By calculating the HAIS-Q scores in Excel for all the participants both before and after playing the game, it was found that there was an increase in HAIS-Q scores for all 5 participants after having played the game. As can be seen in Fig. 22, no outliers were found in the differences of the HAIS-Q scores.

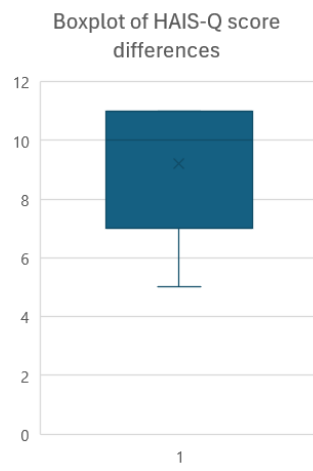


Figure 22: Box-plot of HAIS-Q score differences / improvements

The kurtosis of the HAIS-Q differences is 2.81, which is close to a normal distribution. The skewness of the HAIS-Q differences was found to be -1.67 which would suggest that the distribution was left-skewed. The lack of data makes it difficult to test the normality. The test statistic t was calculated to be 8.26. With $df = 5 - 1 = 4$ degrees of freedom, that gives us a p-value of 0.00059. This means the result is significant at $p < 0.05$. Therefore, we can reject H_0 at $\alpha = 0.05$. So, there is a significant improvement in HAIS-Q score for this group of participants, however a larger sample size needs to be analysed to see how well this finding can be generalised.

8.2 Results phishing signs

One of the open questions in the questionnaire was 'Please list all signs you can think of that would indicate an email is a phishing email', which was asked both before and after participants played the game in VR. The answers to this open question gave an indication of which of the five signs of phishing emails the participants already knew before playing the game, and which of the five signs of phishing emails they still remember after having played the game. The participant's answers were then

analysed for the phishing signs in the game, and counted if they were mentioned in a participant's answer. A graph of the processed results of this question can be seen in Fig. 23, and how these were counted will be explained below.

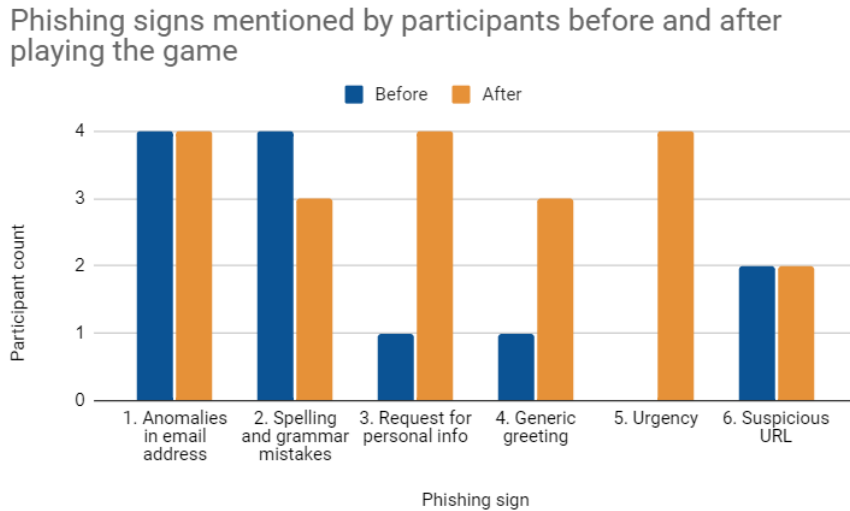


Figure 23: Overview of counted phishing signs in the open question 'Please list all signs you can think of that would indicate an email is a phishing email', before and after having played the game

1. Before playing the game, all four participants already knew 'Anomalies in email address' as a sign of phishing, as expressed by 'weird email address' (x2), 'weird spelled sender email address' or 'email addresses that don't look official'. After playing the game, 'Anomalies in email address', was once again mentioned by all four participants, however they all already knew this phishing sign before doing the intervention.
2. In addition, the second phishing sign 'spelling and grammar mistakes', was also already known by all four participants already as indicated by 'spelling mistakes' (x2), 'spelling errors' or 'incorrect grammar/writing' in their answer to the question. After playing the game, 'Spelling and grammar mistakes', was interestingly mentioned by only three of the four participants, even though all four mentioned this sign before having played the game. This is likely due to oversight by one of the participants
3. The third phishing sign in the game, 'Request for personal info' was already known by one of the four participants, as expressed in 'asking for bank information' in their answer. After having played the game, 'Request for personal info' was mentioned by all four of the participants, as shown by: 'asking (for) personal info(rmation)' (x3) and 'personal information request'.

4. The fourth phishing sign, 'Generic greeting' was already mentioned by only one of participants in the pre-play-test questionnaire, in the shape of 'referring to me by my Instagram name'. After having played the game 'Generic greeting' was mentioned by three of the four participants, as they mentioned 'generic greeting' (x2), and 'General introduction'. This means two of the participants newly listed 'Generic greeting' as a sign of a phishing email after having played the game.
5. The fifth phishing sign, 'Urgency', was not explicitly mentioned by any of the the four participants before having played the game. However, two participants mentioned something which could potentially be coded as 'Urgency', as they mentioned 'very much insisting you click on a link' or 'overly persuasive language'. After having played the game 'Urgency' was mentioned by all four of the participants: 'urgency' (x3), and 'urgent', which shows that this was a well remembered phishing sign from the game.
6. Finally, the sixth sign of phishing emails, a suspicious link or URL, was mentioned by two of the four participants upfront: 'very much insisting you click on a link', or 'Links in emails from unknown people' After having played the game 'Suspicious links / URLs' was mentioned by two of the participants: 'pushing you to click the link' and 'links'.

In addition to the five phishing signs discussed in the game, one other sign which was mentioned by participants before having played the game. This sign or category could be defined as 'a focus on money in the email', and was mentioned by all four participants as expressed in 'payment related content', 'asking for bank information', 'asking for money', 'Advertisement (prizes etc.) in the text'. This is an interesting discovery, and could be included in a new version of the game as a sign.

To summarise the findings of this phishing signs question: the phishing signs 'Anomalies in email address', and 'spelling and grammar mistakes' were already known by all four participants before having played the intervention. Another interesting finding was of an additional sign of phishing, which is not implemented in the game, mentioned by all four participants, which could be defined as 'a focus on money in the email'. After having played the game, the phishing signs 'Request for personal information', 'Generic greeting', 'Urgency' and all saw an increase in mentions, having a respective increase in mentions of three, two and four of the participants. This means the phishing sign of 'Urgency' has seen the most improvement within this participant group, from not being mentioned explicitly by any of the participants to being mentioned by all four participants.

These results show that the designed intervention was successful in educating about a request for personal info, a generic greeting and urgency as signs of phishing, and that the participants can still remember these signs a few minutes after having played the game.

A final interesting takeaway from analysis of the answers to this question was that the URL phishing sign was not mentioned more after having played the game. This could be because of the URL phishing sign text being too small or too subtle, this could be a point for further research.

8.3 Results questions about emails in the game

Regarding the statement 'Do you recognise this email from the game?', all three emails featured in the questionnaire were remembered by all four participants, showing that the emails were memorable for this participant group.

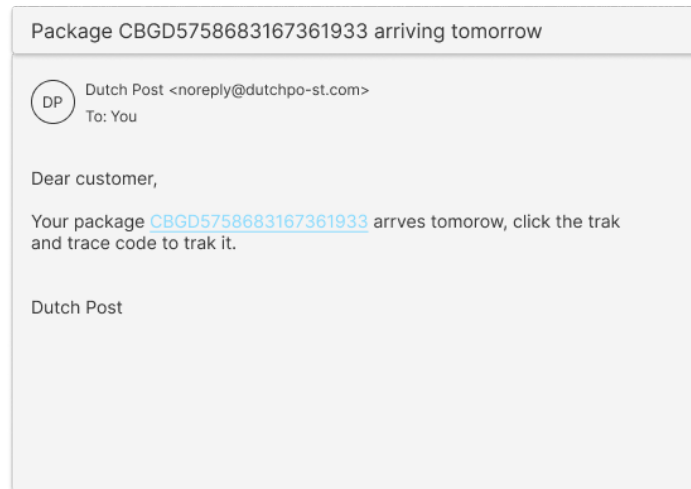


Figure 24: Package email, first email asked in the questionnaire

Regarding the first of these emails, the incoming package email (Fig. 24), the responses to whether the scenario of the email was believable were varied, with one participant answering 'strongly disagree', another 'somewhat disagree', while the other two answered 'somewhat agree'. When asked in the questionnaire about the relevance of this email to a healthcare scenario, none of the participants answered that it is relevant, which gives a potential indication that this email is not relevant for the healthcare sector. This would make sense as this email is modelled after a generic phishing email.

The second email that was asked about, the patient phishing email (Fig. 25), was deemed highly relevant and believable by all four participants, as they all responded with 'strongly agree' to both the relevance and believability Likert scales. This gives a potential indication that this email was successfully designed to be relevant and believable regarding a health context.

The third email, the legitimate reimbursement email (Fig. 26) had varied responses by the four participants. Regarding whether the email was believable, responses were 'somewhat disagree', 'somewhat agree' (x2), and 'strongly agree'. Regarding the relevance of this email, answers were 'somewhat disagree' and 'somewhat agree' (x3).

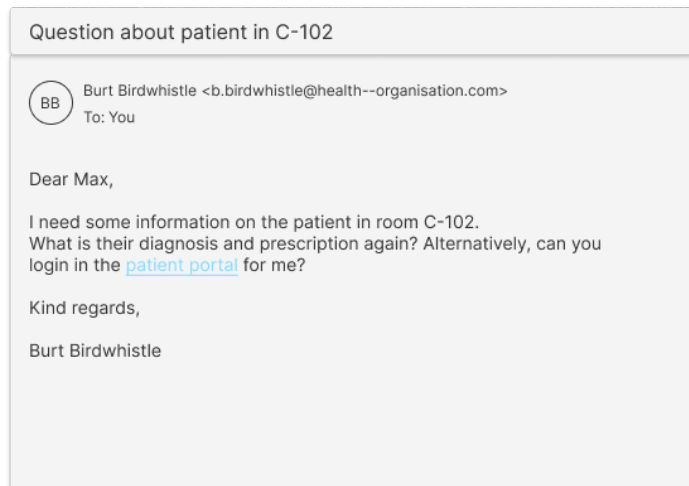


Figure 25: Patient phishing email

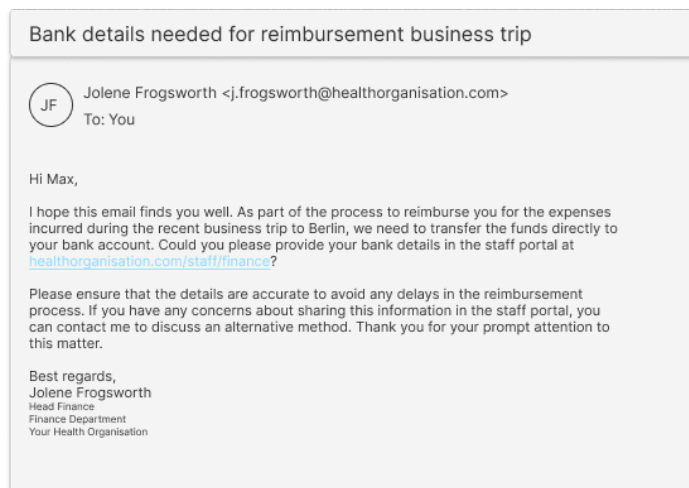


Figure 26: Reimbursement legitimate email

For all of these emails more data would need to be gathered with a bigger participant group to get a clearer picture.

8.4 Results 2FA voice call

The 2FA voice call received mixed opinions but seems to give an indication that it is somewhat believable and relevant by the four participants, as can be seen in Figs. 27 and 28. Once again, more data is needed.

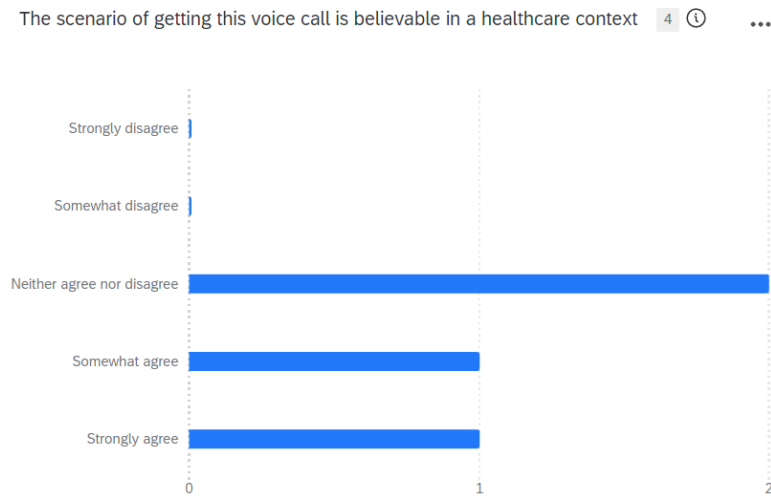


Figure 27: Answers to how believable the 2FA voice call was considering a healthcare context



Figure 28: Answers to how relevant the 2FA voice call was regarding a healthcare context

8.5 Results general questions

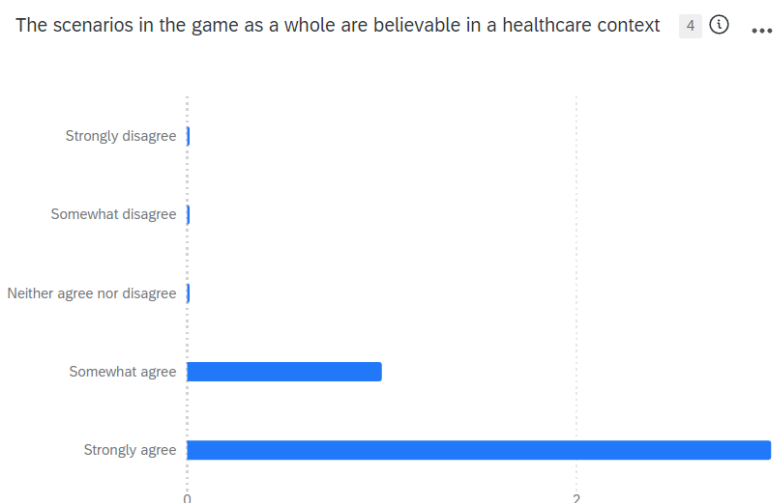


Figure 29: Questionnaire answers to how believable the scenarios were in the game as a whole in a healthcare context

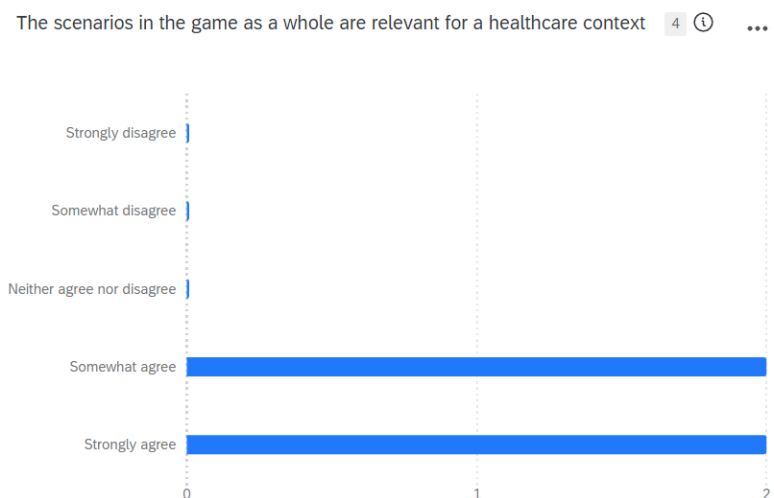


Figure 30: Questionnaire answers to how relevant the scenarios were in the game as a whole

As can be seen in Figs. 29 and 30, the answers to the questionnaire give a potential indication that the scenarios in the designed prototype game as a whole could be considered believable and relevant to a healthcare context, however more data with more participants should be gathered in order to say investigate whether there is a real pattern here when answered by a bigger group of healthcare students.

Regarding the open question 'What could be improved to make the game more believable considering a healthcare context?' some good points of feedback were

obtained. One of the participants suggested to add more contact details to the company contacts list, as a healthcare organisation usually has more than four employees. Other points of feedback mentioned by participants were that the game could focus more on patient information, healthcare products and passwords. Finally, adding emails from (fake) health insurance companies was also suggested to make the game more believable regarding a healthcare context.

Regarding the open question 'What could be improved to make the game more relevant considering a healthcare context?' some additional suggestions were obtained. Three of the four questionnaire participants expressed a sentiment in their answer to this question along the lines of having more patient related cases or scenarios in the game to make the game more relevant to a healthcare context. Specific suggestions regarding more scenarios involving patients were to have scenarios about a patient's information or their health insurance. One participant mentioned in their response to this question that the package email was not healthcare related, but specified that it could be possible to get such an email in a healthcare organisation, because phishing offenders send phishing emails to all email addresses, including corporate ones, and therefore they suggested to leave it in the game.

Finally, in the other remarks section, one of the participants mentioned that the 2FA voice call came very abruptly, which meant they missed the first half of the message. They suggested to add an incoming message on the screen which you need to accept first before the audio starts playing. Another general remark made by a participant here was that they are normally not so critical about analysing emails, but they behaved differently because they knew it was a game about phishing and there were signs on the screen. They thought that they would not have done exactly the same if they did not know that. A last point of improvement that was mentioned here was to increase the size of the text on the emails and the company contacts list.

8.6 Results from observation of game-play footage

Besides the survey data there were also findings about the usability of the program discovered through observation of the game-play. One point of improvement that was found was to only process phishing emails if they have the right stamp combination, as participants could process phishing emails regardless of whether they marked them with stamps or not. This means the participants could miss some of the phishing signs. It was also not clear to some of the participants that a mail can have multiple stamps. In addition, two of the participants expected to put the mail in the phishing area, and then mark them with stamps afterwards, when this happened they were explained how the game expects them to stamp the email before putting it in the phishing section, so that the participant would still get the intended experience. Another point of improvement discovered was that the 2FA voice triggered reasonably soon in the game for 3 out of the 5 participants, three minutes seems too short of a time to trigger the 2FA voice call, as some of the participants were still getting used to the game by that time.

The controls screen was clear, as participants did not open any external menus by using the top buttons on the controllers. Although, one participant did try to move around using the joystick, which was not necessary in the program, but it was not mentioned on the controls screen that the joystick is not necessary. Also, the company contacts list was used intuitively by four out of five of the participants to check the emails from company employees.

9 Discussion

9.1 Implications & limitations

SQ 1: To what extent does the designed intervention influence the score on the Human Aspects of Information Security Questionnaire?

All participants scored higher on the HAIS-Q after having played the game, where the difference was found to be significant between before and after playing the game. However, five participants is too little data to generalise to all students of health-related studies, more data is needed here. In addition, students are a different group from people who already work in the healthcare sector, so these results should also not be generalised to that group.

SQ 2: How well do the participants remember the intended learning goals of the designed game?

The play-testing has shown first indications that the designed hi-fi prototype succeeds in teaching about three of the five phishing signs in the game, as gathered from answers to the open questions which asked the participants to list all phishing signs they knew both before and after having played the game. The phishing signs that were successfully remembered were: 'Request for personal info', 'A generic greeting', and 'Urgency'. The other two signs 'Anomalies in email address', and 'Spelling and grammar mistakes' were already known by the participant group, and could therefore not be investigated and need to be further researched. The additional sign of 'a suspicious URL', did not see an improvement after participants played the game, a future version of the game would have to work on making this sign clearer.

SQ 3: To what extent are the scenarios in the game deemed relevant for a healthcare setting? & SQ 4: To what extent are the scenarios in the game deemed believable for a healthcare setting?

The results to how the participants rated the relevance and believability of the game considering a healthcare context could give a potential indication that the game's scenarios are both relevant and believable considering a health context. Regarding these relevance and believability constructs a test of content validity should be done, as those statements were made by myself. More formulations of the same constructs of relevance and believability would need to be added to the questionnaire to properly investigate this. More could be looked into how to accurately investigate believability and relevance for the healthcare context using a verified questionnaire.

SQ 5: How could the scenarios in the designed game be made more relevant to a healthcare setting? & SQ 6: How could the scenarios in the designed game be made more believable regarding a healthcare setting?

Several suggestions were obtained in order to make the game more relevant and believable for the healthcare setting. The main point was to include more scenarios in the game relating to patients, such as more scenarios involving patient data or patient health insurance. The phishing email about receiving a package appears to not be relevant based on the answers from the participants. However, it is a different question whether that means it should be kept in the game or not, as it could still be

realistic and have added benefit. Whether to include irrelevant phishing emails could be a topic for further research.

Besides having more participants, it would be better to have a more diverse representation of participants of different demographics, such as more variety in gender. The designed program should also be tested with a participant group of participants who have less background familiarity with phishing, as that is likely to influence the results. In the current study all participants were already at least somewhat familiar with phishing, which is a limitation. This background familiarity also made it impossible to test whether phishing signs 'Anomalies in email address' and 'Spelling and grammar mistakes' were successfully taught to the participants, as all participants already knew those two phishing signs before having played the game. There is also the possibility that this open question is not fully indicative of a person's knowledge, as they might forget to list every sign they know, as was seen with the results of phishing sign 'spelling and grammar mistakes'. Another limitation of the user study is that all participants had a university level degree, more research needs to be done on how participants from different educational backgrounds experience the game. An important limitation of the study is that it has insufficient data to generalise these findings to all health related students. A final limitation is that the game itself is still a prototype with elements that could be more polished, and this could influence the effectiveness of the intervention.

9.2 Future work

A primary aspect for future work is to play more into the strengths of immersive VR. The designed intervention ended up not fully making use of all the strengths of immersive VR. Walking around the office, and simulating social interactions in VR would make the program play more into the unique capabilities of VR. A planned feature was for the player to be able to walk to the office of a fellow employee, if the player was doubtful of the legitimacy of the email. Furthermore, immersive VR could also be used to simulate in-person social interactions with cyber offenders.

In the future, the intervention could also be expanded to make use of dynamic difficulty adjustment to help increase learning. For example, the 5 phishing signs system could be used to adapt the game to increase the frequency of emails with the phishing signs that the player is not yet good at spotting by keeping track of how well the player recognises the 5 individual phishing signs.

Another idea for future work is to research the issue of false positives in phishing emails, as there are times where an innocent email is being marked as suspicious. The designed program in this GP could very well be used as a base to investigate how different people categorise emails.

As it was discovered that participants remembered three of the signs of phishing mentioned in the game, future work could research how long participants remember the information that was taught in the game.

Finally, in the future the designed game could potentially be used as a base for practical use in healthcare organisations, however a lot more research with a large, diverse group of actual healthcare employees would have to be done first to validate whether this game works for that group. Besides that, some aspects of the game should also be polished further before it could be used in practice.

10 Conclusion

This graduation project has given insight into how an immersive VR serious game can be designed that educates the user about two social engineering cybersecurity threats in a healthcare setting. The user test that was done demonstrated that the designed serious game is successful at teaching the participants at least three signs of phishing, while the other two signs need to be further investigated as they were already known by the participant group. The additional sign of 'a suspicious URL', did not see an improvement after participants played the game. In addition, the graduation project has given a potential indication that the intervention can improve HAIS-Q scores, and that the scenarios in the designed intervention are relevant and believable regarding a health context, although more data is needed.

The findings in this graduation project give an indication that there is some potential in utilising immersive VR serious games for education about cybersecurity risks in a healthcare context. This graduation project also resulted in great insights on how to create an immersive VR cybersecurity game specifically for a healthcare setting, which can be taken into account by future cybersecurity education programs. This project has given a potential glimpse into how novel ways of teaching, such as ones making use of immersive VR, can help improve the world, and I am looking forward to further developments in this field.

References

- [1] H. Aldawood and G. Skinner, “Educating and raising awareness on cyber security social engineering: A literature review,” in *2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE)*, 2018, pp. 62–68. DOI: [10.1109/TALE.2018.8615162](https://doi.org/10.1109/TALE.2018.8615162).
- [2] A. Baillon, J. De Bruin, A. Emirmahmutoglu, E. Van De Veer, and B. Van Dijk, “Informing, simulating experience, or both: A field experiment on phishing risks,” *PLoS ONE*, vol. 14, no. 12, 2019. DOI: [10.1371/journal.pone.0224216](https://doi.org/10.1371/journal.pone.0224216). [Online]. Available: <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85076696655&doi=10.1371%2fjournal.pone.0224216&partnerID=40&md5=65ee9bb9553da3733035153e8300bf32>.
- [3] S. Bakker, *Literature review on cybersecurity threats and weaknesses for the design of an educational immersive vr intervention*, 2024.
- [4] I. Casey, *Nhs england confirm patient data stolen in cyber attack*, 2024. [Online]. Available: <https://www.bbc.com/news/articles/c9777v4m8zdo>, last accessed 3/7/2024.
- [5] H. Chen and K. Magramo, *Finance worker pays out \$25 million after video call with deepfake ‘chief financial officer’*, 2024. [Online]. Available: <https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html>, last accessed 15/3/2024.
- [6] K.-K. R. Choo, “The cyber threat landscape: Challenges and future research directions,” *Computers & Security*, vol. 30, no. 8, pp. 719–731, 2011, ISSN: 0167-4048. DOI: [10.1016/j.cose.2011.08.004](https://doi.org/10.1016/j.cose.2011.08.004). [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0167404811001040>.
- [7] ElevenLabs, *Text to speech & ai voice generator | elevenlabs*, 2024. [Online]. Available: <https://elevenlabs.io/>, last accessed 25/6/2024.
- [8] J. van den Elshout, *Healthcare workers stop active hacker in cybertruck*, 2023. [Online]. Available: <https://www.utwente.nl/en/news/2023/10/1184733/healthcare-workers-stop%20active-hacker-in-cybertruck>, last accessed 27/3/2024.
- [9] ENISA, “2023 data breach investigations report,” 2023, ISBN: 978-92-9204-645-3. DOI: [10.2824/782573](https://doi.org/10.2824/782573). [Online]. Available: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023>.
- [10] S. Gatlan, *Phishing incident exposes medical, personal info of 60k patients*, 2019. [Online]. Available: <https://www.bleepingcomputer.com/news/security/phishing-incident-exposes-medical-personal-info-of-60k-patients/>, last accessed 3/7/2024.

- [11] I. Ghafir, J. Saleem, M. Hammoudeh, *et al.*, “Security threats to critical infrastructure: The human factor,” *The Journal of Supercomputing*, vol. 74, pp. 4986–5002, 2018. DOI: [10.1007/s11227-018-2337-2](https://doi.org/10.1007/s11227-018-2337-2). [Online]. Available: <https://doi.org/10.1007/s11227-018-2337-2>.
- [12] W. Greenwald, *Brownboxing: The secret to vr development*, 2018. [Online]. Available: <https://medium.com/pcmag-access/the-secret-to-vr-development-brownboxing-303cbc1e3d6e>, last accessed 13/6/2024.
- [13] B. B. Gupta, Arachchilage, N. A. G., and K. E. Psannis, “Defending against phishing attacks: Taxonomy of methods, current issues and future directions,” *Telecommunication Systems*, vol. 67, no. 2, pp. 247–267, 2018. DOI: [10.1007/s11235-017-0334-z](https://doi.org/10.1007/s11235-017-0334-z). [Online]. Available: <https://doi.org/10.1007/s11235-017-0334-z>.
- [14] B. Gupta, A. Tewari, A. K. Jain, and D. P. Agrawal, “Fighting against phishing attacks: State of the art and future challenges,” *Neural Computing and Applications*, vol. 28, no. 12, pp. 3629–3654, 2017. DOI: [10.1007/s00521-016-2275-y](https://www.scopus.com/inward/record.uri?eid=2-s2.0-84961211997&doi=10.1007%2fs00521-016-2275-y&partnerID=40&md5=c9be65bfd15ee4b02b0dce84b3df9616). [Online]. Available: <https://www.scopus.com/inward/record.uri?eid=2-s2.0-84961211997&doi=10.1007%2fs00521-016-2275-y&partnerID=40&md5=c9be65bfd15ee4b02b0dce84b3df9616>.
- [15] C. D. Hylender, P. Langlois, A. Pinto, and S. Widup, *2023 data breach investigations report*, 2023. [Online]. Available: [verizon.com/dbir](https://www.verizon.com/dbir).
- [16] Infosecure, *Security awareness game | infosecure*, 2020. [Online]. Available: <https://www.infosecure.com/nl/security-awareness-game>, last accessed 24/4/2024.
- [17] ISO, *Iso/iec 27001:2022 - information security management systems - requirements*, 2022. [Online]. Available: <https://www.iso.org/standard/27001>, last accessed 27/6/2024.
- [18] M. Jain, A. Sinha, A. Agrawal, and N. Yadav, “Cyber security: Current threats, challenges, and prevention methods,” in *2022 International Conference on Advances in Computing, Communication and Materials (ICACCM)*, 2022, pp. 1–9. DOI: [10.1109/ICACCM56405.2022.10009154](https://doi.org/10.1109/ICACCM56405.2022.10009154).
- [19] J. Jang-Jaccard and S. Nepal, “A survey of emerging threats in cybersecurity,” *Journal of Computer and System Sciences*, vol. 80, no. 5, pp. 973–993, 2014, Special Issue on Dependable and Secure Computing, ISSN: 0022-0000. DOI: [10.1016/j.jcss.2014.02.005](https://doi.org/10.1016/j.jcss.2014.02.005). [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0022000014000178>.
- [20] 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*, ser. SIGCSE ’18, Baltimore, Maryland, USA: Association for Computing Machinery, 2018, pp. 68–73, ISBN: 9781450351034. DOI: [10.1145/3159450.3159591](https://doi.org/10.1145/3159450.3159591). [Online]. Available: <https://doi.org/10.1145/3159450.3159591>.

- [21] L. Klooster, *Vr cybereducation : Improving the human factor in cybersecurity through an educational virtual reality program*, 2022. [Online]. Available: https://essay.utwente.nl/93717/1/Klooster_BA_EEMCS.pdf.
- [22] S. Lyngaas, *A third of americans could have had data stolen in big health care hack*, 2024. [Online]. Available: <https://edition.cnn.com/2024/05/01/politics/data-stolen-healthcare-hack/index.html>, last accessed 3/7/2024.
- [23] A. H. Mader and W. Eggink, “A design process for creative technology,” in *Proceedings of the 16th International conference on Engineering and Product Design, E&PDE 2014*, Enschede, the Netherlands: The Design Society, 2014, pp. 568–573, ISBN: 978-1-904670-56-8.
- [24] S. Nifakos, K. Chandramouli, C. K. Nikolaou, *et al.*, “Influence of human factors on cyber security within healthcare organisations: A systematic review,” *Sensors*, vol. 21, no. 15, 2021. DOI: [10.3390/s21155119](https://doi.org/10.3390/s21155119). [Online]. Available: <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85111344036&doi=10.3390%2fs21155119&partnerID=40&md5=b29edee2c03550d6443c08a63b8b4b28>.
- [25] OneBonsai, *Cybersecurity awareness vr for companies - onebonsai*, 2023. [Online]. Available: <https://onebonsai.com/vr-training/cybersecurity-awareness-training-in-vr/>, last accessed 24/4/2024.
- [26] 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, 2017, ISSN: 0167-4048. DOI: <https://doi.org/10.1016/j.cose.2017.01.004>. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0167404817300081>.
- [27] Qualtrics, *Qualtrics xm: The leading experience management software*, 2024. [Online]. Available: <https://www.qualtrics.com/>, last accessed 25/6/2024.
- [28] Resonite, *Resonite*, 2024. [Online]. Available: <https://resonite.com/>, last accessed 12/4/2024.
- [29] Security.nl, *Ziekenhuis vs waarschuwt 68.000 patiënten voor datalek door phishing*, 2019. [Online]. Available: https://www.security.nl/posting/627261/Ziekenhuis+VS+waarschuwt+68_000+pati%C3%ABnten+voor+datalek+door+phishing, last accessed 3/7/2024.
- [30] Shubham, R. Kumar, A. Aditya, and B. D. Shivahare, “Cyber crime prevention and techniques: A comprehensive survey,” in *2023 3rd International Conference on Innovative Sustainable Computational Technologies (CISCT)*, 2023, pp. 1–4. DOI: [10.1109/CISCT57197.2023.10351225](https://doi.org/10.1109/CISCT57197.2023.10351225).
- [31] Z-CERT, *Cybersecurity dreigingsbeeld voor de zorg 2023*, 2024. [Online]. Available: <https://z-cert.nl/cybersecurity-dreigingsbeeld-voor-de-zorg-2023/>.

A Expert interview questions

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

Demographics questions

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

Education / awareness training questions

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

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

1. What do you think the benefits are of teaching about cybersecurity through a simulation based approach?
 - (a) And what do you think the drawbacks are?
2. What do you think the benefits are of teaching about cybersecurity through a serious game based approach?
 - (a) And what do you think the drawbacks are?

3. All in all, of these two, which one do you think is the best, considering the benefits and drawbacks?

(a) Why do you think this approach is better?

Social engineering questions

1. What technological/organisational elements are there in your organisation that a cyber-attacker could use to do social engineering? (*USBs, phone calls are commonly used in the company for example, can be used to create a scenario in the VR simulation*)

(a) Of those mentioned, what do you see as the most important weakness?

(b) Why do you see this as the most important weakness?

2. What possible social engineering dangers would be good to teach employees in your organisation about?

(a) Why these social engineering dangers?

3. What type of social engineering methods have attackers tried to target your organisation with, be it successful or not? *Do not need concrete examples.*

4. What type of social engineering attacks are already successfully prevented because of current cybersecurity training?

Physical cyberthreats questions³

Concluding questions

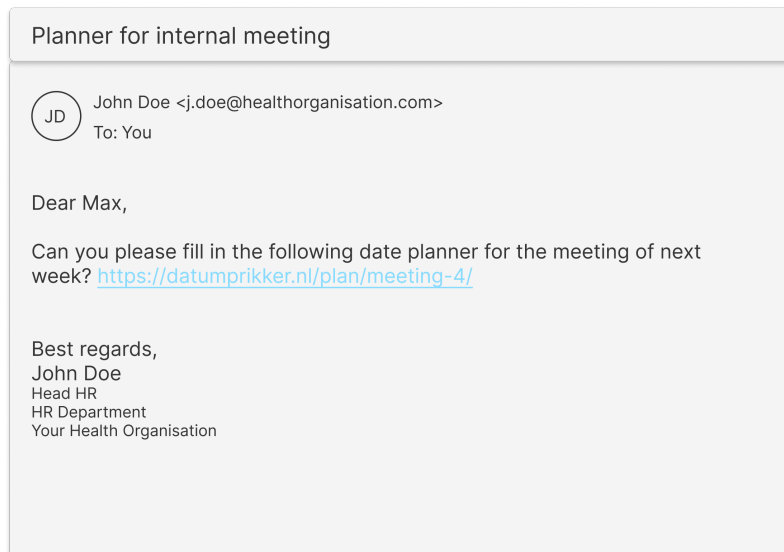
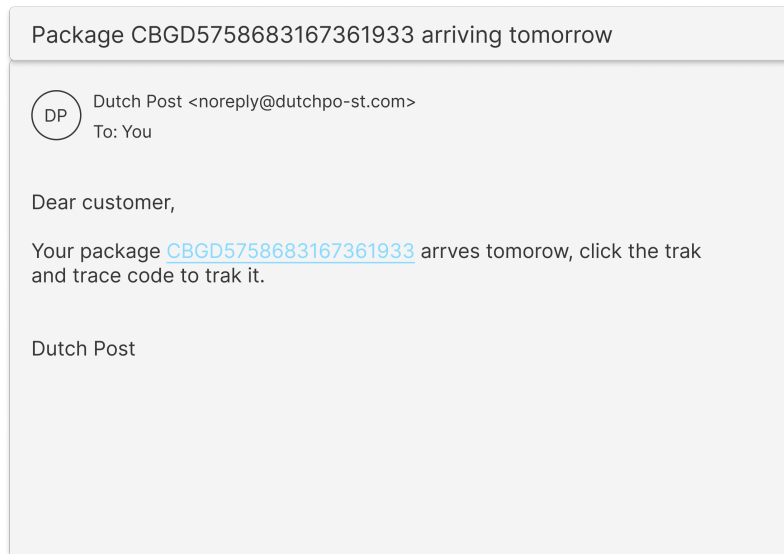
1. What are sources that you consult to stay up to date on cybersecurity?

2. Finally, do you have any other remarks you would like to give us as we conclude this interview?

Thank interviewee and conclusion of the interview

³There were also some questions about physical cyberthreats which were asked to the experts by a student doing a different version of this GP, which focuses on the physical cyberthreats. They are not relevant for this GP and are therefore omitted

B Mock emails used in lo-fi paper prototyping



Bank details needed for reimbursement business trip



Jolene Frogsworth <j.frogsworth@healthorganisation.com>

To: You

Hi Max,

I hope this email finds you well. As part of the process to reimburse you for the expenses incurred during the recent business trip to Berlin, we need to transfer the funds directly to your bank account. Could you please provide your bank details at your earliest convenience? Here's the information we need:

1. Bank Name
2. Account Number
3. Routing Number (or SWIFT/BIC code for international transfers)
4. Account Holder's Name.

Please ensure that the details are accurate to avoid any delays in the reimbursement process. If you have any concerns about sharing this information over email, feel free to drop by my office or give me a call, and we can discuss an alternative method. Thank you for your prompt attention to this matter.

Best regards,
Jolene Frogsworth
Head Finance
Finance Department
Your Health Organisation

Unusual bank activity detected



Bank Security Team <security@banking.com>

To: You

Dear customer,


We have detected unusual activity in your account and need you to verify your information immediately to avoid suspension. Please click the link below and log in with your credentials to verify your account details:

[Verify Now](#)

Failure to verify your account within 24 hours will result in your account being locked. Thank you for your prompt attention to this matter.

Sincerely,
Bank Security Team

Update your PayPal information

 PayPal Security <security@paypa1.com >
To: You

Dear PayPal user,

We have not detected any login to your account in one year. To ensure the safety of your account, please update your account information.


Click the link below to update your information:

[Update Information](#)

Thank you for your cooperation.

Best regards,
PayPal Security Team

Question about patient in C-102

 Burt Birdwhistle <b.birdwhistle@health--organisation.com>
To: You

Dear Max,

I need some information on the patient in room C-102.
What is their diagnosis and prescription again? Alternatively, could I use your login credentials for the patient portal?

Kind regards,

Burt Birdwhistle

C Lo-fi interview questions

The following are the questions asked to participants after they were done with the lo-fi prototype.

1. What was unclear to you, if anything was unclear?
2. What was the most frustrating moment or interaction?⁴
3. Was there anything you wanted to do but couldn't?⁵
4. If you had a magic wand and could change anything about the experience what would it be?⁶
5. What was your favourite moment or interaction?⁷
6. What did you think of the instructions on the computer screen?
 - (a) What did you think of the text version
 - (b) What did you think of the more visual version
7. Did the interface / design of the emails resemble real life emails?
 - (a) Why did the interface / design of the emails resemble real life emails or not?
8. What could be better about looking up contacts / what information would you like to know to verify whether you know the person?
9. What could be improved about the two factor authentication request?
10. Did you learn anything from this experience?
 - (a) If so what was it?
11. Finally, do you have any other remarks or comments you would like to share?

⁴Note: questions 2,3,4 and 5 were taken from Shawn Patton's brownboxing technique [12]

⁵See footnote 4

⁶See footnote 4

⁷See footnote 4

D Consent form and information letter user study

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

YOU WILL BE GIVEN A COPY OF THIS INFORMED CONSENT FORM

Please tick the appropriate boxes

Yes No

Taking part in the study

I have read and understood the study information dated [7/6/2024], or it has been read to me. I have been able to ask questions about the study and my questions have been answered to my satisfaction.

I consent voluntarily to be a participant in this study and understand that I can refuse to answer questions and I can withdraw from the study at any time, without having to give a reason.

I understand that taking part in the study involves participating in a Hi-Fi prototype or a serious game in VR. Before and after testing the Hi-Fi prototype you will be asked to fill in an anonymized questionnaire. During the Hi-Fi prototype anything interesting to the researcher will be noted down.

Risks associated with participating in the study

I understand that taking part in the study involves the following risks: The risk of motion sickness. If I feel any motion sickness during the testing the Hi-Fi prototype I understand that I can take off the headset and that the testing will stop. In addition to this there is a small risk to bump into objects or walls, however the researcher will try to minimize this risk.

I understand that taking part in the study involves the following risks: The risk of discovering and sharing potential cybersecurity weaknesses. The study itself will contain cybersecurity training containing a few tasks of which the performance could indicate weaknesses when performed poorly. These weaknesses can form a risk for potential cyberattacks. To minimize this risk the questionnaires will be anonymous to prevent the researchers from knowing how each participant performs. Any sensitive information will not be shared beyond the research team and there will be no statements regarding specific participants.

Use of the information in the study

I understand that information I provide will be used for a bachelor thesis and that this thesis will be publicly available in the University of Twente thesis repository.

I understand that personal information collected about me that can identify me, such as [e.g. my name or where I live], will not be shared beyond the study team.

I agree that my information can be quoted in research outputs

I agree to share the following demographics: age, gender and type of study.

I agree that my anonymous gameplay footage will be recorded without audio.

Future use and reuse of the information by others

I give permission for the answers of the anonymized questionnaire that I provide to be archived in University of Twente thesis repository so it can be used for future research and learning.

Signatures

Name of participant

Signature

Date

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

UNIVERSITY OF TWENTE.

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

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

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

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

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

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

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

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

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

Study contact details for further information:

Sem Bakker,

Sven Sonneveld: _____

Contact Information for Questions about Your Rights as a Research Participant

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

E Walk-through screenshots of the game







F Recruitment flyer

Hey, are you a student of
BMT, TG or Health Sciences?



Help us with testing a
VR cybersecurity training!

Image by freepik - <https://www.freepik.com/free-vector/realistic-virtual-reality-headset> - 11583265.htm
Image by rawpixel.com on Freepik - <https://www.freepik.com/free-vector/blue-futuristic-networking-technology-vector> - 1961032.htm

Hey! We are Sem and Sven, and we've been working on two versions of a VR cybersecurity serious game as part of a graduation project. The goal of these games is to help raise the knowledge and awareness of cybersecurity specifically in the healthcare sector. For this we would like to have students of healthcare related studies participate in this user test, so that is why you could help us. This user test will take around 45 minutes of your time and will be done on campus, during which there will be snacks. The location is mentioned in the datumpriker. It does not matter if you are experienced with VR or not, as the game should also work for newcomers to VR. Your participation would be highly appreciated!

Important: there is a risk of motion sickness with the use of VR, so please do not participate if you have a history of motion sickness.

There are two versions of the graduation project that teach about two types of cybersecurity threats, you can sign up for either one or both studies using the QR(s) below.

Physical and technical cyberthreats	Social engineering cyberthreats
	

Image by rawpixel.com on Freepik - <https://www.freepik.com/free-vector/blue-futuristic-networking-technology-vector> - 1961032.htm

G Researcher checklist during hi-fi prototyping

Checklist

Before: setup quest link, join the resonite world, set proper user scale, and set movement mode to teleport

Start:

- Oral briefing, information letter, consent form
- Let them scan QR code for first questionnaire
 - [Generate random participant number between 100-999](#)
 - Check if number not taken yet
 - Write down participant number in the list

VR section:

- Explain controls before they go in VR
- Remind them that if they feel uncomfortable or motion sick that they can take a break and take off the headset
- Instruct on how to wear VR headset
 - Confirm that they can read the text in game well
 - Demonstrate the boundaries of the room when they are in VR. So that they can prevent collision with walls
- Start OBS recording of the gameplay
- Guide them through the program if needed

After VR:

- Set up the snacks in bowls
- Let them scan QR code for second questionnaire
 - Remind them their participant number

End:

- Debrief over deception with reason why necessary, with the option of withdrawing consent
- Remind them their number participant number so they can redact their data within one week of the playtesting session if they want

H Pre-play-test questionnaire questions

1. **Welcome to the user test of a VR Social Engineering Cybersecurity game in a Healthcare setting**

Before we start with the playtesting, this questionnaire will first ask a few questions on demographics and ask you to rate a few statements.

2. What is your participant number?

(Text field)

3. **Demographics questions**

4. What type of study are you studying?

- (a) Health related (BMT, TG, Gezondheidswetenschappen, other)
- (b) Non-health related

5. What is your age range?

- (a) 18-24
- (b) 24-30
- (c) 30-36
- (d) 36-42
- (e) 42-48

6. What is your gender?

- (a) Male
 - (b) Female
 - (c) Non-binary / third gender
 - (d) Prefer not to say
-

7. **Demographics: background experience**

8. How familiar are you with VR?

- (a) Have never tried VR (1)
- (b) Have tried VR a few times (1-3 times)
- (c) Have tried VR a good amount of times (4-10 times)
- (d) Have tried VR a lot (10+ times)

9. I am familiar with phishing emails

(5 point Likert scale from 'Strongly disagree' to 'Strongly agree')

10. **Please read the following definition of Social Engineering**

Social engineering refers to a type of cybersecurity attack where the attacker tries to get the victim to do an action that is of the benefit to the attacker through persuasion techniques.

11. I am familiar with the concept of social engineering
(5 point Likert scale from 'Strongly disagree' to 'Strongly agree')

12. **Statements regarding emails⁸**

The following are a few statements about emails, please rate them on what extent you disagree/agree with them

13. I am allowed to click on any links in emails from people I know
(5 point Likert scale from 'Strongly disagree' to 'Strongly agree')
14. It's always safe to click on links in emails from people I know
(5 point Likert scale from 'Strongly disagree' to 'Strongly agree')
15. I don't always click on links in emails just because they come from someone I know
(5 point Likert scale from 'Strongly disagree' to 'Strongly agree')
16. I am not permitted to click on a link in an email from an unknown sender
(5 point Likert scale from 'Strongly disagree' to 'Strongly agree')
17. Nothing bad can happen if I click on a link in an email from an unknown sender
(5 point Likert scale from 'Strongly disagree' to 'Strongly agree')
18. If an email from an unknown sender looks interesting, I click on a link within it.
(5 point Likert scale from 'Strongly disagree' to 'Strongly agree')
19. I am allowed to open email attachments from unknown senders.
(5 point Likert scale from 'Strongly disagree' to 'Strongly agree')
20. It's risky to open an email attachment from an unknown sender
(5 point Likert scale from 'Strongly disagree' to 'Strongly agree')
21. I don't open email attachments if the sender is unknown to me.
(5 point Likert scale from 'Strongly disagree' to 'Strongly agree')
22. Please list all signs you can think of that would indicate an email is a phishing email.
(Multi-line text field)

⁸Questions 13 until 21 in this section were taken from the HAIS-Q [26]

23. **Statements regarding cybersecurity incidents**⁹

The following are a few statements about cybersecurity incidents, please rate them on what extent you disagree/agree with them

24. It's optional to report security incidents.
(5 point Likert scale from 'Strongly disagree' to 'Strongly agree')
25. It's risky to ignore security incidents, even if I think they're not significant.
(5 point Likert scale from 'Strongly disagree' to 'Strongly agree')
26. If I noticed a security incident, I would report it.
(5 point Likert scale from 'Strongly disagree' to 'Strongly agree')
27. If I see someone acting suspiciously in my workplace, I should report it.
(5 point Likert scale from 'Strongly disagree' to 'Strongly agree')
28. If I ignore someone acting suspiciously in my workplace, nothing bad can happen.
(5 point Likert scale from 'Strongly disagree' to 'Strongly agree')
29. If I saw someone acting suspiciously in my workplace, I would do something about it.
(5 point Likert scale from 'Strongly disagree' to 'Strongly agree')

⁹Questions 24 until 29 in this section were taken from the HAIS-Q [26]

I Post-play-test questionnaire questions

1. Post Playtest Questionnaire

Now that you have playtested the game, please answer a couple more questions.

2. What is your participant number?
(Text field)
-

3. Statements regarding emails

The following are a few statements about emails, please rate them on what extent you disagree/agree with them.

4. *This section repeats the 9 HAIS-Q questions about emails that were also in the pre-play-test questionnaire. These are questions 13 until 22 numbered in the pre-play-test questionnaire. For brevity's sake they are not written out again here*
-

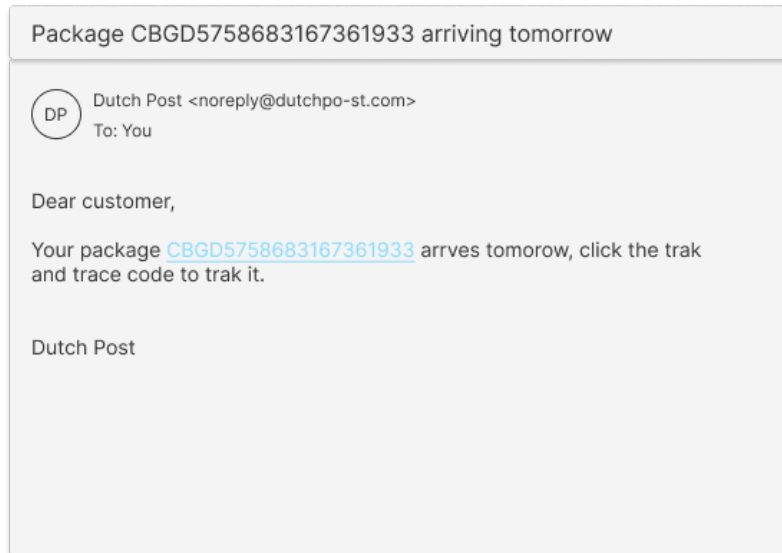
5. Statements regarding cybersecurity incidents

The following are a few statements about cybersecurity incidents, please rate them on what extent you disagree/agree with them

6. *This section repeats the 6 HAIS-Q questions about cybersecurity incidents that were also in the pre-play-test questionnaire. These are questions numbered 24 until 29 in the pre-play-test questionnaire. For brevity's sake they are not written out again here*
-

7. Questions about phishing emails in the game

8. Please look at the following email:



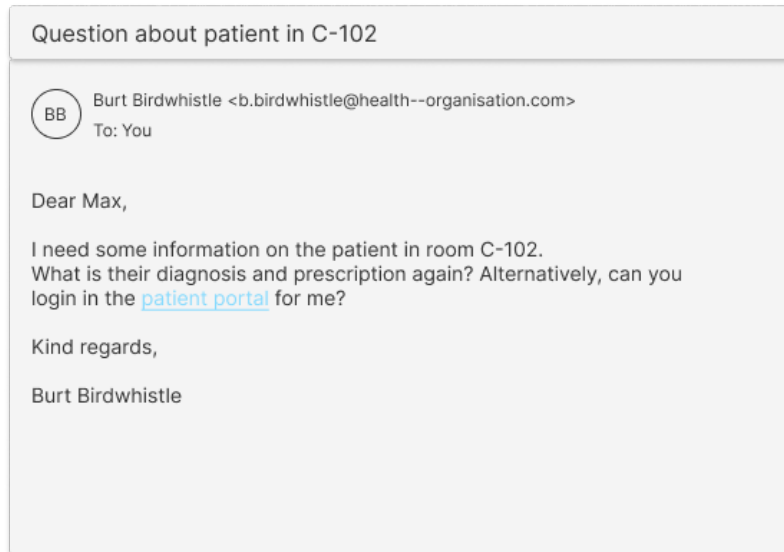
9. Do you recognise this email from the game?

(yes/no)

10. The scenario of getting this email is believable in a healthcare context
(5 point Likert scale from 'Strongly disagree' to 'Strongly agree')

11. The scenario of getting this email is relevant to a healthcare context
(5 point Likert scale from 'Strongly disagree' to 'Strongly agree')

12. Please look at the following email:



13. Do you recognise this email from the game?

(yes/no)

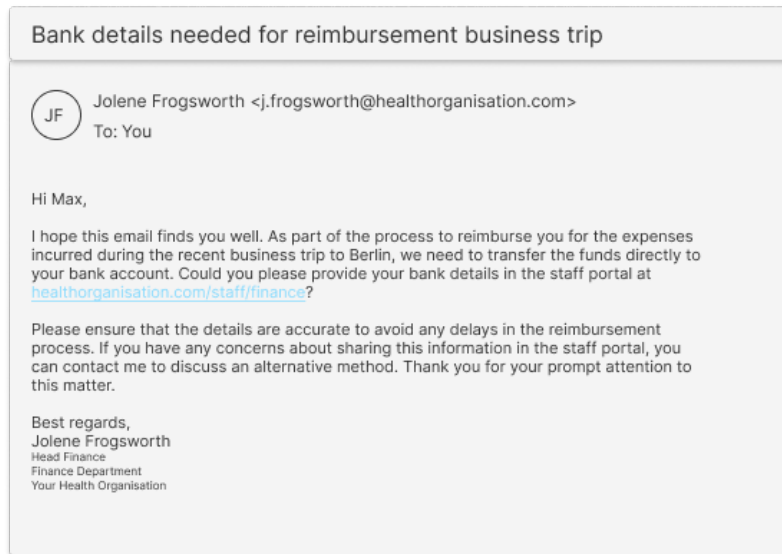
14. The scenario of getting this email is believable in a healthcare context

(5 point Likert scale from 'Strongly disagree' to 'Strongly agree')

15. The scenario of getting this email is relevant to a healthcare context

(5 point Likert scale from 'Strongly disagree' to 'Strongly agree')

16. Please look at the following email:



17. Do you recognise this email from the game?
(yes/no)

18. The scenario of getting this email is believable in a healthcare context
(5 point Likert scale from 'Strongly disagree' to 'Strongly agree')

19. The scenario of getting this email is relevant to a healthcare context
(5 point Likert scale from 'Strongly disagree' to 'Strongly agree')

20. **Questions about the 2 Factor Authentication request voice call**

During the game you got a voice call, which prompted you to either approve or deny a 2 Factor Authentication request, the following are statements about that scenario in the game.

21. The scenario of getting this voice call is believable in a healthcare context
(5 point Likert scale from 'Strongly disagree' to 'Strongly agree')

22. The scenario of getting this voice call is relevant to a healthcare context
(5 point Likert scale from 'Strongly disagree' to 'Strongly agree')

23. **General questions about the game**

24. The scenarios in the game as a whole are believable in a healthcare context
(5 point Likert scale from 'Strongly disagree' to 'Strongly agree')

25. What could be improved to make the scenarios in the game more believable considering a healthcare context?
(Multi-line text field)

26. The scenarios in the game as a whole are relevant to a healthcare context
(5 point Likert scale from 'Strongly disagree' to 'Strongly agree')
27. What could be improved to make the scenarios in the game more relevant to a healthcare context?
(Multi-line text field)
28. If you have any other remarks you would like to share, you can leave them here
(Multi-line text field)

J Attribution of used assets final prototype

J.1 Sound effects

Buzzer sound was sourced and then edited from:

<https://freesound.org/s/271389/>

by 'discokingmusic' - License: Attribution 4.0

Edit made: trimmed a short fragment from the total recording

Bell ding was sourced from:

<https://freesound.org/s/611113/>

by '5ro4' - License: Creative Commons 0

Stamp sound was sourced from:

<https://freesound.org/s/347324/>

by 'newagesoup' - License: Attribution 4.0

Notification sound was sourced from:

<https://freesound.org/s/736267/>

by 'UNIVERSFIELD' - License: Attribution 4.0

J.2 Voice fragments for 2FA request

The 'incoming message' and the authentication request call were both generated using ElevenLabs: <https://elevenlabs.io/>.

J.3 3D models

The monitor, desk, and plant 3D models used in the game were created by Sven Sonneveld. The other 3D models (the office environment and stamps) were created by me, except for the Resonite default player avatar made by the Resonite team.

J.4 Graphics on recruitment flyers

VR headset icon

https://www.freepik.com/free-vector/realistic-virtual-reality-headset_11583265.htm

'Realistic virtual reality headset' Image by freepik

Flyer background image

https://www.freepik.com/free-vector/blue-futuristic-networking-technology_15082511.htm

'Blue futuristic networking technology' Image by rawpixel.com on Freepik