# Introduction

This is the reading guide for the portfolio of my internship in Semester 5 of my study FHICT. This will detail my process in this internship project as well as my conclusion and self-reflection.

This contains the most important information about the project; research findings etc.

# The assignment

This internship is for PIT, the Practoraat Interactieve Technologie in Tilburg. It is a collection of teachers from Onderwijsgroep Tilburg that research how to improve education, by making it more interesting with various technologies such as games and VR/AR etc. It is led by Geert-Jan van Ouwendorp.

My design challenge originates from one of those teachers. My stakeholder is Igor Burger, teacher Cyber-Security. His students will later be trained to become security experts and will have to work with various clients during their study. These clients will have to be instructed in cyber-security awareness. It is then my job to find a way to help his students to get the required knowledge in order to transfer it to these clients.

Igor had done some searching online already and had some ideas of his own. He wanted to have something akin to other cyber-security awareness trainings he found online, but these trainings were specific for larger companies and expensive, not suitable for a school environment.

After a talk with Igor it became clear that the solution would be in the form of a game. This is one of the ways PIT wants to try to improve teaching, and it would be easy to use in lessons.

Igor Burger has given me the following assignment:

*Create a game that will teach his students about cyber-security awareness, so that they can learn to in turn teach their clients about it.*

He has a few requirements at the start of the project:

* The game must teach about cyber-security awareness on its own; there should be no additional training required to play the game (so it is not a test of knowledge).
* The game must have the challenges easily adaptable; hackers find new ways to compromise computers constantly.
* The game should teach the player about the consequences of failure and include information on what to do if it happens in the real world.

# Project approach

I created a project plan to detail my approach of this internship. I decided to work in phases and divide these phases in sprints. Then after each sprint I would reflect and add a retrospective. I work with the Double Diamond method.

**Folder in zip: Project Plan Internship s5**

I also created a planning, folder in zip: Planning for internship

# Phase 0: Preliminary Research

From the assignment I defined the following research questions:

Research Questions:

* What type of game would be the best for teaching about cyber security awareness and what kind of technologies will be used here? Is it beneficial to use AR/VR or any other technology?

Methods used: Survey, Literature Study, Storytelling (user scenarios), Co-creation

* What kind of cyber security awareness trainings exist already, and what can be used from them?

Methods used: Literature Study

* What kind of topics does cyber security awareness encompass, and which of them will be in the game?

Methods used: Literature Study, Expert Interview

* How can I ensure that the players learn from the game?

Methods used: Storytelling, Ideation, Literature Study

As part of my preliminary research, I answered some of these questions to determine the type of game and get a grip on cyber-security awareness. The research to these questions is in the following documents:

**What kind of topics does cyber security awareness encompass, and which of them will be in the game?**

Research Document-cyber-security-awareness-topics.docx

in folder **Expert Interview CSA Internship s5** as well as a dev log in **Research on security awareness s5**

**What kind of cyber security awareness trainings exist already, and what can be used from them?**

Competitive Analysis cyber security awareness games.docx

in folder **Competitive Analysis CSA games Internship s5**

**What type of game would be the best for teaching about cyber security awareness and what kind of technologies will be used here? Is it beneficial to use AR/VR or any other technology?**

Looking at uses for AR and VR.docx

in folder **Research on AR and VR Internship s5**

This research can be concluded to the following:

* The game will be about the topics of Social Engineering and Phishing. These are the topics that users have the most control over in terms of own security, making these the topics Igor’s students will eventually have to teach to their clients.
* The information in the game should be given in a way that incorporates the game mechanics, in order for the player to remember it better. The cyber security trainings out there are indeed only for larger companies and not suitable for educational use.
* AR and VR are not beneficial in this project. VR is not accessible enough to use in a classroom context and AR is not applicable to phishing and social engineering.

From the context of the problem I gathered that the target audience is students from 20-30 years old. I did a target audience interview and made personas to use later in user scenarios.

Folders in zip: **Target Audience Interview Internship s5** and **Personas Internship s5**

## Retrospective phase 0

In this phase, I got a lot of insights on the topic of Cyber Security Awareness in general (the main dangers of social engineering and phishing), as well as some insights in the problem. Games that teach you about cyber security awareness are few and far between and other trainings cost a lot of money and are made for larger companies. Some things are still a bit unclear with the client’s needs at this point.

It is likely that AR and VR will not play a role in this project. The context does not fit for VR (must be playable anywhere) and e-mails are displayed on the screen normally, anyway.

# Phase 1: Design Challenge

## Design Challenge:

At the start of the sprint, I sat down with my stakeholder to talk about my findings and talk about what the real design challenge would be. He reiterated his requirements of the replayability and ease of changing/adding the challenges to the game.

The preliminary research combined with my conversation with the stakeholder led into the following design challenge:

Make a game for students of cyber security, from 20 to 30 years old, to teach them about cyber security awareness, specifically the topics of social engineering and phishing and how to recognize them, where the game has to be replayable in order to keep training the users and where it must provide feedback on what went wrong or right.

## How-Might-We questions:

How might we add replayability to the game, which is one of my client’s needs?

How might we add feedback in a way that the user remembers?

How might we translate the topics of social engineering and phishing into a game?

# Brainstorming

Based on these questions, I started with generating some game concepts to present to the stakeholder.

A close-up of several pink post-it notes

Description automatically generated

I sat down with my stakeholder to discuss these concepts, and we agreed on the concept of the job simulator game. This is because the mails could be easily adapted or new ones could be added, while there could be a degree of randomness in it so the players can keep practicing.

The hacker’s view game was also an interesting concept, however since the stakeholder wants to potentially use this for end-users of his students (which can have varying levels of computer skill) as well, it may be too complicated for them.

The multiplayer game was relatively similar to the job simulator game; the job simulator could be done in class, letting the students vote on whether or not to report a mail.

Lastly, the story-based game would not have enough replayability.

We discussed a MoSCoW for the requirements of the game and the project in general, using the preliminary research I had done. The result can be found in:

MOSCOW csa game.docx in folder **MOSCOW project s5**

**M - Must haves:**

-The game should be for PC and web-based. This allows the stakeholder to host it online and link to it on his personal site.

-The game should contain phishing mails. Mails could be good and bad, where there's enough of them that it feels different each time. There should be some way to point out that it’s phishing.

-There should be feedback on why the mail is phishing, such as the red flags that were there.

-There should be a scenario in the game.

-Disclaimer for educational and non-profit, to prevent any legal issues.

**S - Should haves:**

-Selecting red flags as a gameplay element

-Besides the mails, a section for phone messages.

**C - Could haves:**

-Dedicated multiplayer mode

-Making it easy for the stakeholder to add new mails to the game

**W - Won't haves:**

-AI integration for phone calls and phishing mails (generating new content)

## Retrospective sprint 1

This was a productive phase. Sitting down with the client and working out a MoSCoW allowed me to have a clear goal in mind going in the next phases. I can now start with designing the game based on the how-might-we questions and the concept I picked.

# Phase 2: Game Design

## Sprint 2

## 1-pager

Folder in zip: **One-pager CSA Game**

I started on a 1-page game design document based on the concept picked by me and the client. The decisions for the different aspects are the following:

Genre: Based on the concept, the genre is puzzle and simulation.

For the game summary, I started to brainstorm and look at various office jobs, in order to pick one to simulate. I found <https://www.quora.com/What-do-people-do-at-office-jobs-Like-they-cant-just-reply-to-emails-8-hours-a-day-right> which had some people share about their office jobs. This includes administration, making reports, copying documents and more.

Out of all of these, administration seems like the perfect job. It involves both mails and phone calls, so it can cover both social engineering and phishing.

For the game loop, I took inspiration from real life to make the game more realistic, which is something my client asked for. This means the following:

* Throughout the day, you receive mails on your computer. These mails can differ in how you need to act on them. I chose to add multiple ways of handling the mail, so that the player has to read the context of the mail to actually play correctly and not solely have to focus on the red flags. This paper confirms that people often fall for phishing because they can get lazy from the many mails. <https://lightbeamhealth.com/the-consequences-of-phishing-and-how-to-avoid-being-hooked/>, which is another reason to make the mails more diverse. Phishing mails play into the content of a mail according to Igor, so the gameplay should include this content as well.
* The days’ difficulty ramps up over time. This is to challenge the players so they can learn more by playing more. I found a theory about difficulty curves at <https://www.gamedeveloper.com/design/difficulty-curves> which I will make use of later.

Because of the realism and wanted scenario, I took a look at the different ways offices are represented in popular media. This should be a good starting point for my setting and artstyle, because it should be relatable for the player even though they may not have been in an office before.

In popular culture, office jobs are often depicted as boring or long-winded. To make the game relatable for realism I want to give this same feeling to the player without making them too bored. To make sure the player at least has something to do between mails, I will add some trinkets to the desk; I found myself that toying around with trinkets can help with boredom during work.

## 10-pager

Folder in zip: **Ten-pager CSA game**

I did research on the game Papers, Please by watching some videos on it and noting down interesting mechanics and their purpose. This game’s concept is similar to mine and this means that I could take inspiration from it.

Interesting mechanics from Papers, Please:

-Mechanics that give time pressure (the day is timed, you need enough salary to progress)

-Overarching story spread out over days (this makes the scenario feel more alive)

-Adding new tools over the days (this ramps up the difficulty)

-Instructions manual for reference (this teaches the player about new things)

The kinds of fun are Challenge (to make sure the players learn well from the game) and Fantasy (because of the scenario, you’re put in the shoes of an office worker and their job.)

This leads into the following aesthetics:

Pressure to work fast, hecticness, fear when losing (for challenge), relatable boredom (for fantasy) and understanding towards the hackers’ ways.

As per the relatable boredom aesthetic, I want to make the player feel like they’re not always busy, giving them some time to mess around until suddenly things get hectic, which is part of the difficulty curve, and makes the game more realistic and adds challenge. This will be the “rush hour” dynamic.

This does create moments where the player might not have anything to do. Therefore, I want to implement some trinkets for the player to use while they wait for the next e-mail or message. This fits with my client’s wish to make the game realistic in the sense of the world.

Because phishing often comes unexpectedly, I want to try having this in the game as well. To keep the player not completely focused on finding out if a mail is phishing or not, I want to make sure that there’s more options than just “accept” and “deny”. Papers, Please, a game similar to my concept, does focus on these two options, however it makes you check a lot of different data before you actually accept or deny there. Later in that game you also get more options. I want the player to think about the content of the mail instead of looking for the red flags each time.

For this reason, there will be different ways to handle mails, and selecting red flags will only be relevant once you click the report option.

Using the concept and MoSCoW, I came up with the following gameplay based on the dynamics. I translated this into the mechanics:

-You must answer messages, which can be on phone or in the mailbox. There will be different ways to handle them, based on the mail. This is to keep the player focused on the content of the mail.

-Messages have a certain chance to be phishing. If it is, you must use the report option and select the red flags.

-This happens each day. For every day that passes, the game gets harder, phishing mails get more difficult to detect and potentially new mechanics are added (for example, day 1 could start without the phone, you then get promoted and have to handle phone calls.)

-The client wanted to have feedback on phishing mails. If you handle a phishing email the wrong way, your computer will be compromised, and you will have to spend a portion of your day and money to fix it. It will detail what you missed.

The aesthetics also lead into the sound design:

The “first boredom, then hecticness” means that this should be reflected in the music; boring, calm music at first that soon turns hectic. The sounds themselves are then reminiscent of real life sounds to make it more realistic. It also leans into the pacing section.

The difficulty curve means that every day will add more and more difficulty, in the form of extra mechanics and harder to find mails. This was my justification for the day design.

For the story, I took a look at some other games. They often take inspiration from history or some societal issue. Since the game is about office work and hackers in the current western world, I added a hint of capitalism to the story.

## Retrospective sprint 2

Everything went well. I now have a clear GDD going forward, with the mechanics, dynamics and wanted aesthetics written down. Based off this, I can work on making prototypes to test my gameplay and see if the design needs some tweaks.

## Sprint 3

I created an office in Unity in order to be able to do prototypes with it.

Folder in zip: **Dev Log S5: Designing and implementing the Office**

Using an online service named Marvelapp, I created a prototype of my game, which I then playtested with a timer, to see if the time pressure helped the aesthetics. I asked questions afterward and also let the players choose words they associate with my game.

Folders in zip: **Prototype testing** and **Dev Log S5: Testing Prototypes**

Most of the wanted aesthetics were met, however the game doesn’t feel hectic enough and the following was missing:

* A way to be sure of something; one of the users did not know what a .bat file was.
* Players felt confused on if they did something right or wrong.
* One of my players pointed out some more red flags that I missed.

I then changed the following in the 10-pager based on my test results:

1. Added more info to the “player feedback” section (correct actions should have feedback too.)
2. Added a new mechanic called “Antivirus Scanner”, which you can use to check if something is suspicious but takes time to scan. This is because people were sometimes uncertain about certain red flags.
3. Added a section with all information about mail setup. (which parts can be red flags etc.)

Folder in zip: **Dev Log S5: Mail Design**

## Retrospective sprint 3

This sprint was over a little faster than planned. I could already start on script architecture and working in Unity at the end of the second prototype week. This is beneficial, because it gives me more coding time, while coding is by far the largest part of the project. The prototype gave me useful insights into the design of the project.

# Phase 3: Implementing into Unity

## Sprint 4

In this sprint I want to take extra care to look at the relation between the different scripts that will be in the project. My last (group) project was difficult because we did not do this; causing us to not properly divide tasks because we weren’t sure what script was going to do what.

I made a diagram of the different scripts and GameObjects, based on the mechanics detailed in the 10-pager, how they should work and communicate.

Folder in zip: **Dev Log S5: Script Architecture**

To make interactions with the items in the office possible, I looked into events. They are a way of running multiple functions every time you call the event, which works with the observer pattern. In this way, I made a script that invokes an event each time the button is clicked, which I can subscribe to when necessary.

Folder in zip: **Dev Log S5: Working with Unity events**

I then coded the mails in the game using Scriptable Objects. These have both a good and false version, as well as a phishing chance. This means that the game can check this mail and then based on chance, generate a random mail each time.

Folder in zip: **Dev Log S5: Mail Scriptable Object**

## Sprint 5

I made a proper design for the mailbox to put the mails in the game, inspired by the Office layout.

Folder in zip: **Dev Log S5: Mail Visuals**

This is because the office layout is a working design and is widely used. I then used UI buttons and a script to display the mail scriptable objects in the game, which displays all mails on the side and the selected mail next to it.

This sprint, I also had to present for my company. I created a presentation for this.

Folder in zip: **Pitches**

## Sprint 6

This sprint I worked on the mail interactions and making sure you could handle the mails a certain way.

Folder in zip: **Dev Log S5: Mail interactions** and **Dev Log S5: Office Navigation**

I then worked on the report function and ran a series of tests with fellow students, which can be found in:

Folder in zip: **Dev Log S5: Player Feedback in mails** and **Research s5: Usability test**

From this test, it turned out that the report function wasn’t clear enough. Therefore, I added a hover effect to anything you can report. Combined with a better tutorial it should be clear now.

During the test, I also found the following:

* There’s no way to check information such as contacts.
* The boss’ warning mails were hard to notice.
* Small visual things.

I took a good look at the different consequences that could happen when a mail is handled wrongly or when you click on a phishing mail.

Folder in zip: **Dev Log S5: Player Conscequences**

## Sprint 7

Due to some time restrictions, this sprint extended into the vacation.

At the start of the sprint I sat down with the stakeholder and created a phishing mail together with him. We found out that the way I did the mails made it inconsistent. Because the mail could be either phishing or not, some parts of the mail would look good while it was still phishing due to a different subject. Therefore, I will make some mails always be phishing and other mails always be correct mails. I also made a list of predetermined mails in a day, so that I could prepare a controlled test.

Folder in zip: **Dev Log S5: Target group test prep**

I ran a test with my intended target group; the stakeholder’s students, to see if the game could be used as an educational tool. The results of this were as follows:

Folder in zip: **Research S5: Target group test**

* The testees were able to explain phishing after I put them through the test. Although prior knowledge may be a factor, they told me they are more aware of the potential dangers of phishing mails, which was the point of the game.
* Testees still had some trouble with the feedback. The warning mail from the boss does not stand out enough and the players did not always know what do do with it. Potentially, a different way of giving this feedback is required.
* Testees understood the colour scheme of reporting a mail.
* The tutorial I added was completed well and taught the players how to play the game, but only if they managed to complete it in time. Otherwise, they would go straight onto the next mails that came in.
* There are still some bugs, one with the recolouring of selected red flags, and one where you could cancel the lock screen by clicking on one of the buttons.
* The contacts option was not visible at all. I should include this better in the tutorial.
* The players need more time to read the mails, at least at the start.
* The game needs to have some way of telling the story.

I implemented a dialogue system that serves as player feedback. It explains certain things to the player, such as tutorials or the red flags the player missed. I use dialogue here because it is an effective tool in many games to explain things to the player.

Folder in zip: **Dev Log S5: Dialogue System**

I also did a small test as a control; this allowed me to validate the dialogue system and notice some small mistakes, which I fixed afterwards.

Folder in zip: **Research S5: small-scale test**

From this test it also turned out that if all mails for the day were done, the players would have to sit around bored until the day was over. Therefore, I added a button to end the day, and a dialogue message to explain that all mails had been handled, so the player knows when to use it.

From earlier tests, I received the feedback that the story wasn’t entirely clear. I added a news site; each day your screen starts here to give you useful information on the day and explain the story.

Folder in zip: **Dev Log S5: News Site** and **Dev Log S5: Game tab manager**

Checking with the MOSCOW, the game is now done. I made some finishing touches; adding start/end screens, icons and an easter egg (players in the tests expected something to happen when clicking on a certain object, so I added an interaction there.).

I did a final small test to validate the previous changes. Folder in zip: **Internship S5 small-scale-test w17**

From this test, the only thing that came up were small visual changes and a need for a score screen. This has been a request from teachers at well during the target group test, so I will still add this.

I created a transfer document that describes the game, as well as how to install it and host it, and I added a guide on how to add days and mails. The client can use this guide to add any new mails to the game.

Folder in zip: **Transfer Document**

In case this project is continued, there is also some information about the game design document and code structure, as well as a section about the suggested features to be added.

Lastly, I came up with an assignment that my client can use to create more mails. He will be able to have his students complete this assignment and with the answer, create new mails for in the game.

Folders in zip: **Assignment to create mails S5** and **Dev Log: Using the target audience to generate mails**.

## Retrospective sprints 4-7

Over the course of these sprints I have built a nice game, implementing new techniques such as Scriptable Objects and Unity events, as well as using a more defined workflow in order to keep my code and scripts relatively organized and expandable. I have gone through multiple iterations in order to increase the game’s quality.

From the target group test it turns out that the game is indeed educational. I then took the time to improve the flow and quality of life of the game, adding missing things such as an end-day button and various UI elements.

# Conclusion and recommendation

We started out with the following design challenge:

*Make a game for students of cyber security, from 20 to 30 years old, to teach them about cyber security awareness, specifically the topics of social engineering and phishing and how to recognize them, where the game has to be replayable in order to keep training the users and where it must provide feedback on what went wrong or right.*

After going through the design process, making my GDDs, keeping in mind the target audience and goal of the game, I have made a game that fulfils the design challenge. This game has gone through iterations and has been tested on its educational value. The game is for the correct target group, teaches about social engineering and phishing and how you can recognize them, and has randomly generated mails, which allow for replayability. It provides feedback to the player in multiple visual ways; with colours, text, etc.

At this point, the game needs to have more content in the form of mails to randomly generate, as well as more days in general. But these can be easily added in the form of Scriptable Objects. I am currently planning to have the students themselves create more mails; in this way the current students can already learn about phishing and social engineering and contribute to the game. They would be some of the best to do this; they should learn this information anyways.

In all other aspects, the game is finished. The base game fulfils the design challenge and predefined requirements and could be used in a classroom.

I do however have a few recommendations:

1. Add sound design as detailed in the GDD. There is currently no music and sounds in the game and adding it would help with the aesthetics of the game.
2. Once again for aesthetics, add a mechanic with the phone that makes more use of it. Currently it only holds an address list, and adding gameplay to it could give the game the more hectic feeling.
3. There needs to be more after a day has ended. During the target group test, I ran the game by two teachers as well and they noted that they might want a stats screen at the end, showing you what you did wrong or not. Alternatively, there could be a proper lose condition; for example, if you get hacked three times you would have to restart. At least some way of telling the player how well they did overall. The shop could also be a good inclusion.
4. More interactivity with the trinkets. During my latest test I found that the player was waiting for new mails or the day to end. Therefore, it would be useful to add more to the trinkets in order to give the player something to do.
5. Mail storylines: To improve consistency throughout mails, there is an idea to group certain mails together and only send the next one if the last one has been answered.
6. Hint system: In an earlier test, some testers were unsure about some of the actions they were going to take. The idea is to add an antivirus scan, which would then tell you if a certain part of a mail is safe or not but would take some time to use, so that it has a drawback.
7. Improved visuals.

Thank you for reading!