Bauhaus-Universität Weimar

Social Engineering - The Adventure!
Final Report

Intisar Hasnain Faiyaz
124731
intisar.hasnain.faiyaz@uni-weimar.de

Christoph Peter Hein
125356
christoph.peter.hein@uni-weimar.de

Anastasia Koslova
125115
anastasia.koslova@uni-weimar.de

Deep Rajani
125907
deep.rajesh.rajani@uni-weimar.de

Emmelie Richter
123666
emmelie.richter@uni-weimar.de

Mareike Spies
125110
mareike.spies@uni-weimar.de

Linda Zobel
125821
linda.zobel@uni-weimar.de

Supervision:
Jun.-Prof. Dr. Jan Ehlers, Prof. Andreas Jakoby, Prof. Stefan Lucks

Winter Semester 2023/24

Contents

1 Introduction

In our modern time, social engineering is one of the most effective ways to obtain information about individuals and organisations. In its core, it exploits human nature with the aim to access data that one should not have access to. Even if someone has the strongest password in the world, an attacker using social engineering might still access their private information by playing on the person's humanity and vulnerabilities.

This report is a summary of the project "Social Engineering - The Adventure" that was driven by seven Bachelor and Master students as well as three supervisors. Over the course of a semester, the team was dedicated to exploring the techniques of social engineering while developing the prototype of a game in the end.

The goal of the game is to educate the average internet user on the dangers of social engineering and the techniques used by attackers to access someone's personal data. The game is designed such that the player takes on the role of the attacker, slowly uncovering a political scandal. The player is asked to gather information on parties involved such as companies and politicians. The story progresses until the scandal is revealed.

By providing a choice for different actions, players learn more about different social engineering techniques, making them more aware of its dangers and possibly spread awareness by sharing this knowledge with their social environment. This can be seen as an additional goal, extending and supporting employee education in the public and private sector on privacy and security measures, possibly outperforming other mediums such as educational videos.

For the prototype, the story, graphics and programming mini-games were implemented to make the game both educational and fun. At the current state, the story is developed until level 4. The game engine used for development is Ren'Py, and the code can be found on GitHub: `https://github.com/akoslova/social-engineering-game`.

The game is mainly story based with the player being able to choose actions to take next. Some of those options will definitely lead to the access of information, some won't and could perhaps lead to the player getting caught. This means that the game creates a tree of choices for the player to make with some branches leading to a positive and some to a negative outcome.

This prototype is not a fully developed game yet and needs expansion by future project groups. While some bugs and errors were already noticed and fixed, the game still needs to be thoroughly tested before it becomes fully playable. However, this stage of the prototype provides a decent basis for future development and improvement.

2 Social Engineering

Social engineering has two distinct meanings according to the dictionary. One is the use of centralized planning in an attempt to manage social change and regulate the future development and behaviour of a society, also called "mass social engineering". The second is the use of deception in order to induce a person to divulge private information or especially unwittingly provide unauthorized access to a computer system or network, therefore also known as "interpersonal social engineering". Nowadays a mixture of the two can be observed, called "mass-personal social engineering", which uses social media and large data bases to manipulate individuals on societal scales (cf. Hatfield, 2018; Gehl & Lawson, 2022).

The social engineering type, which is focused and touched on in this report, is the form of attacking personal security by infiltrating PCs and networks. There are several techniques used in the present time which will be introduced in this chapter by looking at available papers and sources describing prevention techniques and specific cases of SE being practised in the past.

Social Engineering in the Past

"Social engineering" as we understand it today within its cybersecurity context began with the "phone phreaking" phenomenon of the late 1950's through the early 1970's, which predated the creation of ARPANET, the precursor of the modern internet (Hatfield, 2019). Phone breakers used their technological knowledge to hijack the telephone system for their own purposes, whether that be to avoid fees, connect to foreign conference calls, or gain access to areas of the network considered off-limits (Rosenbaum, 1971). To do so, they also needed information from the Bell telephone company. John Draper describes in an interview the actions he and his friend Dennis Dan Teresi would take. "The ability of going in and talking to people on the inside of the phone company. . . making them believe you were working for the phone company" (Lee, 2001) is what they named social engineering. By 1990, the technical terrain on which computer hackers operated had become so complex that information gathering through manipulation and impersonation or "bullshitting" to the anonymous authors of 2600 and Phrack became the primary goal of social engineering attacks (cf. Hatfield, 2018).

Today, computer network security maintains enough robustness and sometimes even automated vigilance that experienced hackers no longer seek to replace social engineering, but rather view it as an integral part of any successful hacker's toolkit (Mitnick & Simon, 2002).

Context and Techniques

In our attempts to program and provide an educational experience in the form of a decision-based game, confronting the player with different scenarios and techniques practised in social engineering, numerous sources were used to acquire a general knowledge of these situations and methods. Those sources ranged from governmental agencies such as the Bundesamt für Sicherheit in der Informationstechnik (BSI) and the European Union Agency for Cybersecurity (ENISA) to the private sector including private cybersecurity sofware companies. Most of the sources on the internet like the BSI describe social engineering as the manipulation of individuals with the objective to gain unauthorized access to systems, data or physical locations by exploiting human psychology rather than technical hacking methods (BSI, 2024).

Social engineering, as mentioned before, is not a phenomenon of the information age, but with the advances in technology and the internet, the data that can be found has now a higher value and importance and there are many more ways to approach the target. Furthermore, digital communication gives the attacker easier access and has less potential for failure, since the charade does not have to be carried out in person and therefore fewer senses need to be conquered.

Moreover, private and professional social networks offer con artists an easy opportunity to gather and link a wide variety of background information about people or employees of a company which can be used then in an attack. The gold mine everyone is hunting for are bank information and passwords, which provide a way to access the individual's wealth and provide possibly the highest profit for the attacker. To trick people into breaking security practises and revealing information the attacker uses psychological manipulation. Human characteristics such as a willingness to help others, trust, fear, or respect for authority are exploited to manipulate the target into giving out crucial information. These human weaknesses are put into principles, creating Cialdinis set of 6 principles published in his book *"Influence: The Psychology of Persuasion"* in 1984, which can be used to manipulate the human being:

- **Social Proof:** People tend to do what they see other people doing.
- **Reciprocity:** People in general often believe that if someone has done something nice for them, they owe it to that person to do something nice back.
- **Authority:** People tend to obey authority figures, even if they disagree with them and even if they think what they're being asked to do is wrong.
- **Likeability:** People are generally more persuaded by people they like than by others.

- **Consistency and Commitment:** When people make a commitment to achieve a goal and internalize that commitment, it becomes part of their self-image, and they're likely to try.
- **Scarcity:** If people think a particular resource is scarce, regardless of whether it is, they will want it even if they don't need it.

The attacker utilizes these principles in different forms and techniques through the process and the steps of social engineering. Oftentimes, the attacker claims a false identity, such as a technician or employee of a particular company, in order to pretend some kind of power or legitimacy of their actions. In this role the perpetrator gives the victim the impression of increasing the security or solving an issue which however results in the total opposite.

Social engineering can be described having a life cycle that is made up of investigation, a hook, the play and an exit. In the investigation process, attackers identify possible entry points and weaknesses based on personal information found on the internet or on social media. Within the chosen method, they engage the target and spin a story, using the information found to hook the other person on an interest or problem they have. This initial interaction is designed to build trust and allow the attacker to take control as the interaction progresses. The play then provides the stimulus for a subsequent action that breaks a security practice, reveals information, or grants access. An example for these plays is: Hooking an individual on their interest on cars and sending them a tailored message with a link to a specific and desired car which however is a bait and allows consequently unauthorized access to the computer for the attacker. With the exit, the attacker tries to remove traces and cover their tracks by ending the charade in a natural way, trying not to arouse suspicion or alarm the victim and reveal the security breach.

There are several techniques to carry out the attack. One well-known and widely used method is **phishing** or **spear phishing** (targeted phishing attacks towards a specific individual or organization). These are fraudulent emails that mimic legitimate sources in order to steal sensitive information. In a recent case, a teenager with an Amazon Fire TV Stick sent these emails to employees of the developer studio Rockstar and, through their incautiousness, managed to gain access to their Slack groups with all the files and prototypes of the game (Dymoke, 2022). With these in hand, he tried to blackmail the company and later leaked all this information on Reddit, becoming a historic data leak and precedent of SE.

Vishing (**Voice phishing**) is a phone-based scam using impersonations of colleagues, technical support, police or other figures of authority to request an immediate access or action or personal information.

Smishing is a similar technique utilizing SMS sent to the target.

Baiting is offering something alluring and providing easy access like free software or private pictures on a USB stick to prompt an action of the target and installing malware or opening the opportunity to steal private credentials.

Pretexting involves creating a believable story to justify requests for information or physical access. This can be a fake doctor's call to a secretary pretending to need some vital information from a patient that should have been received by now, and through the pressure of time and the possibility of consequences if a mistake is made, gaining access to this highly sensitive information.

Tailgating is a method to acquire physical access to areas which have security measures in place. The perpetrator utilizes tactics like acting as a delivery person, distractions or waiting by the doors to slip in when someone leaves to enter these restricted areas.

Impersonation/in particular CEO scam is taking the authority of the CEO and demanding the release of budgets or placing purchasing orders in order to skim money of the company. This can be done in emails or messages, but a recent occurrence saw the attackers utilizing deep fakes to hold meetings with staff in Microsoft teams and giving the order to transfer money to non-existing business partners (Chen & Magramo, 2024).

Social media impersonation is another modern development where attackers impersonate famous individuals or entities on social media, claiming to be the authors of the accounts and soliciting investment from followers through direct messaging.

Dumpster diving is the practice of sifting through garbage to find valuable information that has not been properly disposed of, but it can also be seen as rummaging through old hardware in an attempt to recover information that has been intentionally deleted.

Quid pro quo (something for something) involves a request for information in exchange for a compensation. This may be access to a discount or solving a victim's problem.

Scareware is the method to cause false alarms regarding the infection of a personal computer with malware to prompt the user to install software which is actually the malware.

Water holing and **tampering** are merging techniques from social engineering and hacking. While tampering means manipulating data in transit or as it resides on systems of targets, water holing is to capitalize on the trust of people in specific parties and websites and breach them to insert malicious links or malware.

Honeytrap is when an attacker poses as an attractive person to engage victims into a false relationships and gain their trust.

When conducting research on the topic of social engineering, the team was divided into three groups, each studying different resources about social engineering. The results were shared with each other afterwards with the goal to increase knowledge on social engineering. One group was reading the German book "Ein Falscher Klick" by Eva Wolfangel (2022). The second group was summarising the book "Social Engineering - How Crowdmasters, Phreaks, Hackers and Trolls Created a New Form of Manipulative Communication" by Robert W. Gehl and Sean T. Lawson (2022). And the last group researched the history and techniques of social engineering on the internet, as well as government and corporate cybersecurity information sites.

As it is seen, the amount and quality of techniques for social engineering have evolved over the last few years with the progress in technology. Techniques such as dumpster diving were most likely present over hundreds of years already and proved perhaps to be the most efficient way to gain information about someone in the past. With the rise of the internet and later social media, the methods of social engineering expanded and developed further, allowing the possibilities of contacting anyone on the internet for information. Thus, attackers have now even more efficient methods to access unauthorised information. Hence, to protect oneself, people need to be aware of the dangers and techniques in social engineering now more than ever.

3 Project Structure

In order to successfully work on the project, the first step was to choose a team structure and a game engine. The division of tasks and responsibilities as well as the three main options for a game engine are discussed in the following sections.

3.1 Team Structure

The team of seven students was divided into three departments for the implementation of the game: Story, Design and Programming. Each team was focusing on their specific tasks while collaborating with the others when needed. Simultaneously working on the same levels was not always possible as the story needed to be set before graphics could be created and code implemented. This way, the story team had to be slightly ahead of the other departments in order to allow for a smooth implementation.

The story team's core task was to write the script for the game. They researched thoroughly techniques on social engineering that they could include in the game to educate the player. Additionally, they had to develop the choices for the player to choose from in order to allow for different outcomes of the game. The story department's final task after each level was to transfer the script into the Ren'Py files as well as playtesting to a certain level to make sure the story and choices are comprehensive.

The design department's activities were split into two main topics: creating visuals for the background scenes and the characters on one hand and creating the user interface and and visual mini-game elements on the other. The visuals were created using artificial intelligence (Scenario) and follow a pre-agreed overall theme. In the end, the design team was also responsible for placing the visuals into the game files where they were needed. For the user interface and everything that involves texts, Photoshop and a web-based Photoshop clone (Photopea) were used.

The programming team's tasks were to supervise the code implementation, fixing errors when needed and implementing story design choices, for example not being able to click a choice twice. Furthermore, the programming team implemented mini-games and further design elements that were embedded into the story. The player had to for example write their name, guess a password or piece a letter back together. A journal was also created that collects all the information revealed throughout the game.

3.2 Game Engine

First of all, choosing the right game engine for the game was essential for a smooth development and effective completion of the project's goals. When choosing a game engine, three options were considered: Ren'Py, Twine and

GDevelop. The team was divided into three groups investigating the advantages and disadvantages while also developing a small prototype, showing what the game would look like.

Ren'Py

For Ren'Py, one of the main advantages was that it was quite easy to work with and simple to understand. When installing Ren'Py, there was a whole tutorial section, explaining how the game engine works and what story elements can be implemented. Also, there exists a thorough documentation on Ren'Py on the internet that proved to be very helpful. Furthermore, this game engine has already all basics for a game covered such as the saving mode while allowing for many elements that could be included such as audio files and mini-games. Its underlying programming language is Python, meaning that the game could even be expanded through new code. With that, it was also possible to create a git repository to allow collaboration between team members. The only disadvantage that was noticed was the lack of overview and structure in the overall game files. There was no tree, indicating how the story develops, and the amount of code can become overwhelming and difficult to keep track of.

Twine

Twine delivers simple visual creation of stories without any setup needed. It is an open-source tool used to create non-linear stories and can be used either in a browser or in a desktop version. The elements containing story segments are displayed as visual nodes (see figure 1) and can be easily organized. The story can be written without any code or extended with variables, game states, images, CSS and JavaScript. The export format being HTML makes it very flexible.

Within Twine, there are different frameworks called "story formats" based on HTML and JavaScript. The most popular ones are well documented and have an active community. One story format would have to be chosen in the beginning, as they all have different functionality and features. One disadvantage is that Twine does not support collaboration. The use of a versioning tool would be necessary. But as the files are simple HTML-files, it would be easy to merge changes.

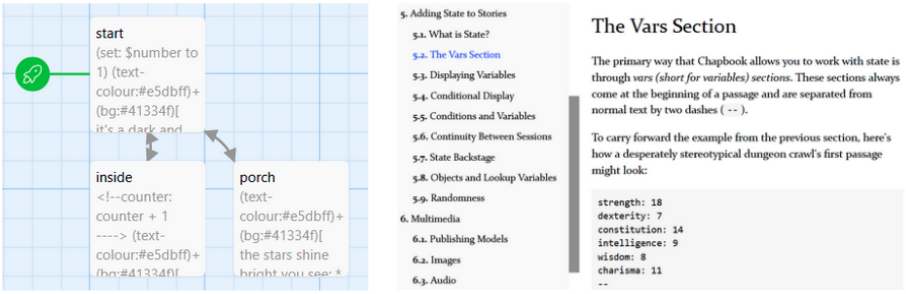


Figure 1: Nodes in Twine (left), documentation on the use of variables (right). Source: Own screenshot.

GDevelop

GDevelop was chosen by the third group due to its features and advantages.

Advantages:

- Accessibility: GDevelop has a user-friendly interface, making it accessible even to people with little programming knowledge.
- Versatility: The engine supports a variety of platforms, including Windows, macOS, Linux, Android and HTML5, making it accessible to the target audience.
- Visual Programming: GDevelop's drag-and-drop interface and WYSIWYG facilitates rapid prototyping and iteration, allowing to efficiently test and implement various game aspects.
- GDevelop has a vibrant community that provides several tools, tutorials and extensions to help improve the development process.

Disadvantages:

- Complexity Limitations: While GDevelop's visual scripting approach is adequate for simple game concepts, it may limit the implementation of more sophisticated features or interactions.
- Customization Limitations: Because of the engine's established templates and behaviors, it may not be possible to fully alter certain components of the game, potentially limiting creative freedom.
- Collaboration: While Gdevelop has online collaborating tools, it is not that fluent and robust like GitHub repositories, making it a challenge to work on a game as a team and needs further extra training for future collaborators.

Although GDevelop and Twine each have their own specialties and benefits, it was ultimately decided to use Ren'Py as the game engine. The main arguments for it were the scripting flexibility, visual novel expertise and compatibility with the project objectives. Ren'Py offers powerful capabilities like branching narratives and character management that are specifically matched to the project's needs. It was also important to allow for smooth collaboration and a flexibility in the programming part which Ren'Py both offered through GitHub and Python.

3.3 Gained Experience & Lessons Learned

Story

There were challenges in creating the stories. The integration of complex, technical knowledge into readable and captivating stories has been the biggest task. Therefore, it was very useful to get an overview of relevant media such as movies and other games that use social engineering techniques in order to understand the concept of integrating them into a working story. Examples that can be mentioned here are scenes from Who AM I, Hacker and Hannibal Lecter, which provided a good impression of how these scenes could be integrated into the game and how they could be formulated.

Iterations and feedback were necessary to strike a balance between entertainment value and educational depth. By dividing the tasks, there was the challenge of making the pieces work together in a meaningful way. This required additional meetings and discussions so that options and information found earlier in the level could be used by the player in a meaningful and interesting way later on. It was also debated how to educate people about social engineering in a way that is instructive without unintentionally encouraging abuse.

The research for the game was never really complete, as it was needed to ensure that the scenarios reflected the latest strategies and remained relevant, requiring the team to keep up with the ever-changing world of cyber threats. To portray real scenarios and attacks, everyone added to this vision with screenshots of real attacks or stories heard to make this game rich in variety and an actual representation of real world activities. These difficulties, however, only served to strengthen the game that would be both fun to play and an important weapon in the fight against social engineering.

Division of Tasks

In the beginning, there were some communication issues between the departments as it was not completely clear who is responsible for what. For example, the design team created the backgrounds and characters but it was not discussed whether they or the programming would place the designs into the right part of

the story. But after discussing all of those misunderstandings, a clear working structure was established.

There was also the alternative that the team could have been divided into groups that would focus on one level each. However, it was decided against this method as there was the concern that the levels would be incoherent. Hence, throughout the implementation, each department was responsible for their tasks through all levels, gradually moving from level to level. All in all, it was proven to be successful as the story, design and programming parts are all coherent.

It also needs to be mentioned that as expected, not all teams could work perfectly parallel. The story team needed to be the first step in the development which means they needed to work ahead in order for the other teams to provide work. They were responsible for explaining the design team what visuals they needed and discussing possible mini-games with the programming team. Hence, the programming and design team were always working after the story team provided their material. For the future, it is important to be aware of this as the story team needs reliable and driven team members for a smooth implementation.

Ren'Py

All in all, the team was satisfied with the use of Ren'Py. The programming team was able to implement the mini-games using Ren'Py functionalities and Python code. There was a lot of documentation and examplary mini-games on the Internet which was very helpful in the implementation. The implementation of the script and visuals were also pretty straightforward and easy.

However, one disadvantage as already known before was the fact that there was no build-in mind map to keep track of the different paths diverging in the choices. The story team initially wrote the script into a word document before moving it into the Ren'Py files. Keeping track of all paths and the logic in the story therefore proved to be very difficult. The only way to reduce logical errors was to play through the whole game which ended up being time-consuming.

It is recommended for the future to consider implementing some external mind map such as in Miro or putting the text into Twine to test the game flow without having to code anything. It would mean extra effort but at the end, it could help tremendously to reduce logical errors without needing to play through the whole game.

4 Implementation and Game Design

To provide an overview over the technical implementation, this section explains how the game was set up, what the story plot entails, how social engineering techniques were integrated into the story, how the code is structured and which other tools apart from the engine were used and why.

4.1 Game Set Up

For the game, a git repository on GitHub was created to allow for collaboration: `https://github.com/akoslova/social-engineering-game`. The next project team is encouraged to clone the repository to one of the new team members' git profiles such that the addition of new collaborators and further commits will be handled smoother.

A developer for the game should first install the game engine Ren'Py on their device from the official website `https://www.renpy.org/latest.html`. After having installed it, there should be a folder called '`renpy`' in the device's directory. In this folder, it is possible to clone this git repository, meaning that the folder containing the repository needs to be placed into the "`renpy`" folder.

If someone would like to clone the repository, then they need to open their terminal, go to the '`renpy`' folder and enter the following command:

```
git clone
https://github.com/akoslova/social-engineering-game
```

Then, this team member needs to create a new git repository in their git profile with a title like "social-engineering-game-2.0". After, they need to set the remote URL of the cloned repository to the URL of the new git repository. For this, the following command serves as an input into the terminal (with YOU being the new GitHub profile name):

```
git remote set-url origin
https://github.com/YOU/social-engineering-game-2.0
```

It is possible to check if the local repositoy is now connected with the repository on GitHub by inserting the following command:

```
git remote -v
```

This all should only be done by one person because all other team members will be added as collaborators. A collaborator needs to be added by the team member that cloned the git repository. Then, a collaborator needs to clone the new git repository.

```
git clone
https://github.com/YOU/social-engineering-game-2.0
```

After that, the collaborator should be able to have the repository locally and to commit changes. For the development, all team members need a code environment that supports Python such as Visual Studio Code. The benefit of Visual Studio Code is that it also has an extension called `"Ren'Py Languages"` that can be installed. This tool helps when writing Ren'Py code.

Furthermore, it is advised to install the `GitHub Desktop` app on the development device. This app is useful for tracking changes in all files and supports easy committing and pushing changes to the git repository.

In order to start the game for development purposes, the Ren'Py application (executable file in the `"renpy"` folder) needs to be opened. Now, the social engineering game should be appearing the same way as the preinstalled tutorial does. When choosing the social engineering game, the landing page of the social engineering game should open, and the player can start the game.

4.2 Game Structure and Elements

The game is divided into several levels, in which various social engineering techniques are used. Each level increases in difficulty. In each level there are several ways to successfully complete the level. However, there are also points in the game where the player can no longer progress, because the wrong options have been chosen. To make the game less frustrating, there are several checkpoints in each level to which the player returns, so that it is not necessary to play the whole level again. The aim was to keep the story as entertaining and exciting as possible, so that the player remains engaged and wants to know what happens next.

A journal was implemented that can be accessed throughout the whole game. On one hand, there is the knowledge tab that collects the information gathered throughout the game. On the other hand, there is the people tab that collects information about a person the player is meeting, including a picture, the name and the profession. The knowledge tab will add more pages after five pieces of information so that the text won't overflow. Furthermore, the journal contains a sticky note with the goal that the player currently pursues. The goal is updated throughout the game.

The map that occurs occasionally throughout the game is a visualisation of where the player currently is in space. It asks the player to go for example to the café where the only highlighted and clickable place on the map is exactly the café. It aims at helping the player to follow the story better and have a better imagination on where they are at the game. The map is implemented for the tutorial and level 1 but it still needs to be added at the right places in the other

levels. Whenever the player changes location, it would be wise to show the map.

Both tools were added to increase the level of interactivity and diversity of the game. The ultimate goal is to have an interesting and fun game with different elements. More ideas and tools can be discussed in the future.

4.3 Story

Currently, there are a tutorial and three levels that are fully fleshed out with dialogue options and various choices. The fourth level has a rough structure but has not yet been completed.

In the tutorial, the player is introduced to their workplace at TastyFoods and their position as a penetration tester. Soon they find a suspicious document on a PC they had just accessed, which sets the plot in motion. After consulting with a close friend who also works as a news reporter, the player begins their mission to uncover the scandal and mischief of a group they found hints of in the secret file. To shed light on these activities, the player works closely with the reporter.

In the first level, the player's goal is to infiltrate the construction company CORE, which seems to be involved in illegal rain forest clearing under the guise of a construction company and gather evidence. The player will investigate the outside of the building and the surrounding area, eavesdropping on conversations, using impersonation tactics in confrontations, and trying to find a way in. If the investigation is successful, the player will enter the building the next day with an intact disguise. While maneuvering through the offices and other areas, the player will again have to use different tactics to stay hidden and unnoticed while gathering information on where to find incriminating documents. This leads them to a computer room where they can find the desired information after solving the password puzzle. The player completes the level by leaving the building without being caught. With information that a senator has been implicated based on photographs and a ship manifest showing the delivery of certain heavy machinery to a vast area, the player again consults their accomplice, which leads to the action in level two.

The second level sees the player first investigate the depicted senator and the location of his office with a typical internet research. In the next part, however, they get their hands dirty to find documents and other useful information in the trash that reveal the senator's involvement. The player makes plans with their accomplice to attend the event after they found an invitation to a charity event with a hint that there will be a secret meeting taking place at the event location. The plan again involves using disguises or manipulating people to get in. Planning to record or eavesdrop on the secret meeting between those involved in TastyFood's and CORE's activities, the player places a recording device in the room. After successfully retrieving the recorder, the level ends

with the player listening to the recorded conversation, revealing the plan to hire a group of mercenaries to protect the ongoing operation from strikes and violent resistance.

In the third level, the player must target the Crimson Group, which employs the aforementioned mercenaries, a small group of friends who served together in a regiment. Using a variety of social engineering techniques, the player must find evidence of their atrocities, using phone calls, WiFi traps, and phishing emails to gain access to their private computers and cloud storage. If successful, the player will find body cam footage of violent attacks on workers and locals, as well as the exact location where these illegal activities are taking place. With this strong evidence, the revelation comes close to being a news story. However, the head of the operation and the background of the senator's involvement are still in the dark. Therefore, in level four the player has to build deep fakes from voice and face recordings. With these in hand, the player gets into a video conference to get incriminating material on the head of this operation, who is the son of their boss from TastyFood, trying to build an empire in the background with illegal means. The story ends with the player deciding whether to publish the story or take the hush money and leave the country.

4.4 Integration of Social Engineering Techniques

Social engineering techniques are very versatile, but all have the goal of finding and exploiting human vulnerabilities. An important aim of the game was to reflect the diversity and power of the different techniques. To make the game realistic and credible, the techniques were always selected to suit the situation. The following techniques are integrated into the game.

Tutorial level

Phishing: In the tutorial, the player, who has been hired by their company as a penetration tester, is given their first training task: to send a phishing email to their colleague Frank. There are two different emails to choose from. One with fashion advertising and one with a funny cat meme. As the player has previously learned, Frank is a cat lover, so the cat meme email is successful (see figure 2).

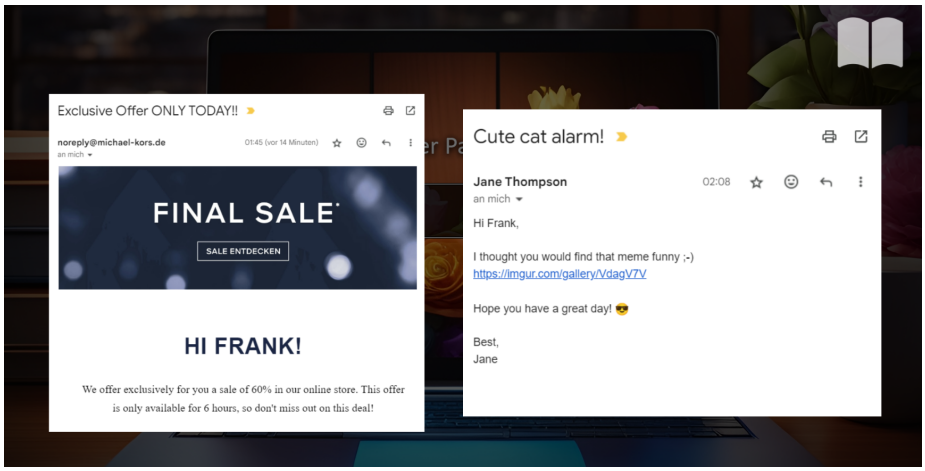


Figure 2: Example of a phishing technique task. The player has to select the correct email in order to make the target click on the link. Source: Own screenshot.

Level 1

Vishing: In the scene, the player calls a high-ranking executive on the phone and has the options to pretend to be IT support, a colleague or the CEO. Since they use an internal number, the executive thinks he is talking to a colleague and tells them secret information (see figure 3).

Tailgaiting: Furthermore, the technique tailgaiting has been integrated into the game. In level 1, the player has to find a way out of the company building without getting caught. Therefore they blend in with a group of employees to pass the security gate at the exit (see figure 4).

Pretexting/Impersonation: The method pretexting is used in numerous parts of the game. The player often needs to create a fabricated scenario to obtain information from a target. This also involves impersonating someone such as being part of the kitchen staff or calling an employee as a person in authority. In a scene from the first level, the player can choose to leave the building through the canteen exit. To prevent them self from being noticed, they pretend to be part of the kitchen team. (see figure 4).

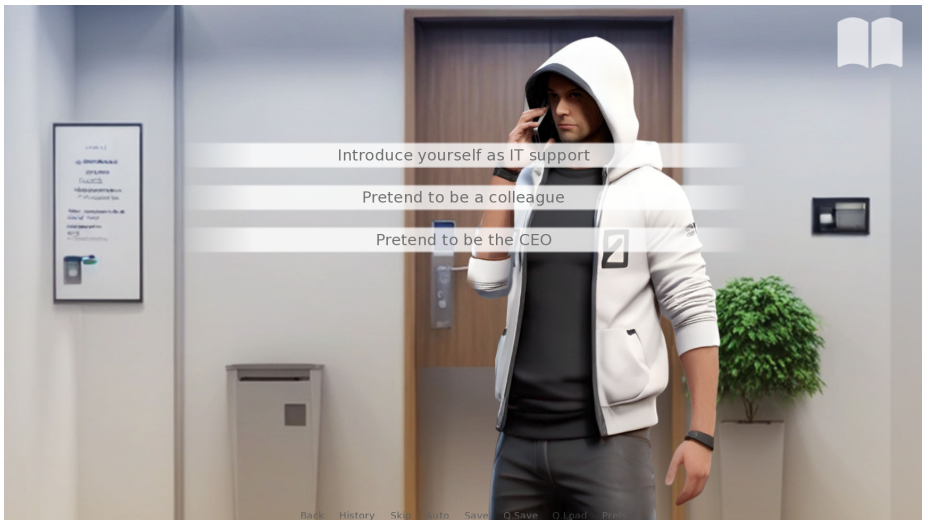


Figure 3: The player uses the vishing method by calling the target on the phone. Source: Own screenshot.

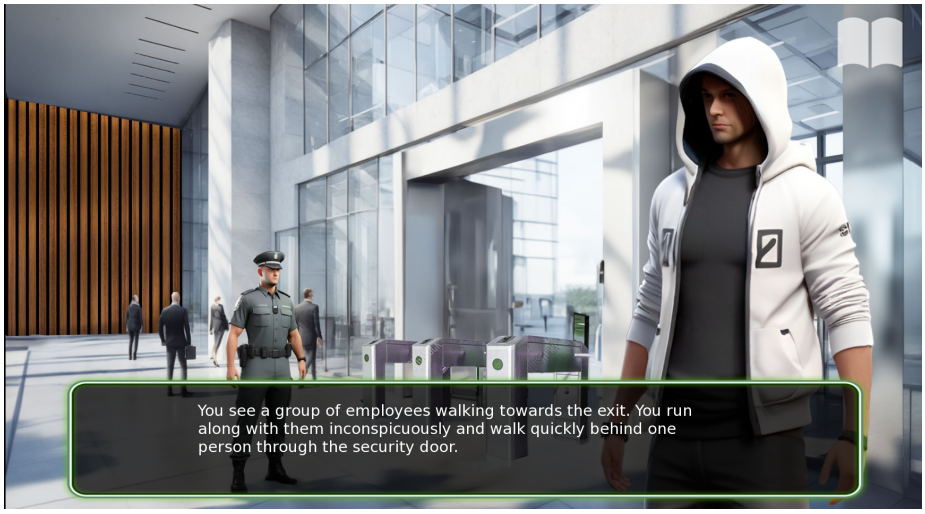


Figure 4: Tailgaiting: The player blends in with a group of employees to sneak through the exit with them. Source: Own screenshot.

Figure 5: To avoid attracting attention when using the canteen exit, the player disguises themselves as one of the kitchen staff. Source: Own screenshot.

Level 2

Dumpster Diving: The common technique dumpster diving is also an integral part of the game. In level 2, the player first searches the internet for information on Google and Instagram. With their research they find out the location of the senator's office. Then, in the next scene, they search a dumpster outside the office for valuable documents or information (see figure 6).

Baiting: Baiting is used when the player finds a stray cat causing a commotion near the dumpsters. The cat was making noise so to avoid unwanted attention, the player offers a snack to the cat. The snack acts as the "bait", leveraging the cat's immediate desire for food to manipulate its behavior for the player's benefit (see figure 7).

Quid Pro Quo: The quid pro quo happens between the player and Cathy, the journalist. Cathy provides the player with information and suggests plans such as stealing catering clothes for disguise that enable the player to access restricted areas and gather evidence. In return, the player conducts the groundwork, gathering evidence and information that Cathy needs for her investigative story. This exchange of services — Cathy's planning and the player's investigative efforts — illustrates a quid pro quo relationship, where each party offers something the other needs, establishing a mutually beneficial arrangement (see figure 8).

Figure 6: The player goes dumpster diving in order to find relevant information for his attack. Source: Own screenshot.

Figure 7: The player offers a snack to the cat, so that the cat remains silent and does not make any noise. Source: Own screenshot.

Figure 8: The player is talking on the phone with Cathy (reporter). The player provides an investigative story to Cathy and Cathy in return helps the player in stealing catering clothes so that the player can enter the charity event. Source: Own screenshot.

Level 3

Spear-Phishing / Baiting: In level 3, the player sends a phishing email to all mercenaries in the Crimson Group. This entices them with an offer for life insurance. One of the mercenaries, who has a family with children, falls for it. He clicks on the infected link and thus gives the player access to his computer.

Smishing: Used in a sequence where the player first contacts a mercenary by phone and then, after successfully spinning the story of an emergency, sends him an SMS with an infected link. This then allows the player to locate the phone in an area of the rainforest, pinpointing the location of the illegal operation.

Evil Twin: In one scene of level 3, the player follows a mercenary into a hotel where they clone a public access WiFi point. After the victim logs into the fake WiFi, the player can track the victim's activity and find more evidence of illegal activities.

4.5 Structure of Code

Written in Ren'Py, there were some present files when creating the game such as "screens.rpy". In the main space, all script files with each level written in one file were added manually. Additionally, the "custom_screens.rpy" and "inventory.rpy" were added to implement the journal for the player to access throughout the whole game.

The file "script.rpy" is the starting point of the game and lets the player choose between levels. The label "start" is always the starting point for the player in Ren'Py games. Right now, all levels are unlocked because the game is still in development. For locking the games, remove the input boolean True in the level declaration in the file "script.rpy". The default value should be False. At the end after each level, the boolean value needs to be changed to True. This still needs to be implemented in the end when the game is fully developed.

All levels need to include the file "inventory.rpy" and the previous level files so the information collected from before does not get lost. If the unlocked boolean is changed and the player finished playing one level, a new level should be unlocked and the player will return to the level selection screen. Ren'Py has a built in save functionality so the player should easily save their progress any time.

Python code can be easily embedded into the Ren'Py code by using the key word "python" or "$" if it is only one line of code. In the game, it is used for creating classes such as the level class or Python specific functionalities such as the input function.

All background and character images by the design team can be found in the folder "images". The visuals for the mini-games can be found in the "gui" folder such as for the phishing email and invitation letter game. Background images have start with "bg" whereas all characters immediately contain their name.

In the end, in Ren'Py, it is possible to build distributions, containing an executable for the preferred operating system. Then, the game should be possible to be played without having Ren'Py or Python installed.

4.6 Tools

AI Tools

For the game arts, primarily artificial intelligence (AI) tools were used that harness the power of Stable Diffusion 1.5 and SDXL. Initially, local Stable Diffusion clients like Automatic1111 and NMKD were tried but they had a major

drawback of limiting how many LORAs or checkpoint models (anime style, 3D style, painting style) are possible to use, as each of these model files can take 7-12GB of storage space for 1 style only.

Checkpoint models are basically large trained data sets and LORAs can be paired on top at various strengths to combine the base models with a slight style variation (for example LORAs that are specifically trained on just 'hands' can be paired with a base model for cartoons to give them more accurate hands). As consistent and anatomically correct AI art is all about trial and error, and getting the intended results, different styles and versions were tried out, filling up the storage memory and putting tremendous stress on the GPU for each generations. The best solution would be online services like MidJourney but that comes with a price-tag for a semester-long project.

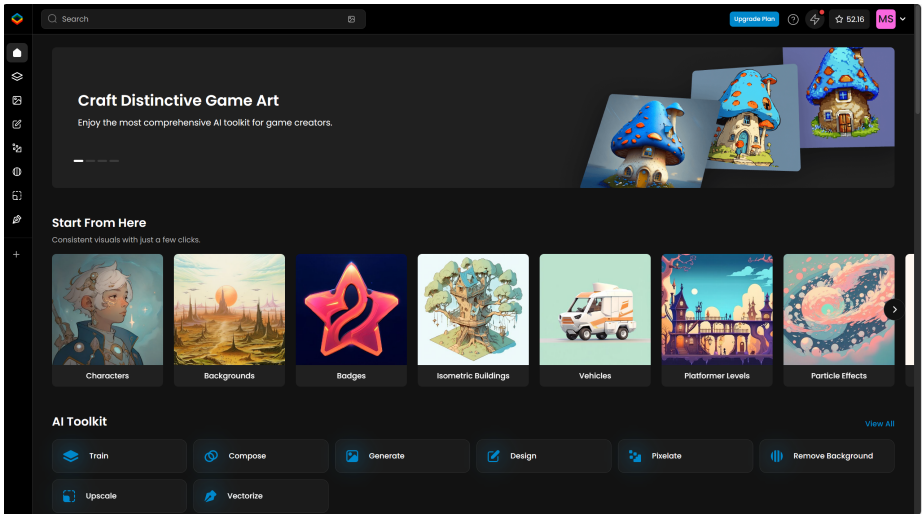


Figure 9: Welcome page inside Scenario.app dashboard. Source: Own screenshot.

But then, a completely free online AI art generator named Scenario.app was found that boasted a huge library of styles to choose from and all the generation was on their cloud server, putting PCs to rest. (As of 25.03.2024, Scenario.app is no longer completely free and only allows limited free generations with the free account, then requires subscription or credit refilling). It was as simple as navigating to the library of trained models from the sidebar, choose one model, give intended ratio and settings and prompt and hit generate.

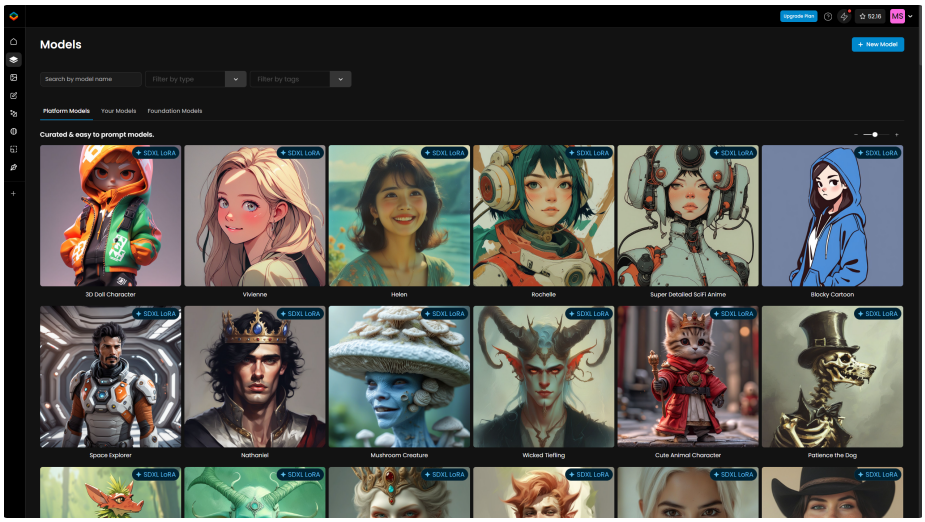


Figure 10: Vast library of models to choose from. Source: Own screenshot.

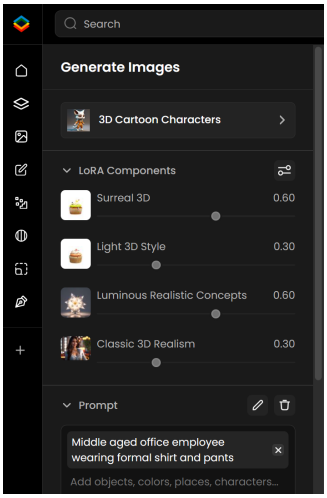


Figure 11: LORAs/styles stacking in Scenario. Source: Own screenshot.

The free version had a wait time after extensive use, but it can generate 4 images at once and was enough to try out hundreds of styles over a short period of time. For the images, simple prompts like "middle aged office employee wearing formal shirt and pants" were used to prototype with creative freedom, and in case of specific looks for the central characters, further details were needed in form of in-depth prompts on their appearances, along with negative prompts which tells the AI what aspects to stay away from. For the character designs, it was initially decided to try three styles: 2D anime, 3D cartoon, or pixel art. Finally, it was decided on the 3D render style and used a style in Scenario which uses 4 LORAS stacked on top of SDXL model.

Scenario.app also allows image-to-image generations which means that it was possible to give a reference image and adjust the guidance scale for it to generate an intended image following that. For collecting references and inspirations, another free AI art platform called play-

ground was used, which allows to search publicly available AI art generated by users from around the world along with their prompts and settings to copy or remix our own.

The AI arts were not flawless in terms of game characters, and for backgrounds it did not always portray the game narrative accurately. Hence, it was needed to heavily rely on modifications/corrections using graphic design tools such as Photoshop and Photopea.

Photoshop

Adobe Photoshop was a key tool used in the creation of the game. It was used to create conversation boxes, characters, backdrops and user interface elements.

- Visual Design: The game's story and aesthetics were enhanced by designing characters, backgrounds and user interface elements thanks to Photoshop's robust and flexible features.
- Character Design: To develop expressive and varied characters that fit their respective roles and characteristics in the game, along with pose changes, expression changes and clothing changes, it was needed to use Photoshop, as AI tools aren't too consistent with variations. These character images were exported in PNG format with transparent backgrounds, allowing for easy placement and layering within scenes.

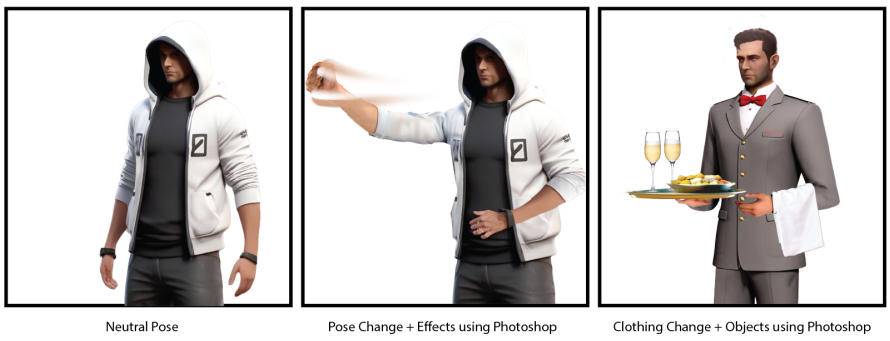


Figure 12: Photoshop manipulations on the main character. Source: Own screenshot.

- Backgrounds: Photoshop made it easier to modify the AI generated backdrops so that they are accurate to the storyline and set the mood and setting. As they did not require transparency like the overlaying characters. These backgrounds were exported in JPEG format to maintain

quality while minimizing file size, ensuring smooth performance within the game.

- Dialogue Boxes and UI Elements: Player engagement was improved by creating slick dialogue boxes and user-friendly UI elements using Photoshop's features.

A layout.psd file was maintained to keep the designs consistent throughout the game, especially as placement of individual characters and objects in each scene using Python was prone to human errors. The character layers in Photoshop were hence created with blank/transparent backgrounds in PNG format so that they could be placed on top of of JPEG backdrops and could be interchanged with each scene.(see figure 13).

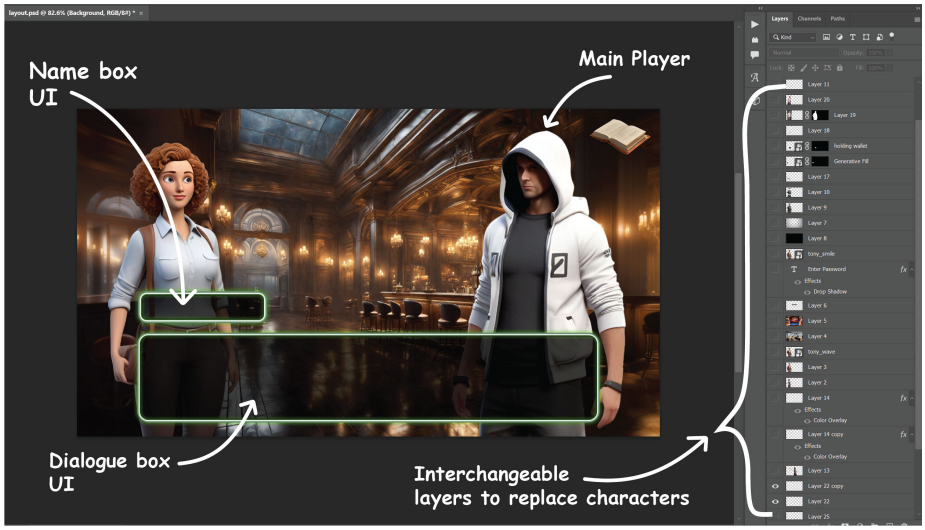


Figure 13: Overview of the design layout in Photoshop. Source: Own screenshot.

The Student Trial License's implications:

- Time Constraints: Although the trial gave users complete access to Photoshop's functionality, there were time restrictions, so users had to use the program quickly to finish projects on time.
- Compliance: Meeting Adobe's requirements required using the software for non-commercial purposes and honoring trial expiration dates.
- Future Licensing Considerations: In order to maintain Photoshop use for continued development, it was intended to investigate licensing solutions

after the trial.

Despite the trial constraints, Adobe Photoshop was invaluable for creating the visual components for the game. When the project develops, it is wished to investigate licensing opportunities for ongoing use. In the meanwhile, more game assets were developed, using the free browser based tool Photopea.

Photopea

Photopea is a free, browser-based photo editor with high similarity to Photoshop. It is easily accessible and offers almost the same functionality as the high-cost alternative. It was used to create parts of the user interface including icons, the journal as well as the various mini-games like the torn-apart letter. The resulting PSD files are saved in the git repository and opened in Photopea to edit them.

The click detection in Ren'Py checks at the click location which PNG layer is on top and has a non-transparent alpha value at this exact location. Therefore all icons or interactable areas of an image have to be exported layer-wise as separate PNGs, so for example a button is separated from the background. To position them within the frame the material has to be placed within a 1920x1080 pixel canvas. This way they can be used in the code without having to be positioned anymore.

As Ren'Py supports a hover state if the cursor hovers over an interactive area, all interactive PNGs are given a second version that shows them in a hovered state. For icons, this means the white icon turning grey and for selective options like in mini-games or on the map they get a highlight using the layer effect "outer glow" (see figure 14).

To achieve a higher usability and more comfortable handling, icons or convex clickable shapes get a simple shape like a rectangle or sphere as a background with 1% transparency. The almost transparent and basically invisible background gets exported together with the convex symbol into one single PNG. This way, the symbol does not have to be clicked exactly but in the roundabout area.

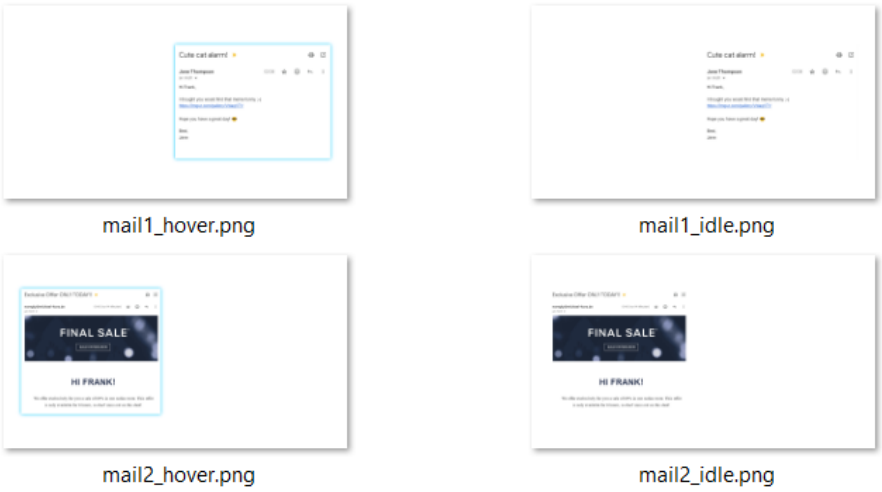


Figure 14: Images exported from Photopea. All states and "buttons" are separate images. Source: Own screenshot.

Code Snippets and Design Integration

The following is a code snippet showing few initialization of characters and backgrounds:

```
...
...
image Receptionist2="receptionist2.png"
image Receptionist2 angry="receptionist2 angry.png"
image Receptionist2 smile="receptionist2 smile.png"
image k1 stressed="chef1 stressed.png"
image k1 happy="chef1 happy.png"
image Me canteen="playercanteen.png"
image Me chef="playerchef.png"
image e4="e4.png"
image e5="e5.png"
image e6="e6.png"
image e8="e8.png"
image e9="e9.png"
image e4 smile="e4 smile.png"
image k2 stressed="chef2 stressed.png"
image k2 happy="chef2 happy.png"
image k2 angry="chef2 angry.png"
...
```

```
...
image bg n42="bg n42.jpg"
image bg coreback="bg coreback.jpg"
image bg coreback2="bg coreback2.jpg"
image bg coreback3="bg coreback3.jpg"
image bg main ent="bg main ent.jpg"
image bg main ent2="bg main ent2.jpg"
image bg garage="bg garage.jpg"
image bg cafe="bg cafe.jpg"
image bg cafe1="bg cafe1.jpg"
image bg cafe2="bg cafe2.jpg"
...
...
```

The code snippet begins with the definition of character and background images using the image keyword. Each image is assigned a variable name along with its file path, specifying its location within the game's directory structure. As mentioned before the characters are in PNG format while the backgrounds have a `bg` prefix to identify them easier with JPG format. After defining, here is how the images are used in game scenes:

```
...
...
label canteendisguise:
    scene bg coreback3
    show Me with easeinleft:
        xzoom -1.0

    "Disguised as canteen employee, you walk towards
       the back entrance that leads to the companys
        canteen."
    scene bg canteendoor
    show Me
    "Heavily loaded and appearing to be busy with work
       , you move toward the door and open it. Then
       suddenly a kitchen employee looks at you
       weirdly."
    scene bg kitchen
    show Me canteen
    show k1 stressed
```

```
    menu:
        "Hide your face and try not to drag too much
           attention on you":
            jump hideface
        "Act friendy and ask him for help with the box
            you are carrying":
            jump askhelp
...
...
```

In this snippet, the label `canteendisguise`: defines a specific scene in the game where the player character is disguised as a canteen employee confronting another character.

The command "`scene bg coreback3`" sets the background to "`bg coreback3`". It establishes the backdrop for the upcoming events, depicting a location relevant to the narrative.

The line "`show Me canteen with easeinleft:  xzoom -1.0`" introduces the player character (Me) with a transition effect (easeinleft) and flips the image horizontally (xzoom -1.0). This action suggests movement or entry into the scene.

The command "`scene bg canteendoor`": This command changes the background to "`bg canteendoor`". The code "`show Me canteen`" lets the player character (Me canteen) to be displayed again, indicating continued presence in the scene.

The command "`show k1 stressed`" introduces a new character to the left of the screen as it is designed with that position from the layout.psd.

5 Outlook

The open tasks and ideas presented here have been discussed by the current implementation team and were supposed to be implemented. However, due to the time constraint of the project, those tasks were not completed or implemented yet. Hence, they are summarised for the future team here. Nevertheless, it is encouraged to look beyond the ideas proposed here and develop the game further with new ones.

5.1 Story Department

For the story department, key ideas to deepen and expand the narrative were identified, focusing on enhancing the further levels and player engagement.

Level 4 Expansion

In level 4, the player faces the task of developing convincing deepfake materials of the head of the Crimson Group, employing various tactics such as infiltration and hacking to collect voice and face recordings. After obtaining the necessary materials, the player needs to navigate through strict security measures to gain access to a heavily guarded video conference where the head of this operation, who is the son of the boss from TastyFood, is present, carefully presenting the evidence without arousing any doubts or suspicion. This leads to, where the player faces a crucial decision: whether to reveal the evidence, risking backlash, or take the money and leave the country, with each option having important moral implications. The outcome of this decision branches into multiple endings, shaping future interactions and story lines based on the player's actions.

Integration of further Social Engineering Techniques

Although many techniques have already been covered in the game, there are techniques that have not yet been featured. The following methods could be interesting for an expansion. Scareware could be integrated by displaying a message or pop-up to a target that their PC is infected with a virus. The honey trap method could also be incorporated. For example, a victim could be tricked into revealing sensitive information on a dating site by posing as an attractive person. With new methods appearing all the time, it is certainly exciting to keep up to date and integrate new, more unusual techniques into the game.

5.2 Design Department

Update Level Selection and Map

For each new level added, the preview images in the level selection PSD need to be updated. This is done by editing the smart object's content within the PSD file (Layer > Smart Object > Open (edit contents)). They need one locked

state (zero saturation and the lock icon), an unlocked state (normal image with white border) and an unlocked hovered state (copy layer effect "outer glow" from existing layers). The images used are backgrounds that play a key role in the respective level.

Updating the map is done in a similar way: For each new location the player goes to, a new location has to be added on the map. This can be done by just selecting the existing layers of one arbitrary location and copy pasting them (e.g. by using CTRL+J) and then just replacing the content. Smart objects have to be made separate copies, otherwise the content of all smart objects is being affected by change. This is done using the right-click menu option "New Smart Object via Copy". Locations only appear once they have been visited and have different states too: idle state (has been visited already), active state (supposed to be selected now) and active hovered state (active and hovered by the cursor). An exemplary state for when the CORE company is the next location to visit can be seen in figure 15.

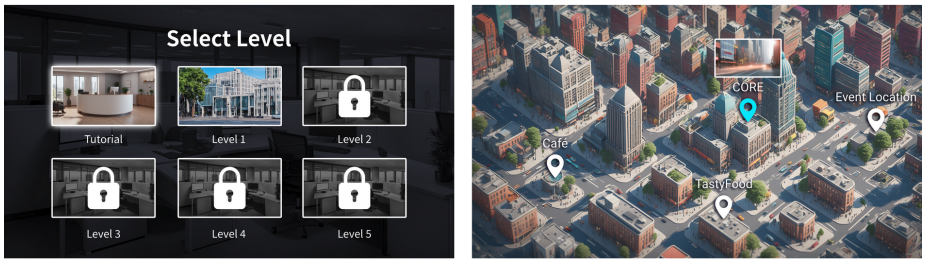


Figure 15: Level selection (left) and map (right). Source: Own screenshots.

5.3 Programming Department

For the programming department, there are several open tasks for future development. However, it is advised to think beyond those open tasks and ideas to enhance the player experience.

Choose your Character

In the beginning, the current team decided that the player should have the choice between different sprites as a character. It was discussed to offer a small range of female-, male- and non-binary-looking characters. While the design team needs to design those different characters, the programming team needs to implement the code for the selection of character and make sure that this character is saved and visible throughout the whole game. It is suggested that this functionally will be implemented when starting the tutorial before the story begins.

Implement the second phishing email mini-game

There is one mini-game that was proposed by the story team but was not implemented yet. The corresponding material can be found in the appendix. The idea is to create a phishing email, being able to choose between two options. Every paragraph or sentence of the phishing email should have two choices for the player to choose from such that they build a unique email. These choices should be somehow evaluated in the end such that it will impact the story further. An idea was discussed to have the two options for each part next to another such that the player can click the desirable option. The options can internally be assigned to some score such that the overall phishing email can be later evaluated. A difficulty could be to make the game visually appealing while the overview of the whole email is still preserved because the email seems to be lengthy. For that purpose, the programming and design team need to cooperate and find a good solution for it.

Implement voice recording and mini-game in level 2
For level 2, in the story the player records important information from the senators meeting and afterwards listens to this with Cathy. Here our plan was to actually listen to the voice recording, so the game feels more interactive and not repetitive. The voice recording is already created with AI. The other mini-game that is missing, is getting the recording. We thought, we would like to make the hand over of the recorder more interesting. In the story, Cathy hands the recorder over discreetly, so as the mini-game the player has to find this recorder in a picture and click on it to take it.

Add map and journal elements

The map and journal (inventory) are already implemented but not inserted into all levels yet. The tutorial and level 1 have examples of the map being introduced and inserted as well as inventory information collected. This needs to be continued throughout all levels. Every time, there is a change in location, the story should for example read "Go the café." and the map is supposed to appear with the only clickable choice being the café. For the journal, every time a new character is introduced or new, useful information is discovered, there should be an addition to the journal for the player to look back upon.

Add a starting image and logo for the start page

When opening the game, the background image is the preset Ren'Py background. This should be changed by creating an image specific to the game. The programming department can delegate the design and creation to the design team but will need to insert it in the code. The same applies to the logo when building a distribution with an executable file which currently contains the Ren'Py logo.

6 Conclusion

Social engineering and its techniques were discussed as a first step in this project. Based on this knowledge, the team decided to develop a story-based game using the RenPy engine. By giving the player options to choose from, the story would progress and lead to the uncovering of a scandal involving various parties. The application of social engineering was done in a similar fashion and could succeed or fail based on the player's decision. Within this concept, the team believed that the user would have a more fun and interactive learning experience, leading to more awareness on security measures regarding potential social engineering attacks.

During the development of the story, many different actions and ideas were incorporated in order to create a divers game with as many different elements as possible. The goal was to build and expand a multi-level story without being repetitive. In addition, the use of generative AI was mostly successful in designing character sprites, backgrounds and some of the dialogue. However, additional time was needed to rework and design appropriate images and text, as some of the AI's work involved errors such as distorted body proportions. These types of mistakes could not be fixed by formulating additional prompts, requiring the design team to use additional software to create the desired, error-free images.

For the next iteration of the game, the team would like to expand on new and currently used social engineering techniques instead of more old school and direct confrontations. In particular, the involvement of generative AI in attacks is a topic that will be addressed in the planned level four, which has a high impact on the future and will require additional levels to fully convey the new risks and deceptions to the user. The involvement of AI can increase the credibility of deceptions. Since the effectiveness of pretexts depends on the overall impression of authenticity, the increasing sophistication of natural language processing through generative AI could make this form of hacking even more realistic. For example, generative AI could be used to mimic the writing style of trusted organizations or individuals to make phishing attempts appear more credible.

AI could also enhance attacks by significantly increasing their scale. Through automation and the ability to acquire language skills for attacks in foreign languages, this will result in large-scale attacks that are normally very time-consuming. Because of this, generative AI will play a big role in social engineering in the future, but it could also be the solution to building defense systems that rely on AI, identifying said attacks.

References

[1] H. Chen and K. Magramo. *Finance worker pays out $25 million after video call with deepfake chief financial officer*. 2024. URL: https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html.

[2] R. B. Cialdini. *Influence: The Psychology of Persuasion*. William Morrow; Revised edition (1 Sept. 1993), 1993.

[3] E. Dymoke. *GTA 6 leaks and Uber hacked through social engineering*. 2022. URL: https://www.hoxhunt.com/blog/gta-6-leaks-and-uber-hacked-through-social-engineering.

[4] Robert W. Gehl and Sean T. Lawson. *Social Engineering: How Crowdmasters, Phreaks, Hackers, and Trolls Created a New Form of Manipulative Communication*. The MIT Press, 2022.

[5] J. M. Hatfield. "Social engineering in cybersecurity: The evolution of a concept." In: *Computers & Security, 73* (2018).

[6] R. Lee. *The Secret History of Hacking*. 2001. URL: https://www.youtube.com/watch?v=PUf1d-GuK0Q.

[7] K. D. Mitnick and W. L. Simon. *The art of deception: Controlling the human element of security*. John Wiley & Sons., 2003.

[8] R. Rosenbaum. *Secrets of the little blue box*. 1971. URL: http://www.thestacksreader.com/secrets-of-the-blue-box-ron-rosenbaum-steve-jobs-influence/.

[9] Bundesamt für Sicherheit in der Informationstechnik. *Social Engineering - the "Human Factor"*. 2024. URL: https://www.bsi.bund.de/dok/11287460.

[10] Eva Wolfangel. *Ein falscher Klick. Hackern auf der Spur: Warum der Cyberkrieg uns alle betrifft. Wie wir uns gegen Angriffe aus dem Internet schützen*. Penguin, 2022.

A Appendix

In the appendix, the script for the second minigame on the phishing email (open task) ca be found. The document with the initial game concept is attached as well.

Task: Arrange the email snippets to create an effective phishing email

Dear Employees,

Dear Crimson Family,

We hope this email finds you well. At Crimson Group, we are always committed to providing our employees with solutions to meet their evolving needs. Because we know how dangerous your job is, we would like to provide you with life insurance, ensuring that you and your loved ones are covered at every moment.

We hope this message finds you well. We are writing to inform you of a matter that requires your immediate attention. Unfortunately, we have identified a security breach in our email system that may have impacted your mailbox. Upon thorough investigation, it has come to our attention that unauthorized access was gained to our email servers, and we believe that your email account may have been compromised.

To learn more about the specifics of our Life Insurance coverage and how to enroll, please click on this link.

To ensure the security of your account, we recommend following the steps provided on this link.

Keep in mind that this opportunity is time-sensitive, and the offer may expire soon.

We believe that this addition to our benefits package reflects our commitment to the well-being of our Crimson Group family. Your dedication is the foundation of our success, and we want to ensure that you and your loved ones are provided for in all aspects of life.

If you have any concerns or need further assistance, please do not hesitate to contact our support team at Crimson Group. We sincerely apologize for any inconvenience this may cause and appreciate your understanding as we work to resolve this issue promptly.

Thank you for your continued hard work and dedication!

Best regards,

Crimson Group

Successful:

Dear Employees,

I hope this email finds you well. At Crimson Group, we are always committed to providing our employees with solutions to meet their evolving needs. Because we know how dangerous your job is, we would like to provide you with life insurance, ensuring that you and your loved ones are covered at every moment.

Keep in mind that this opportunity is time-sensitive, and the offer may expire soon.

To learn more about the specifics of our Life Insurance coverage and how to enroll, please click on this link.

We believe that this addition to our benefits package reflects our commitment to the well-being of our Crimson Group family. Your dedication is the foundation of our success, and we want to ensure that you and your loved ones are provided for in all aspects of life.

Thank you for your continued hard work and dedication.

Best regards,

Crimson Group

Dear Crimson Family,

I hope this email finds you well. At Crimson Group, we are always committed to providing our employees with solutions to meet their evolving needs. Because we know how dangerous your job is, we would like to provide you with life insurance, ensuring that you and your loved ones are covered at every moment.

Keep in mind that this opportunity is time-sensitive, and the offer may expire soon.

To learn more about the specifics of our Life Insurance coverage and how to enroll, please click on this link.

We believe that this addition to our benefits package reflects our commitment to the well-being of our Crimson Group family. Your dedication is the foundation of our success, and we want to ensure that you and your loved ones are provided for in all aspects of life.

Thank you for your continued hard work and dedication.

Best regards,

Crimson Group

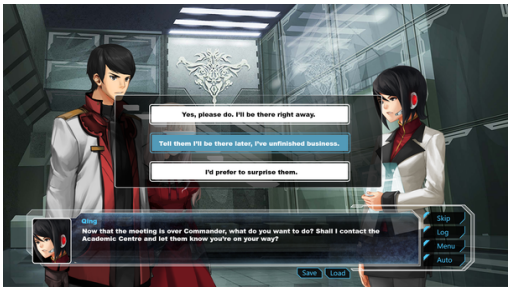
Game concept

Idea

- Robin Hood kind of story
- player is a pen tester
- during testing the player realizes there is a conspiracy and the companies are the bad guys
- attack different companies → use different techniques
- goal: find information and leak to the press

Plot

- pen test a food manufacturer Tasty Food Co.
- they sell avocados, which are cultivated in the rainforest by farming company AvoHarvest
- player discovers:
    - they burned the area illegally down to get more space
    - politician Veronica Manipulo covers it all up and provides them benefits
    - Tasty Food Co. finances her political campaign
- optional story elements: pen tester is commissioned by a company that's evil too, assassinations are involved, love story with news reporter friend…
- ending:
    - usb stick with info to a friend working at a newspaper publisher, story published → they date <3
      everyone imprisoned, make politician compensate workers in rainforest
    - blackmail companies and politician, keep the money, buy a yacht



Game design

- player:
  - name: user input
  - no clearly defined gender
  - profile pic: set of 5 character designs, player chooses
  - backstory: started hacking as a child 😎
- location: big unspecified city, all parties are there
- interaction:
  - intriguing but not too complicated to follow → goal is educating
  - point and click to investigate a room or choose a building to enter
  - apart from that: dialogues and multiple answers
  - learn methods (email, tailgating, …) and apply those depending on the situation, like an inventory / skill set
  - no help buttons: new tools are explained, no way to get stuck
  - hints for choosing methods, point out mistakes → educational
  - timer depending on situation, e.g. get caught → decide dialogue option fast
- minigames:
  - depending on story
  - keep player's interest, make it more interactive
  - some results are not unnecessary → realistic
  - repeat if failed
- level structure:
  - pen testing phase as tutorial level → then discover the company has a secret
  - not 4 clear phases (you need to go back and forth)
  - each company = one level, each consisting of the four phases
  - reach next level:
    - find information that you need to proceed
    - collecting points to visualize the progress
  - trial and error: if you miss the timer for example, then you have to redo a subsection of the level, but you keep the information from the previous parts
- "inventory":
  - notebook / journal:
    - notes, information
    - tasks
    - objectives
  - objects only for specific subsections where you need them (key, usb stick, letter, …)
  - https://f95zone.to/threads/creating-a-smart-renpy-inventory-system-using-lists-in-python.54815/