Table of Content

1. Purpose / Project Objectives

1.1 Abstract

Social engineering refers to the “psychological manipulation of people into performing actions or divulging confidential information”. The Verizon Data Breach Incident Report 2020 states that 22% of data breaches were related to social engineering attacks and 96% of these attacks were executed through emails (Ward & Pritam, 2020). Social engineering utilizes tools such as emails or text messages to prey on victims in order to achieve its objectives. It is therefore extremely important for us to have an in-depth understanding of social engineering. Equipping ourselves with such knowledge will allow us to be more wary and better guard ourselves against such threats.

In a social engineering attack, a perpetrator would usually investigate the general background of intended victims in order to gather necessary information before proceeding with the attack. A social engineering attack is especially dangerous compared to other forms of cyber security attacks because it relies heavily on manipulating victims and human error instead of vulnerabilities in software and operating systems. Perpetrators will attempt to gain the victims’ trust and thereafter provide stimuli for subsequent actions that could break security protocol. This might involve manipulating individuals into revealing sensitive personal information or information that would allow perpetrator to gain access to important resources. These would eventually compromise the privacy of an individual or an organization.

The social engineering life cycle illustrated below shows the general sequence of steps that a perpetrator would carry out in an attempt to scam individuals.

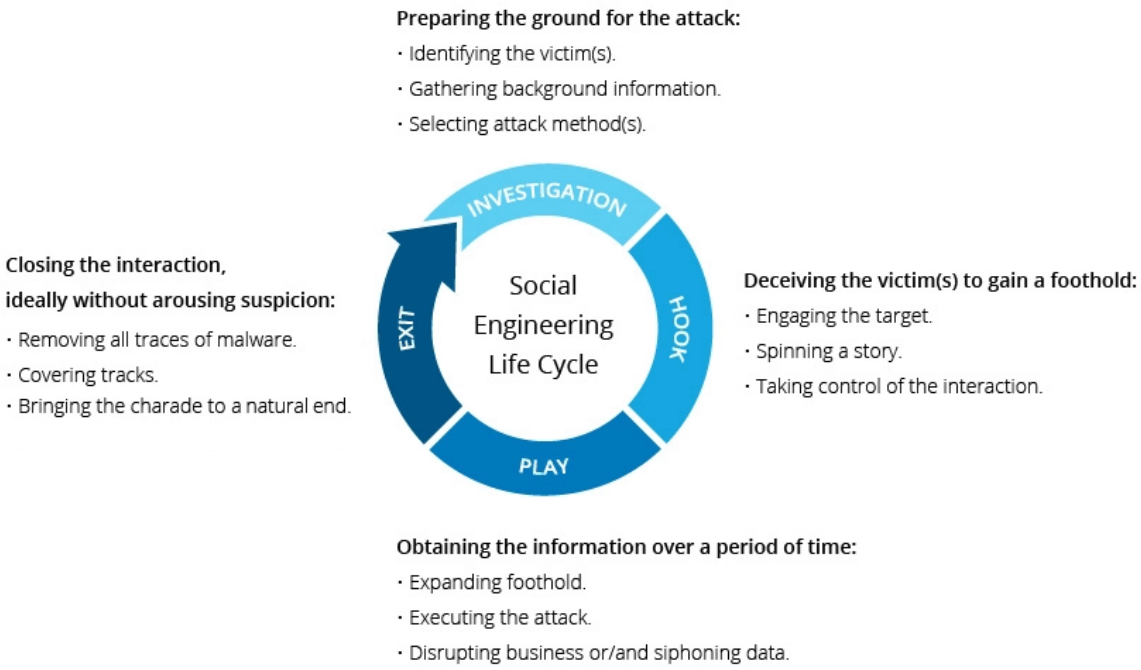

Figure 1: Social Engineering Life Cycle, Source : Imperva

Social engineering attacks have been the cause of several incidents involving high profile individuals. One of them includes the Twitter Account Hack in 2020. In July 2020, hackers were able to gain access to several high-profile Twitter accounts such as those belonging to Elon Musk, Joe Biden and Bill Gates (Leswing, 2020). They were able to do so through the unauthorised use of internal administrative tools which were obviously unavailable to the public but available to the company's employees. The perpetrators were able to successfully convince a Twitter IT staff that they were fellow co-workers who required access to the admin tools. This allowed the perpetrators to gain full access to several high profile Twitter accounts and also allowed them to post tweets from as many as 45 Twitter accounts. As many as 300 followers of these accounts were scammed into 'donating' bitcoins to these scammers. The tweets assured victims that their donations would be returned in double. Furthermore, with these tweets being posted on official accounts of high-profile individuals, it was much easier for perpetrators to gain the trust of these victims.

Another incident was the Magellan Health Breach. In the Magellan Health breach in April 2020, the perpetrator was able to gain access into Magellan Health's systems by sending a phishing email (Davis, 2020). The perpetrator impersonated as a client and

was able to successfully obtain data which included sensitive personal information of employees. The perpetrators eventually deployed ransomware into the company's system. This incident once again illustrates clearly illustrated that social engineering can also be used as an entry point for secondary, and more devastating cyber-attacks.

All these incidents show how dire it is for individuals to be aware of social engineering attacks and the common tactics that perpetrators often deploy in order to achieve their objectives. This would allow for individuals to protect themselves as well as organizations associated with them in the event of a social engineering attack.

1.2 Introduction

Our project theme is Cyber Security and more specifically on the 'Detection and Mitigation of Social Engineering Attacks'. A social engineered attack is a non-technical method of intrusion that relies on human interaction, trickery and manipulation. It uses psychological manipulation that results in people performing actions of divulging confidential information. Since our project falls under the theme of Cyber Security, we will be focusing on digital social engineering attacks. These digital social engineering attacks leverage on digital tools and platforms to manipulate victims.

There are a few types of social engineering attacks which we will be focusing on, namely phishing, baiting and quid pro quo, as these attacks are easier to replicate through an immediate interactive platform as compared to a phone call involving a real conversation.

Phishing is a form of social engineering attack in which victims are contacted by email, telephone or text message by someone who is posing as a legitimate or reputable institution or source in order to lure individuals into providing sensitive data such as personally information, banking and credit card details, and passwords. With this information, the perpetrator will then be able to access important accounts which can eventually result in identity theft and financial loss.

Baiting is a type of social engineering attack where a perpetrator utilizes online tools such as website pop-ups to advertise attractive prizes and or rewards to the victim. If the victim falls prey to such false promises, the perpetrator will be able to successfully lure a victim into a trap which may steal personal and financial information or inflict the system with malware.

Lastly, quid pro quo is another form of social engineering attack in which perpetrators will impersonate a legitimate source of assistance. The most common example is the case of technical support impersonation, and these perpetrators will attempt to offer some sort of assistance. Through offering 'assistance' to these unknowing individuals, victims are eventually guided through a series of steps as instructed by the perpetrator. Instead of rendering assistance, the scammers will be able to gain access to the victims' computers or personal information. This will then provide the scammers with a platform to launch malware or gain access to sensitive personal information.

2. Project Summary

2.1 Objective

We aim to educate individuals on how to detect and mitigate such social engineering attacks through an interactive game and education platform. We feel that it is important for individuals to be aware of such attacks since these attacks can be easily disguised as something harmless.

2.2 Project Description

Since such social engineering attacks can often be prevented by awareness of such situations, we intend to create an interactive game that would be a stimulation of such attacks in seemingly normal situations such as a regular website or a harmless email. Since we are unable to include all variations of such attacks in a one platform, we also intend to include an 'Education' segment in addition to the 'Game' segment to provide individuals with more resources and knowledge towards handling such situations.

3. Scope

3.1 Project Deliverables

We intend to focus on three main types of digital social engineering attacks: phishing, baiting and quid pro quo attacks. We will be incorporating scenarios through an interactive platform as well as educational resources that will allow users to have a better idea of the forms in which these social engineering attacks can present themselves in.

3.2 Summary of Work

In order to create the proposed educational game, we utilized the Unity game engine. Unity allows for the creation of 2D or 3D games and the engine also offer primary scripting in C#. Through using Unity, we created an educational game that would allow users to gain awareness on the various scams that we chose to replicate. The educational game will have 2 main sections: the ‘Game’ segment and the ‘Education’ segment. We carried out research and studied some case studies on the various scams which we intended to replicate.

3.3 Schedule

3.3.1 Initiating Phase

During the Initiating Phase, we were introduced to our team members as well as the themes which we were allocated to. We appointed members for the positions of team leader as well as the treasurer. We were also briefed on a few means we can look into to start our project development.

3.3.2 Planning Phase

In the Planning phase we brainstormed for ways in which we were able to incorporate the content that we were introduced to during the first few weeks of the course into our project. We identified the main idea which we all agreed upon, which was the

interactive game website. After the proposal presentation, we also discussed with our mentor on the various areas for improvement and the ways in which we would be able to expand on our idea.

3.3.3 Execution Phase

In the Execution Phase, we were each allocated a segment of the game to develop ideas for. Each segment of the game generally involved a different scam and hence we focused on the respective type of attack which we were allocated to. We also sourced for educational resources and came up with quiz questions based on the type of attack that we worked on. Throughout the project we made improvements to the code in Unity and rearranged the sequence and flow of our content.

3.3.4 Closing Phase

After finalising the flow which we all agreed on for the interactive platform, all the various segments of the game were integrated together and started working on the group report as well as presentation slides.

3.4 Project Design and Development

We first started the project by identifying the specific examples of social engineering attacks which we wanted to focus on. We did this by going through a series of case studies in order for us to make a better decision on the attacks which would be feasible to replicate through an interactive gaming platform.

3.4.1 Case studies

In this portion we will be sharing about the characteristics of the various scenarios that we intend to replicate through this project.

3.4.1.1 Phishing: Email Spoofing

Email spoofing is a technique used in spam and phishing attacks to trick users into thinking a message came from a person or entity they either know or can trust. In spoofing attacks, the sender forges email headers so that client software displays the fraudulent sender address, which most users take at face value. Unless they inspect the header more closely, users see the forged sender in a message. Since it is a name that victims recognize, they are more likely to trust it.

Example: PayPal email spoofing

There are instances where scammers send emails that resemble emails from PayPal. The message tells the user that their account will be suspended if they do not click a link, authenticate into the site and change the account's password. If the user is successfully tricked and types in credentials, the attacker now has credentials to authenticate into the targeted user's PayPal account, potentially stealing money from the user.

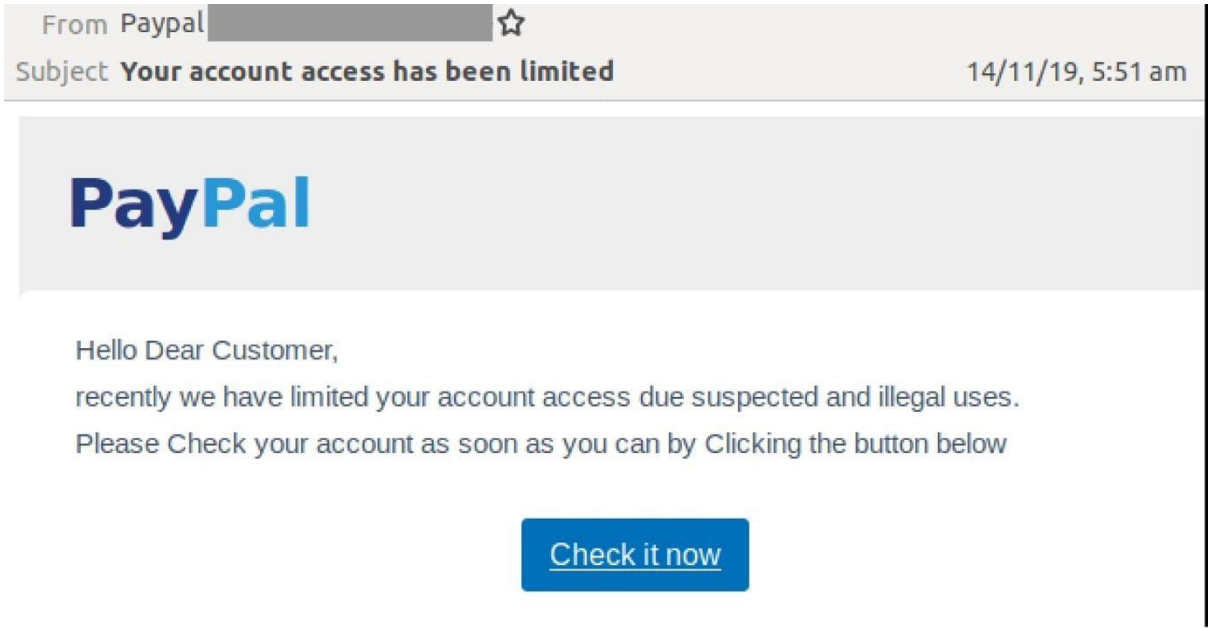

Figure 2: Example of Paypal email spoofing, Source: MailGuard

Replication of the scam

We decided to replicate the scam in our interactive platform by having users spot the tell tale signs of an email phishing scam. This way they will be able to know the key characteristics of such scams.

3.4.1.2 Quid Pro Quo: Tech Support Scam

Tech Support Scam is a common method used by scammers to deceive unsuspecting individuals into divulging their personal information such as their bank account details. This infographic provides information on how this scam typically works, the signs individuals can look out for if they suspect they are being scammed, and how individuals can protect themselves against such scams. From January to December 2019, 249 tech scams were reported in Singapore and $13.9 million was cheated in Singapore alone (Chee, 2021).

Example: Microsoft tech support scam

Microsoft has been fighting against tech support scams since 2014, with scammers leveraging on Microsoft's brand for impersonation purposes (Sethi & Pek, 2021). Tech support scammers impersonating as Microsoft employees started with cold calls fraudulently notifying people that they were victims of malware infections or other harmful attacks. This evolved into fake "pop-ups" displayed on people's computers, again trying to convince them that something was wrong with their computers so the scammers could extract payment for "fixing" fake issues. Each month, Microsoft receives about 6,500 complaints from people who've been victims of tech support scams, which is down from 13,000 reports in an average month in prior years (Yik & Woo, 2021).

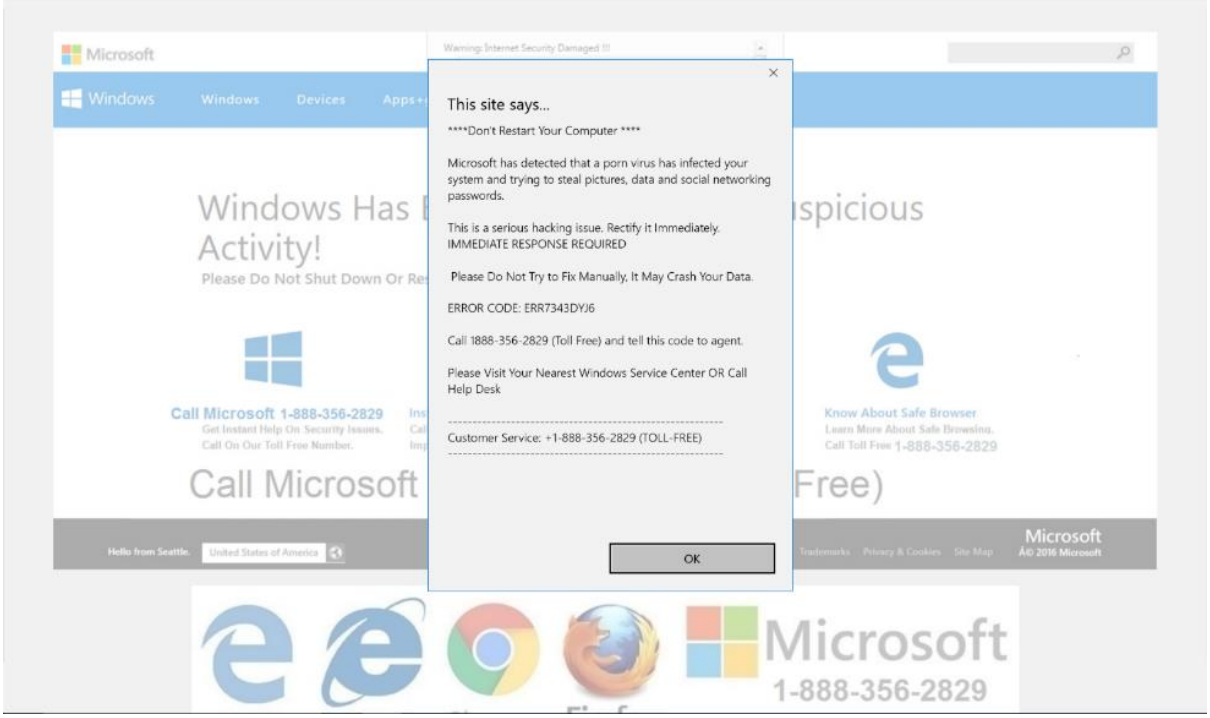

Figure 3: Example of tech support scam, Source: Microsoft

Replication of the scam

We decided that to replicate the internet pop-up version of the tech support scam in our educational game since it is one of the most common and recent ways tech support scams occur. Through this replication, the players will be able to experience how a tech support scam can occur even through browsing the internet. This would also allow players to be aware of how to prevent such incidents by avoiding them.

3.4.1.3 Baiting: Giveaway Scam

The giveaway scam is another common method that used by scammers to lure victims through using attractive and allegedly free prizes as bait. It is extremely common for such scams to present themselves in the form of emails or internet pop-ups. These prizes being ‘won’ by the victims are not free and would scam victims of their money by tricking them into paying a down-payment to receive the prize.

Example 1: Internet pop-up giveaway scam

The most common way which the giveaway scam presents itself in, is through an internet pop-up since it is a convenient way to catch victims' attention when they are browsing through the internet. Such internet pop-ups are also often customized to the region in which the victims are viewing these pages. In Singapore for instance, such internet pop-ups used to be targeted towards locals or elderly individuals by having prizes such as 'Sheng Shiong Shopping Vouchers' or 'Fairprice lucky draw'.

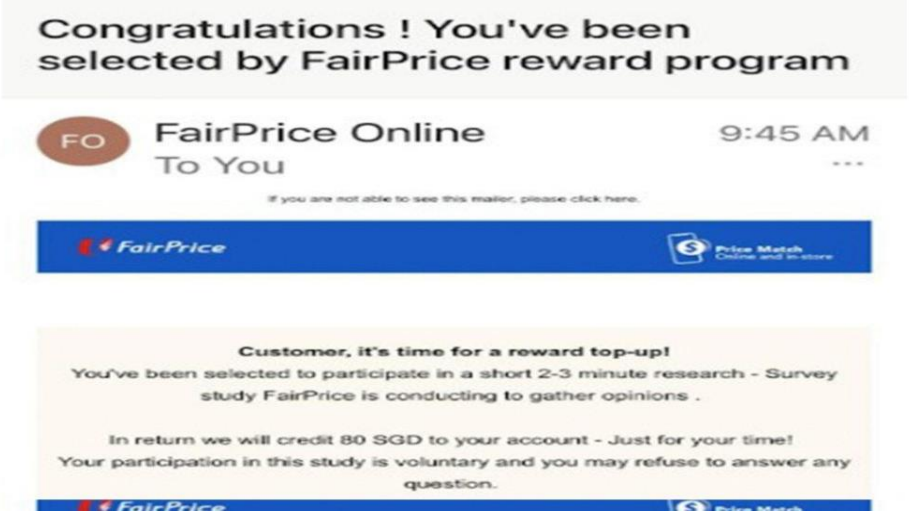

Figure 4: Example of Internet pop-up giveaway scam

Replication of the scam

We decided to replicate the internet pop-up version of the giveaway scam since it is the most common and widespread way for a scammer to reach victims or various demographics. This scenario will be included in our educational game in which the game will stimulate the player browsing through the internet and encountering one of these pop-ups. When the player clicks on the pop-up and is directed to the payment section of the scam, the players will be able to see how such scammers can easily obtain account information through the false assurance of a prize at the end of the transaction.

3.5 General flow of Interactive Game Platform

3.5.1 Login, Home page

Users will first be instructed to login since they will be able to earn points throughout the interactive experience. Once an account is successfully created and they managed to log in, they will then be directed to the home page where they will be able to choose whether they would like to proceed with the Education segment first or the Games segment.

Figure 5: Game Interface - Login Page

Figure 6: Game Interface - Welcome Page

Figure 7: Game Interface - Main Menu

3.5.2 Game Segment

Figure 8: Game Interface, Game - (Main Menu)

If the 'Game' segment is selected, the user will be directed to the interface as shown. The interface will show the themes of games that they will be playing. The 'Game' segment offers different levels: Easy, Medium and Difficult. This allows the educational game to offer a slight challenge for the users to complete the segment successfully. Each difficulty level will be directed by the replicated scenarios as mentioned above. The 'Easy' level will include a replication of the Giveaway scam, 'Medium' level with the Email spoofing scam and 'Hard' level with the Tech support scam.

The user will only be allowed to progress to the next segment after clearing the level that he/she started playing in. Each level ends with a quiz, except for the last level, and the user will be required to answer all questions correctly before proceeding to the next level.

3.5.2.1 Easy Level : Giveaway Scam

This will be the first level that the users will be playing when they enter the game segment. The three types of scams that we intend to focus on will also act as different levels for the game based on the complexity of the scams. The baiting scam in the form of an internet pop-up giveaway is the simplest scam out of the three that we have decided to focus on since it mainly requires awareness to avoid falling prey to such a scam.

As this simulation game is a simple run through of a giveaway pop up, whereby its aim is to get the user to explore pop up scams from “their” desktop, there will be no tutorial.

Figure 9: Game Interface, Game - Task 1 (Welcome page)

Once the user clicks “Start”, they will be led to “their” desktop.

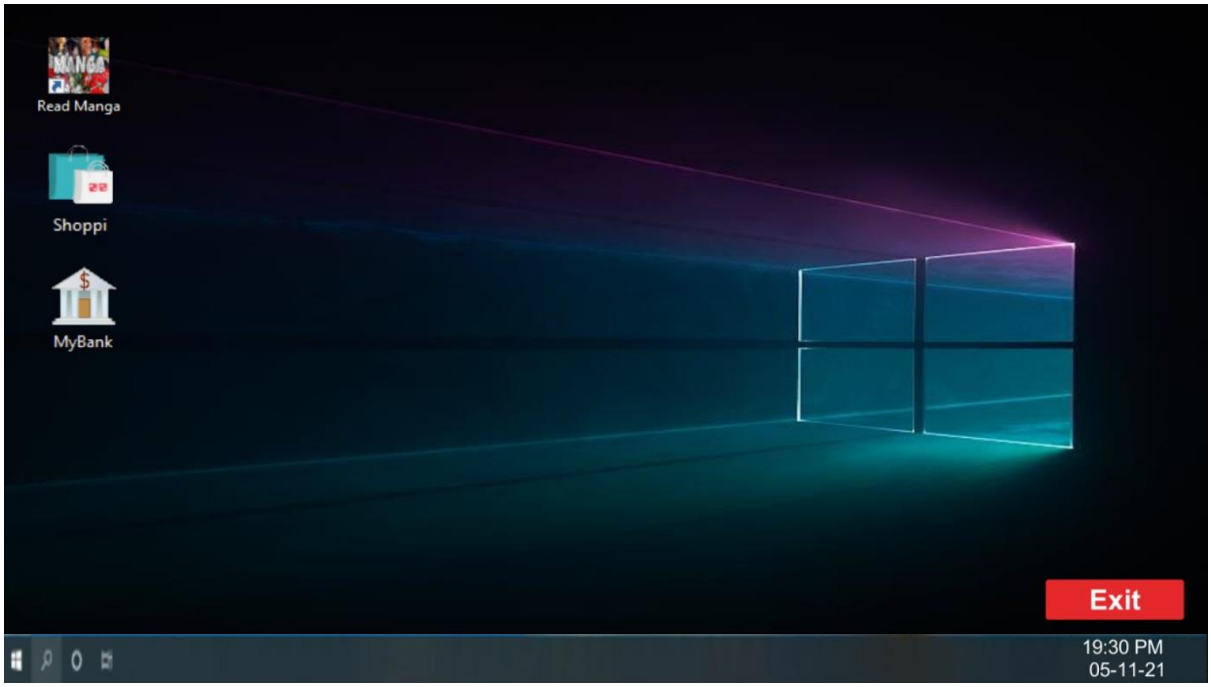

Figure 10: Game Interface, Game - Task 1 (Main Menu)

The storyline of this first scenario-based level involves a desktop screen with an anime browsing icon and shopping icon. When either of the icons are clicked, there will then be an internet giveaway pop-up that will show up on the screen. We wanted to show the user the scenario that will follow if that pop-up is being clicked on.

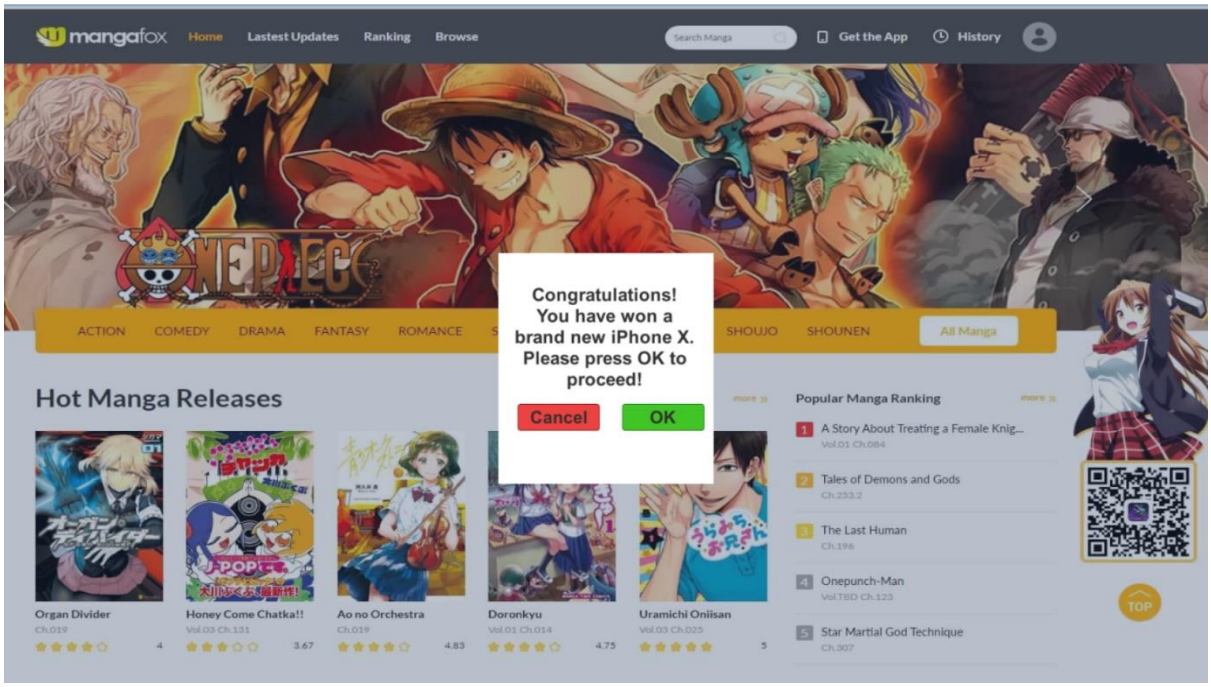

Figure 11: Game Interface, Game - Task 1 (Scene 1)

This level will then showcase the way a scammer will try to lure the victim into giving away sensitive personal information such as credit card information. If the user clicks on the wrong options that will result in 'financial loss' they will be required to replay the scenario to increase their awareness of such scams.

This is the initial amount in the user's bank and can be viewed via the "MyBank" icon from the desktop.

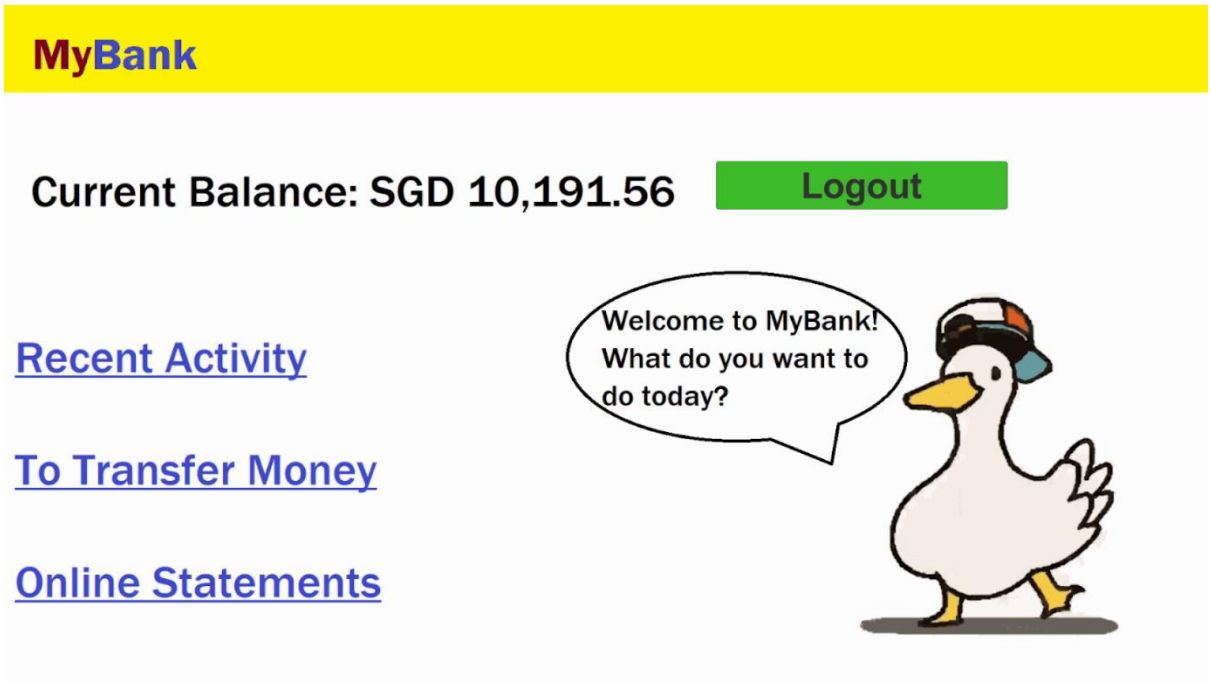

Figure 12: Game Interface, Game - Task 1 (Scene 2)

When the user selects "Ok" to the pop-up message, they will be directed to a site that asks for credit information.

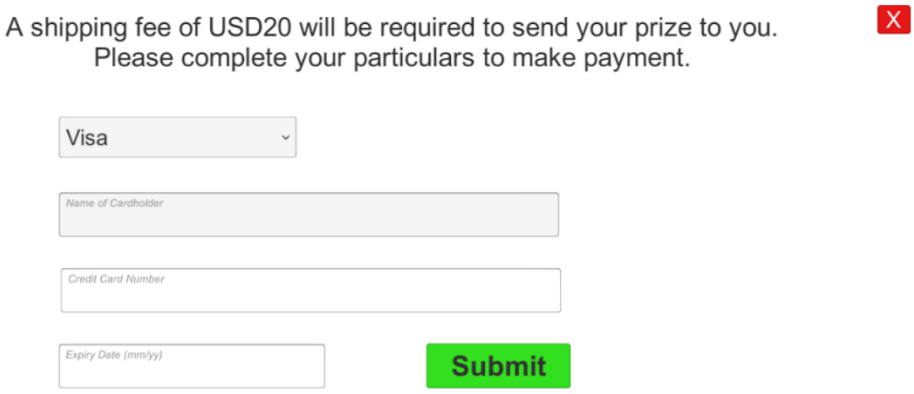

Figure 13: Game Interface, Game - Task 1 (Scene 3)

If the user submits their particulars instead of exiting out, the consequence will be displayed to them as shown.

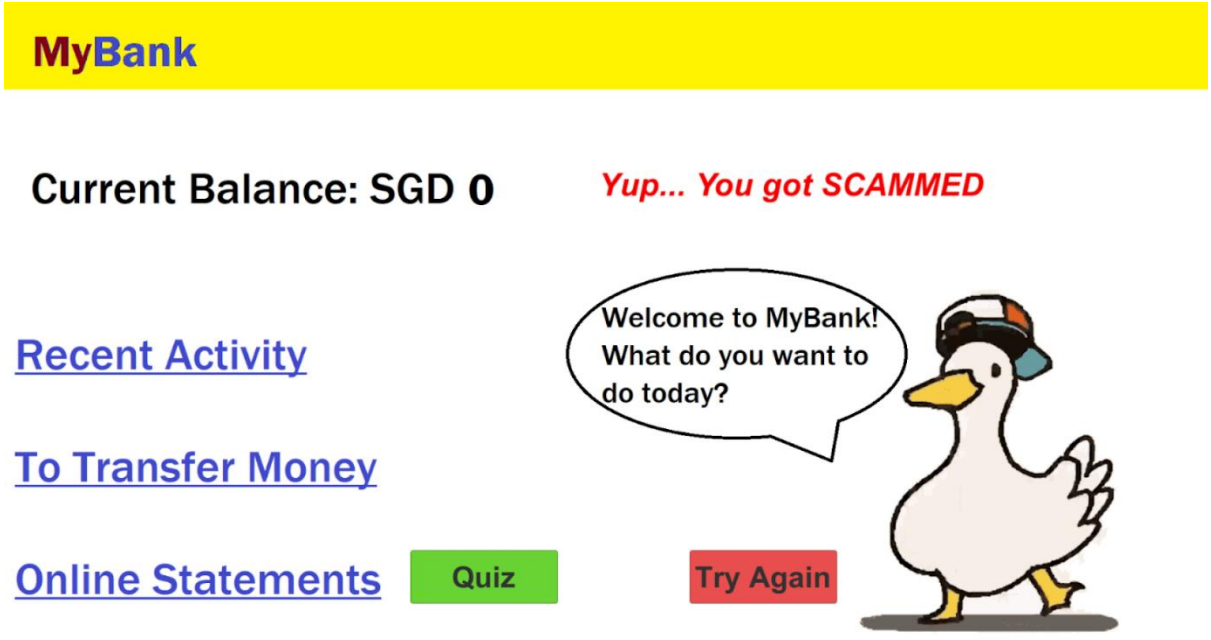

Figure 14: Game Interface, Game - Task 1 (Scene 4)

If the user does not fall for any scams, an advice will be displayed, and users can proceed to do the quiz.

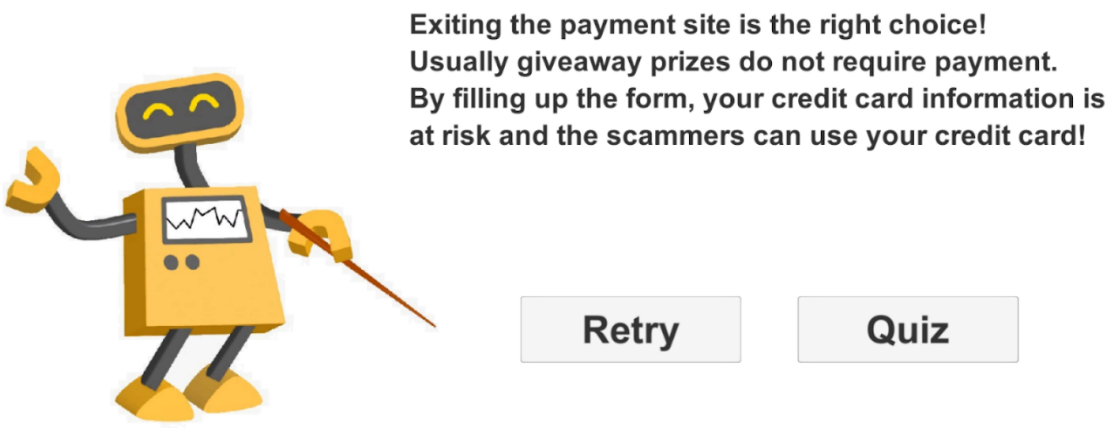

Figure 15: Game Interface, Game - Task 1 (Scene 5)

The user successfully completes the gameplay regardless of if they got scammed or not when a “Quiz” button is shown to them. By clicking on the “Quiz” button, they will be required to complete a set of questions that are randomized. The user will also be required to obtain full marks for this quiz section before proceeding to the next level. Meanwhile, they can also choose to retry the simulation game by clicking on the “Retry” button.

There will be 8 questions in total for the first quiz. This is an example of a quiz question.

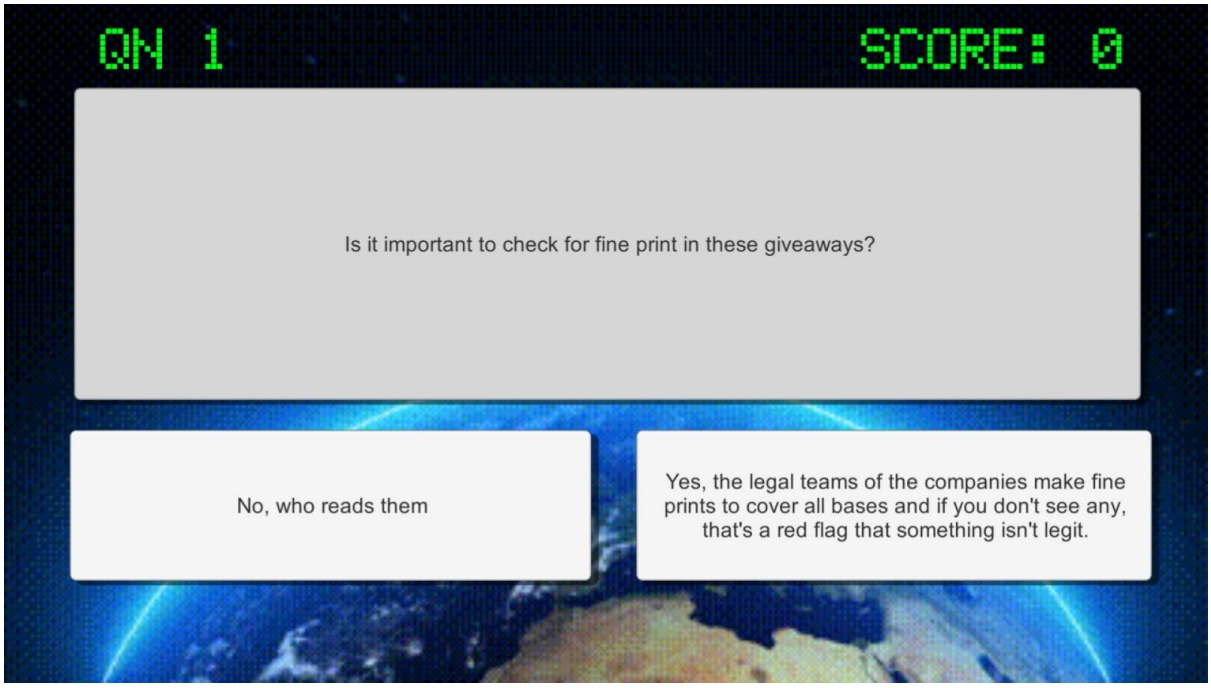

Figure 16: Game Interface, Game - Task 1 (Sample Quiz Interface)

If the user does not score full marks, they will be forced to retry as they will not be able to proceed to the next level.

Figure 17: Game Interface, Game - Task 1 (Sample Quiz Fail Page)

Users will only be able to continue to the next level of the game when they score full marks for the quiz.

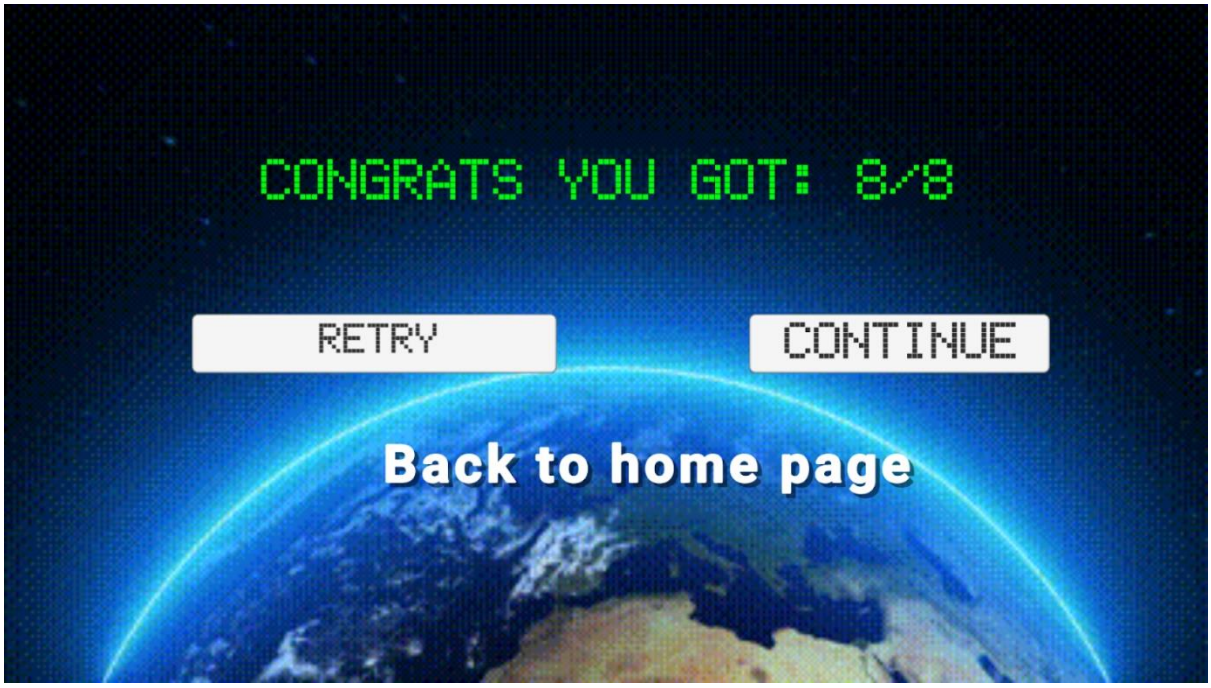

Figure 18: Game Interface, Game - Task 1 (Sample Quiz Pass Page)

3.5.2.2 Medium Level : Email Spoofing Scam

This will be the next level that the users will be playing after the giveaway scam game. Users will have to spot errors in the emails and click on them. Wrong clicks will lead to deduction of score points and will fail the round if insufficient points are attained in that round. There will be a total of 3 rounds for this game. This game requires users to be cautious and meticulous when reading emails so they can identify if the email is disguised as a scam.

As the email spoofing game is of a higher difficulty level, a tutorial is inserted before the start of the game.

Figure 19: Game Interface, Game - Task 2 (Welcome page)

The robot will walk the user through this tutorial.

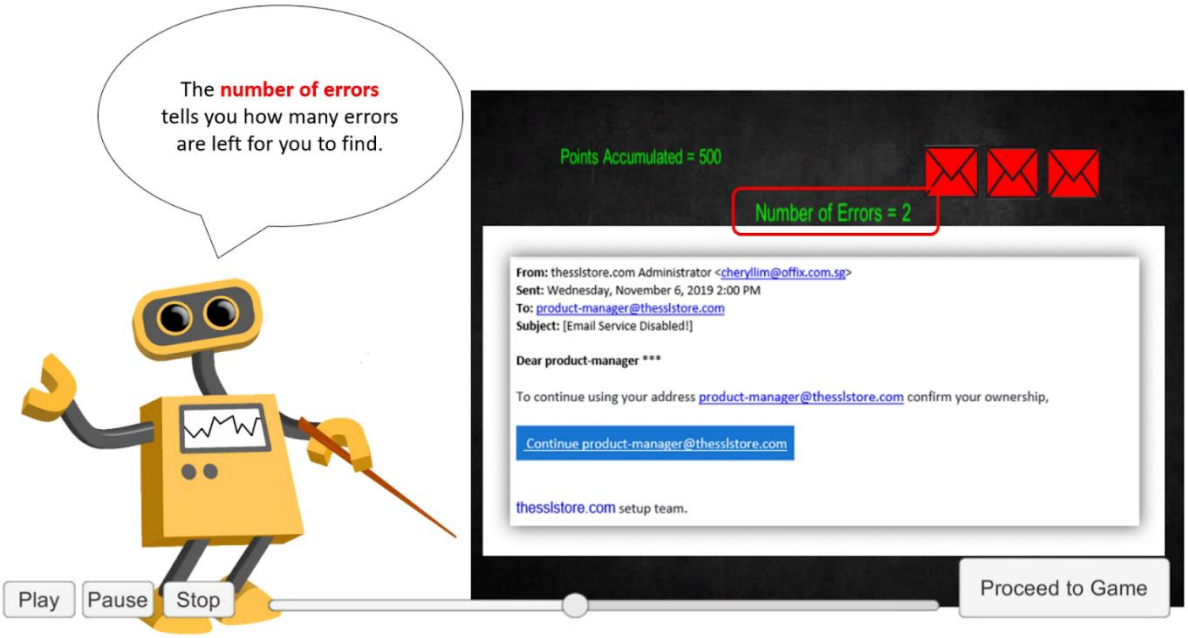

Figure 20: Game Interface, Game - Task 2 (Scene 1)

Users must attain sufficient points in a round to proceed to the next round.

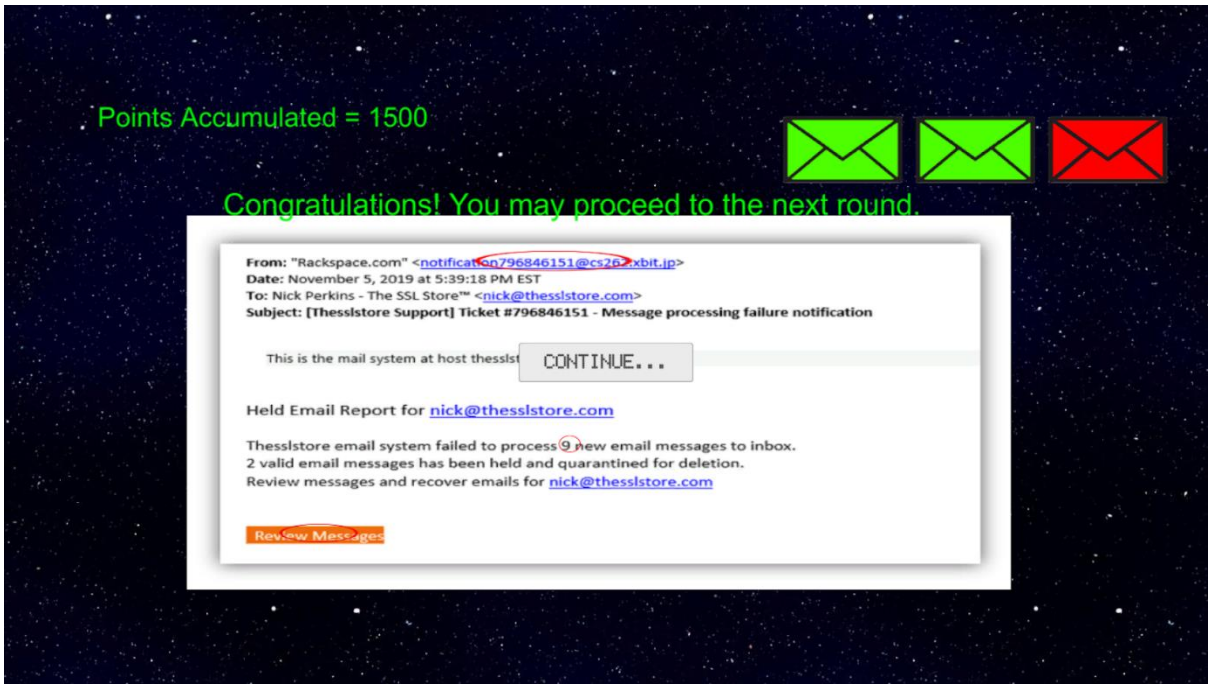

Figure 21: Game Interface, Game - Task 2 (Scene 2)

If the user does not attain sufficient points, they will have to retry that round.

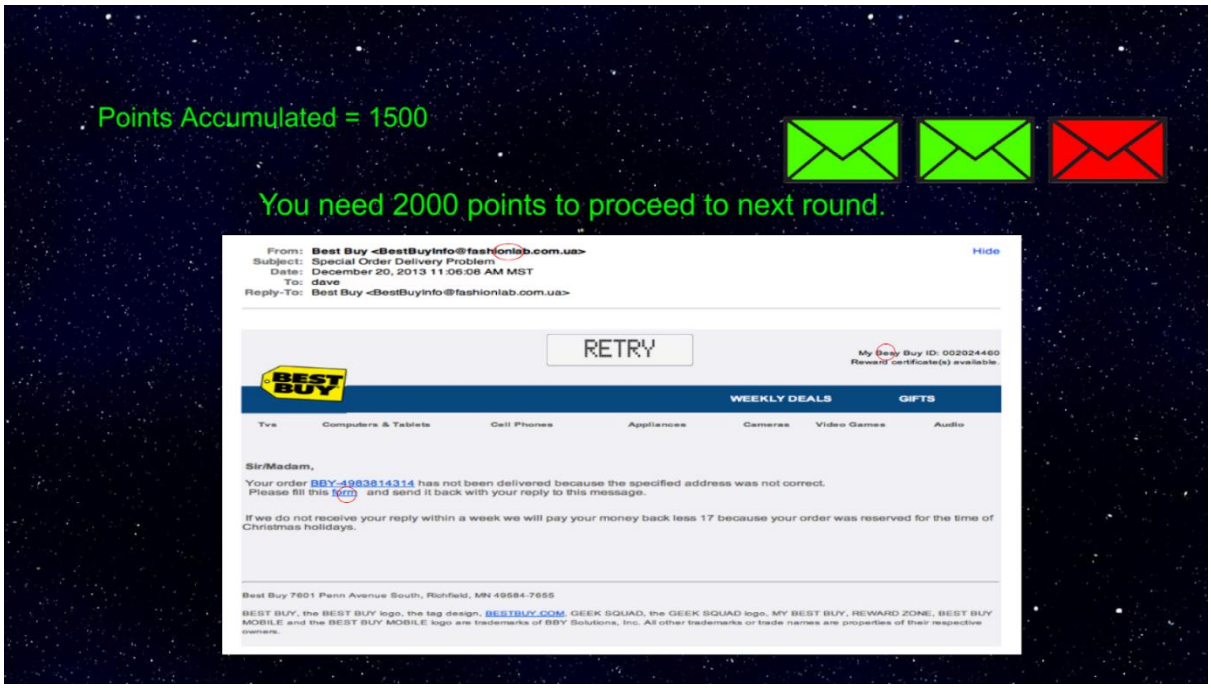

Figure 22: Game Interface, Game - Task 2 (Scene 3)

Similar to task 1, we will end the second game with a quiz with the same format. The email spoofing quiz will have 5 questions and the user must attain full marks to advance to the final level.

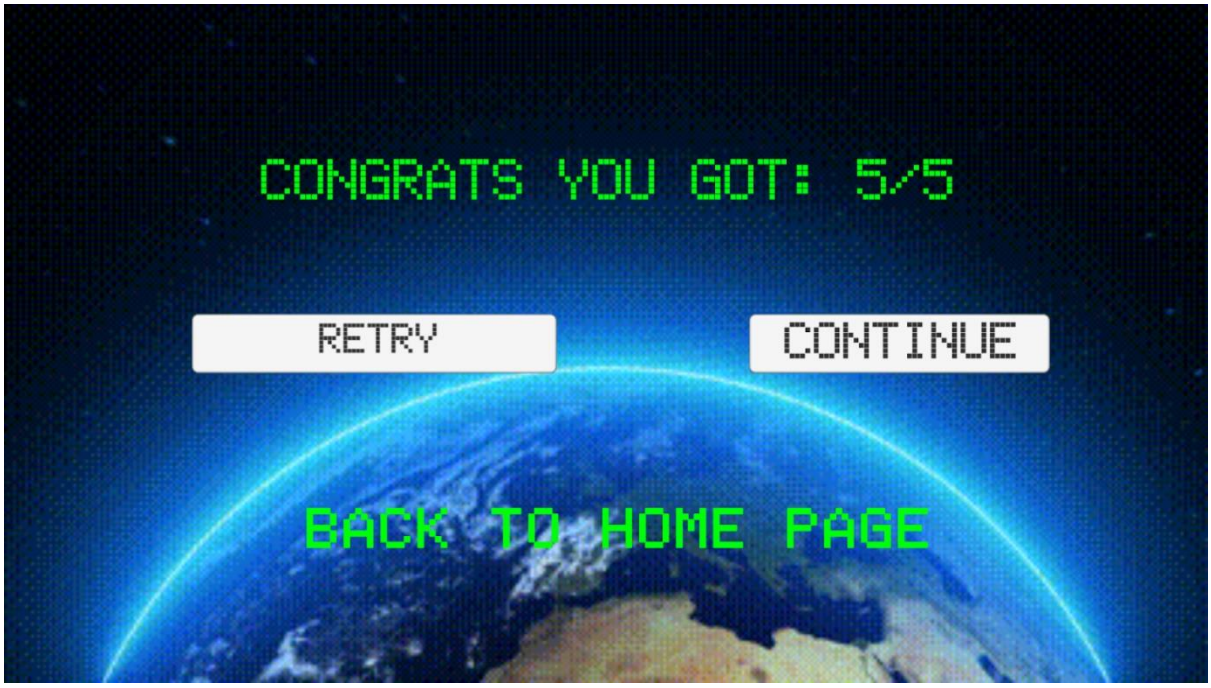

Figure 23: Game Interface, Game - Task 2 (Sample Quiz Pass Page)

3.5.2.3 Difficult Level : Tech Support Scam

Users must control the spaceship to avoid the tech support pop up advertisements. The main purpose of this game is to tell the players to always be cautious of pop-up advertisements and to always close them(in this game, to avoid the pop-ups) if they are unsure of the legitimacy of the advertisements. There will be no quiz for this section. This game is endless. Hence, players can continue to play this game for as long as they want to either beat their own high score or their friends' high score.

Likewise, there will be a tutorial for this game.

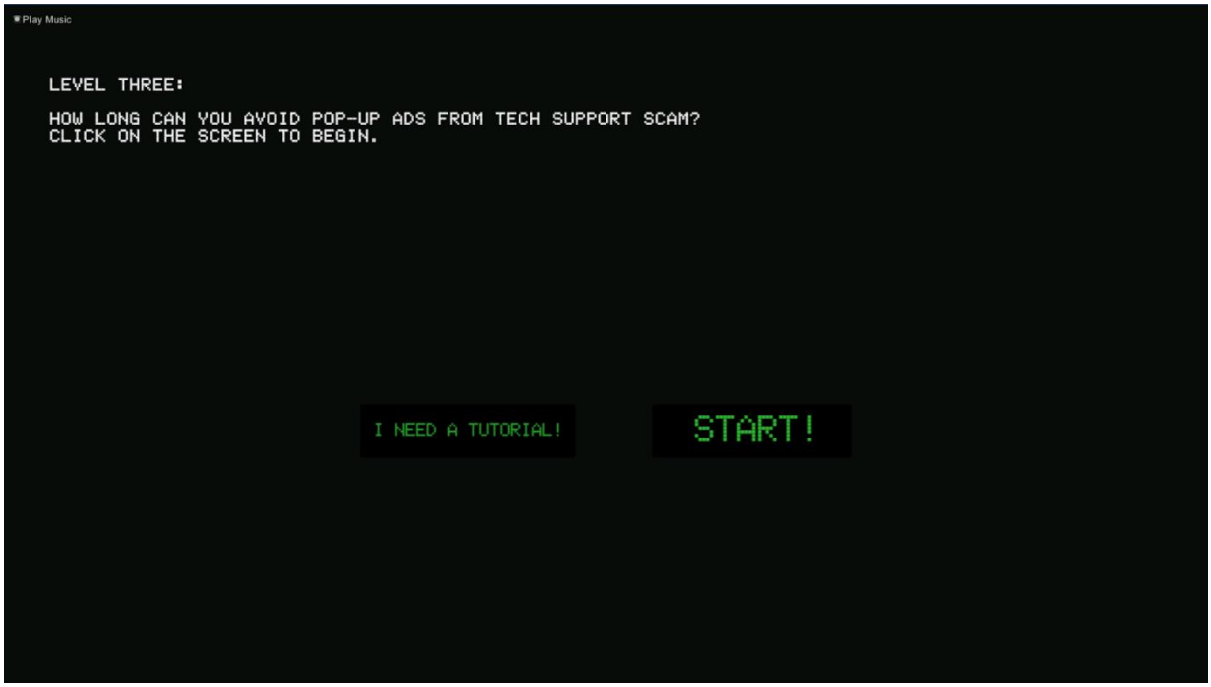

Figure 24: Game Interface, Game - Task 3 (Welcome page)

The gameplay is as shown here. Using the “up” and “down” arrow keys on the computer keyboard, users can control the movement of the spaceship either up or down to avoid the pop-up advertisements. The user is allowed to replay the game as many times as they like to beat their own high score.

Figure 25: Game Interface, Game - Task 3 (Infinite Run)

It will be game over when the spaceship hits a pop up.

Figure 26: Game Interface, Game - Task 3 (Infinite Run - High score)

3.5.3 Education Segment

Figure 27: Game Interface, Education

When the user selects the “Education” button, they will be given three types of videos to be viewed. The videos are selected according to the corresponding scams that we have replicated through this educational game. Hence users will be able to access these informative resources to learn more about what entails such social engineering attacks. We have attached and credited videos that we found provide information and details on the characteristics of each type of scam and the ways to avoid or prevent them.

Each type of scam that we have included in the game segment will have their own educational resources attached. The user will be free to select the type of scam that they wish to learn more about. They will not be restricted to any sequence to view the educational resources. For example, when the user clicks on the educational resources for the baiting attacks, an educational video will automatically start playing.

Figure 28: Game Interface, Education - (Main Menu)

After viewing each video, they will play a simple simulation game to learn and practice what they have learnt. There will be three simulation games in total from this education segment.

3.5.3.1 First video: Avoiding scams

The first button will direct the user to the first educational video, which is on the topic of how to avoid scams online. The video will be played. Users can either choose to play, to pause or to stop and can also toggle the knob at any point of time. Upon completing the video, the player will then be able to move to the first scene.

Figure 29: Game Interface, Education - (Giveaway Educational Video)

After watching the first video, users will be asked simple scenario questions. Depending on their selection, different scenarios will be shown.

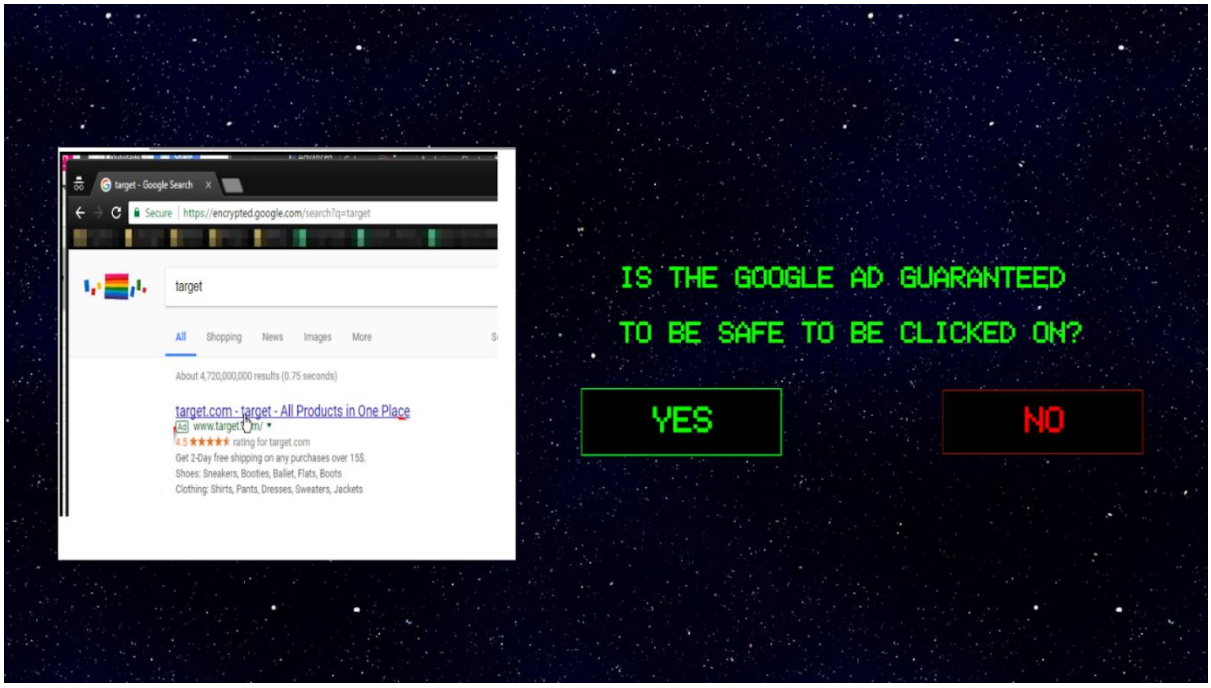

Figure 30: Game Interface, Education - (Scene 1)

If the correct option is selected, a positive scenario will be displayed, and they will be allowed to advance to the next scene.

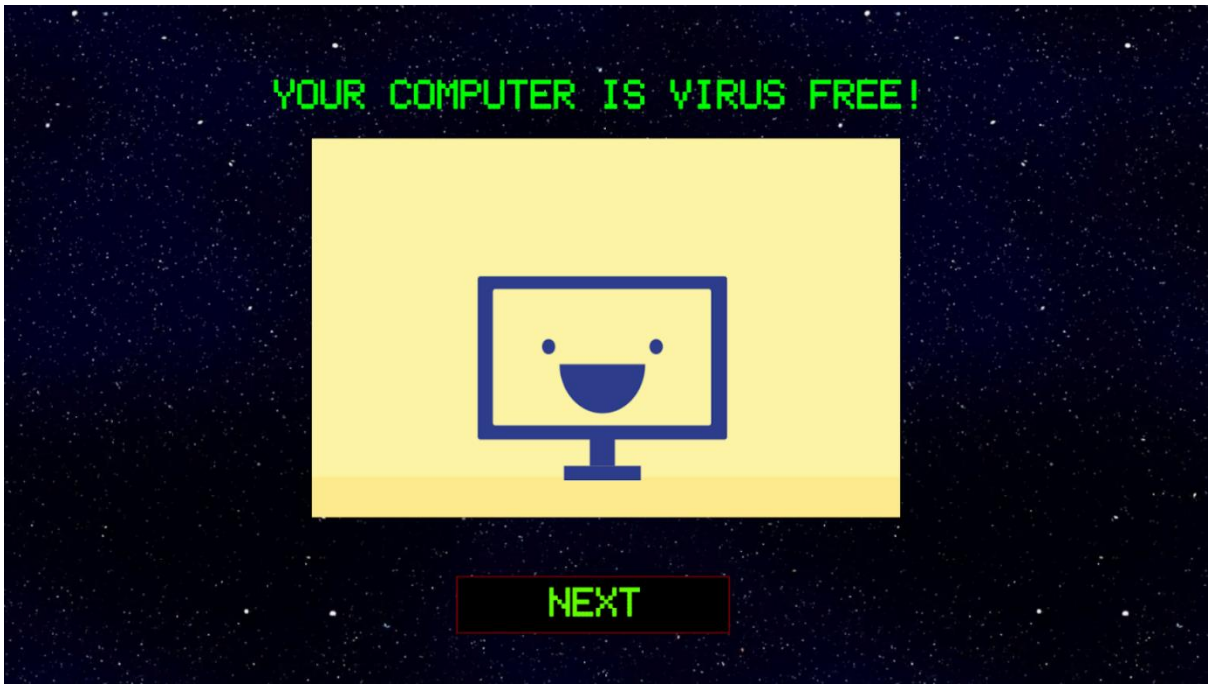

Figure 31: Game Interface, Education - (Part 1, Correct Choice)

However, if they have selected the wrong choice, a negative outcome will be displayed, and they will be forced to retry.

Figure 32: Game Interface, Education - (Part 1, Wrong Choice)

In between the scenes, depending on the options selected, some tips will also be displayed so users can learn more about the various scam tactics.

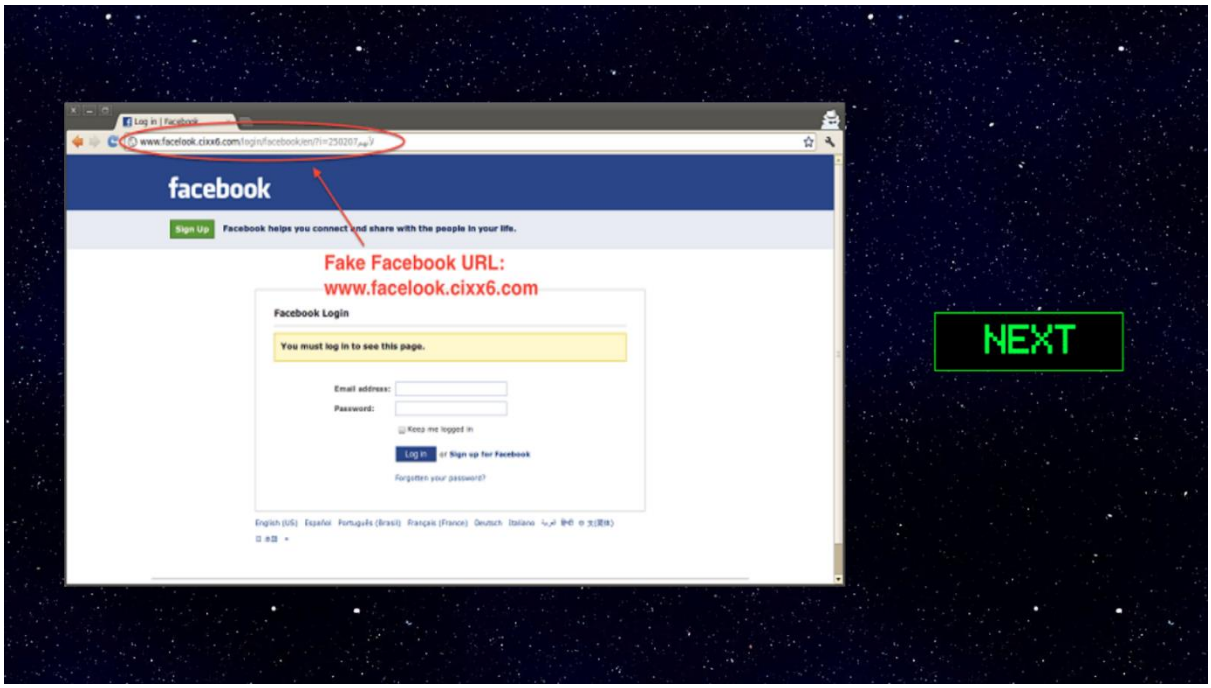

Figure 33: Game Interface, Education - (Part 1 - Tips Example 1)

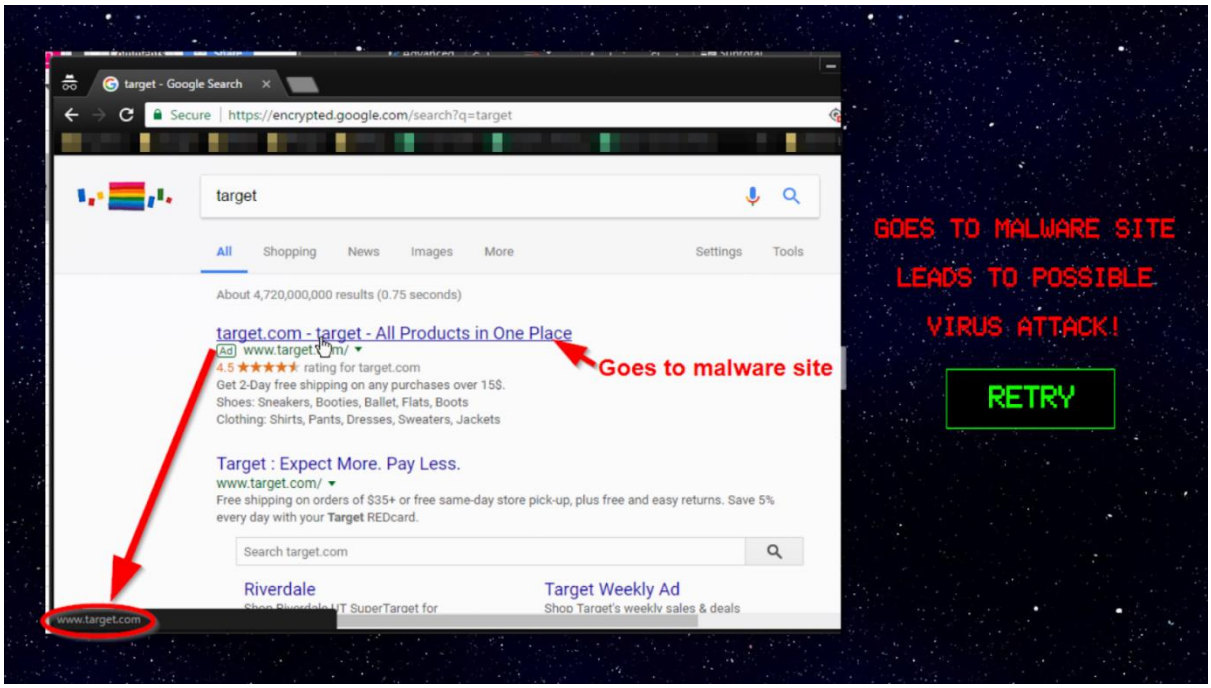

Figure 34: Game Interface, Education - (Part 1 - Tips Example 2)

Upon successful completion of the scenario-based game, they will be congratulated. There is a button at the top right corner that awards the player a certificate to showcase their achievement in learning what entails a social engineering attack.

Figure 35: Game Interface, Education - (Part 1 – Congratulations Scene)

Users can type in their real names into the input section "…type your name here…" and then save the certificate afterwards by pressing on the floppy disk at the bottom right-hand corner of the scene. This image will be retrievable in their respective user folders.

Figure 36: Game Interface, Education - (Part 1 – Certificate)

Figure 37: Game Interface, Certificate – Saving Image to Folder

A green text will pop up at the top of the scene, telling the user that the directory of the picture has been copied into their clipboard, and they will have to go onto their file explorer's directory box and paste it there in order to go to the access point of the image.

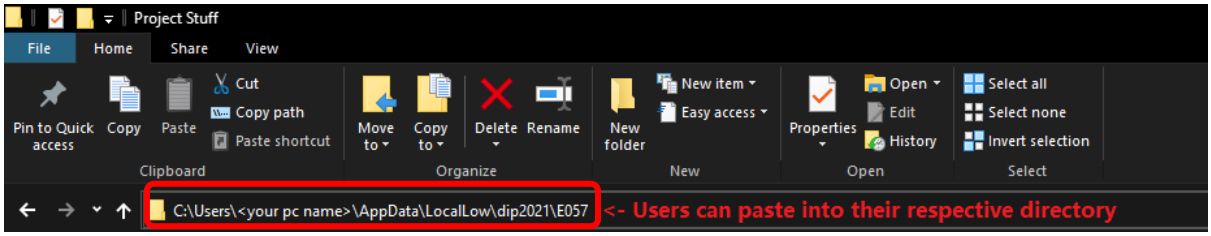

Figure 38: Game Interface, Certificate – Pasting Text into Directory

After pasting onto the box, the player will notice that there is a “<your pc name>” indication inside the text. The player is supposed to replace that part of the text to their actual PC user’s name. For example, if the PC’s name is called “jolen”, the player will need to key in that name into the text, as seen in the figure below.

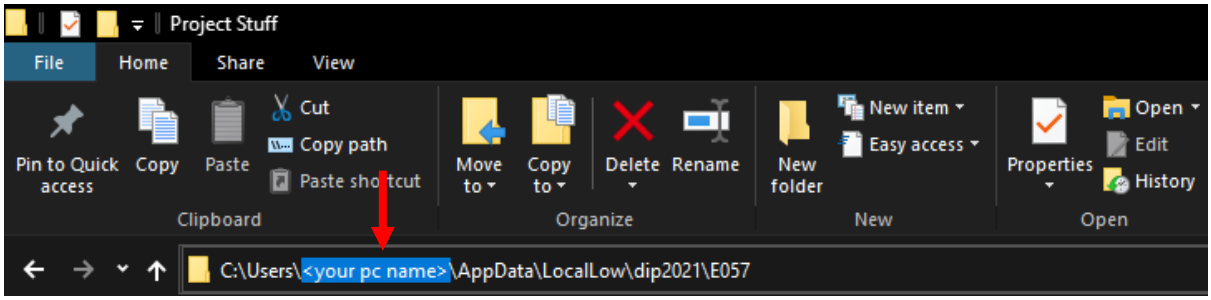

Figure 39: Game Interface, Certificate– Highlighted portion that must be amended by the player

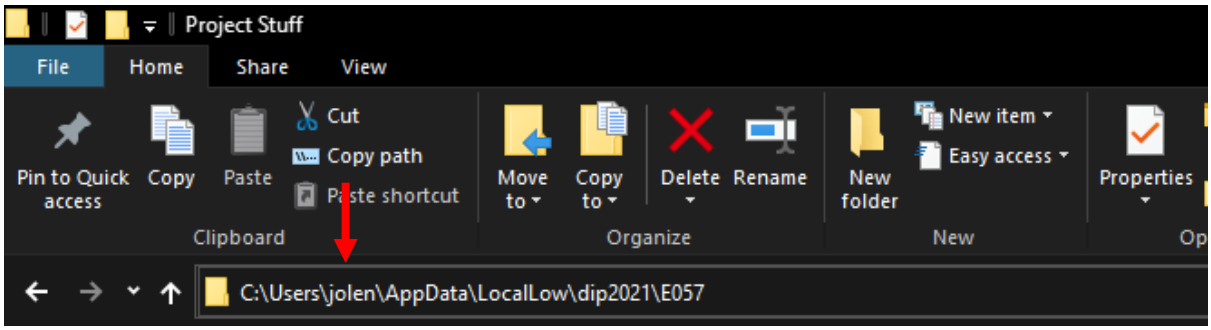

Figure 40: Game Interface, Certificate– After replacing the name with the PC user’s name

Once done, the player needs to press Enter key on the keyboard, and the user will be directed to this page. This means that the player has successfully entered the right directory for the game. The player will be able to see a image file(.PNG extension) that is titled “YourCertificate”. User can then click on that image to see their certificate.

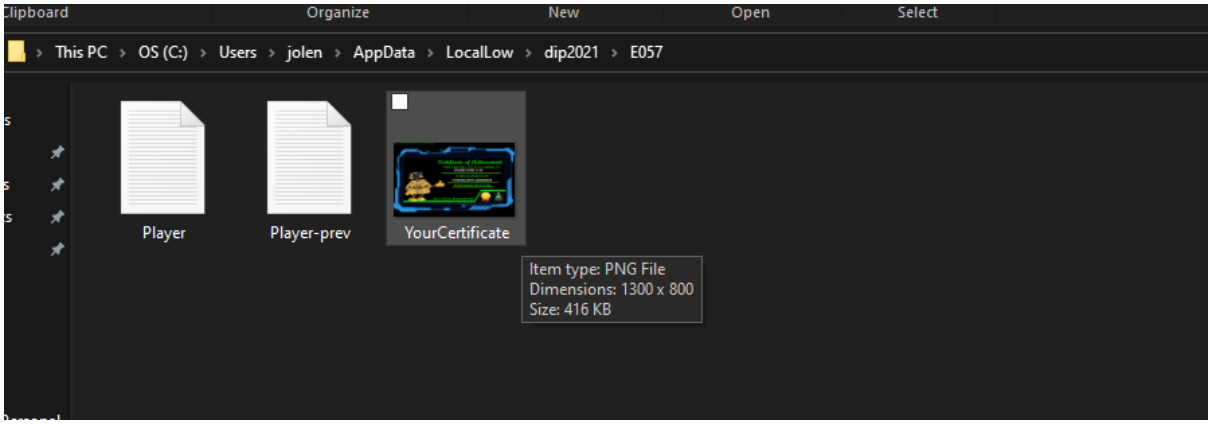

Figure 41: Game Interface, Certificate– Game Directory with "YourCertificate" image

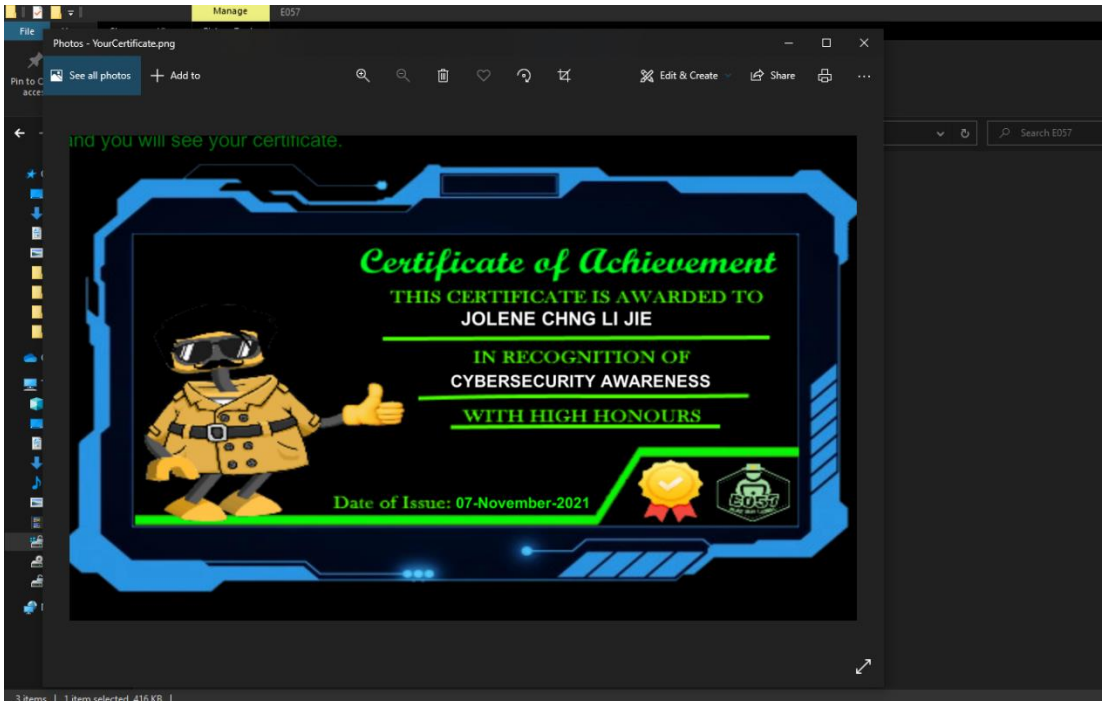

Figure 42: Game Interface, Certificate– Certificate of Player's Achievement in a printable PNG file

After the completion of the Giveaway scenario, the player can then revert to the Education Menu and can choose to proceed on to the next educational video under email spoofing.

3.5.3.2 Second video: Email Spoofing

Upon clicking onto the second button in the education menu, users will be redirected to the next form of social engineering attack – email spoofing. They will first watch the video that is done by one of our teammates, on the explanation of email spoofing. The video also comprises of a demo at the end that uses Virtual Box Machine to illustrate how email spoofing happens in real life scenarios.

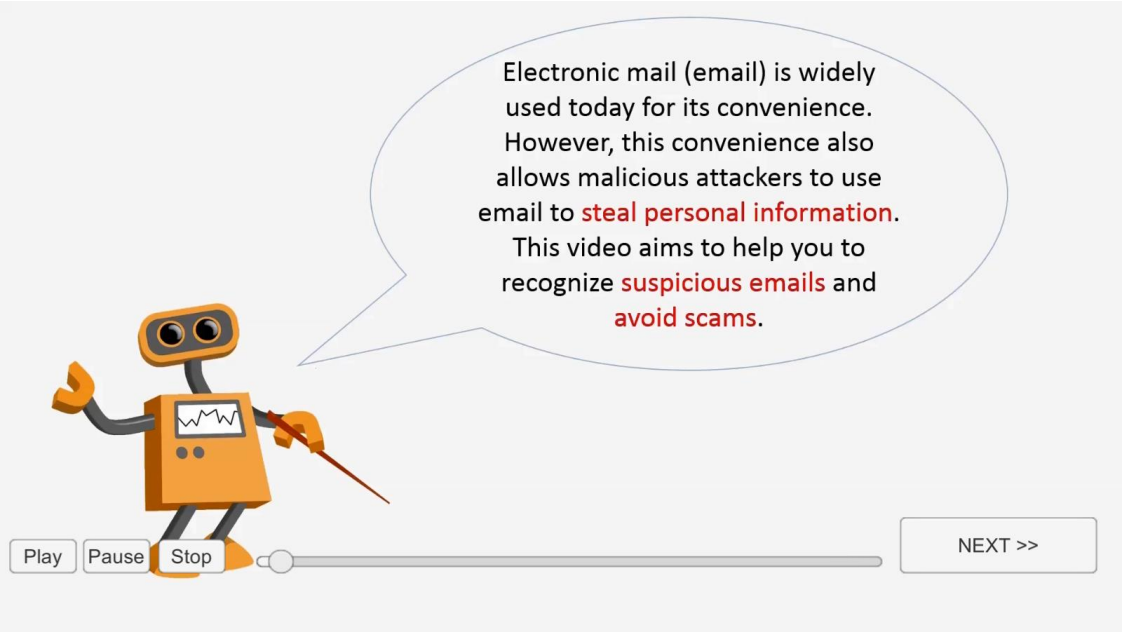

Figure 43: Game Interface, Education – (Email Spoofing Scam)

After watching the video, the player can then move on to the next part of the educational game. In the educational game, users will be exposed to three different scenarios. They will have to select the correct option to proceed to the next scenario.

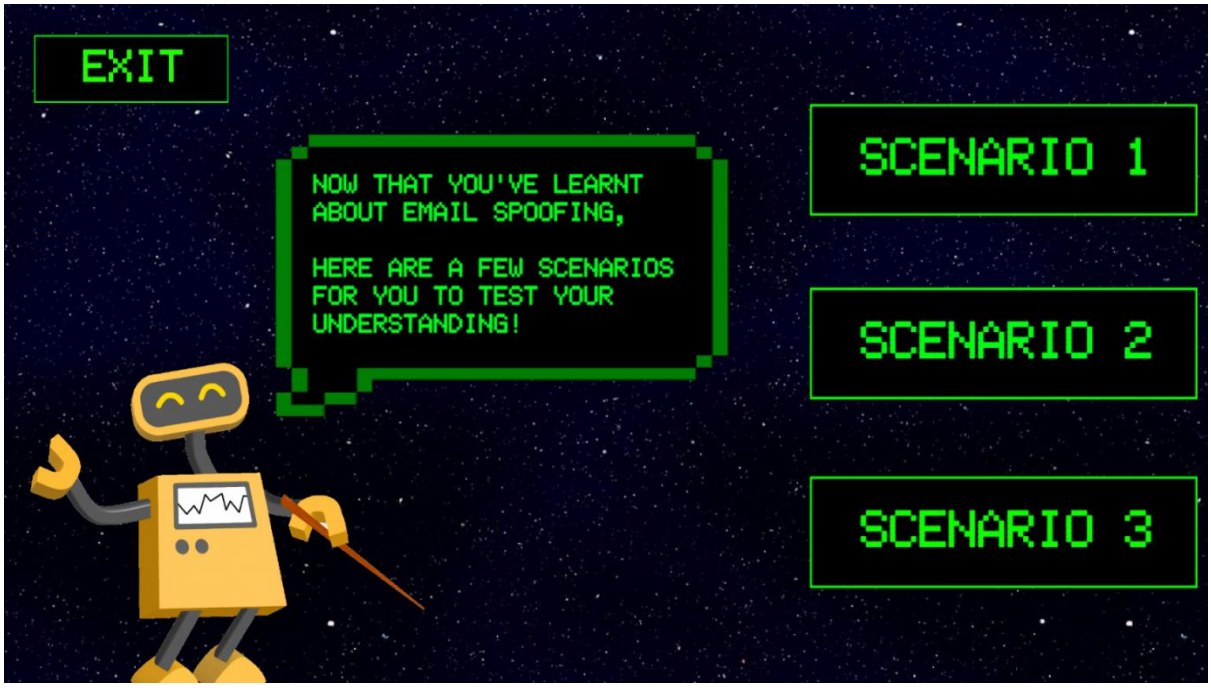

Figure 44: Game Interface, Education - (Part 2 - Homepage)

This is an example of one of the scenarios.

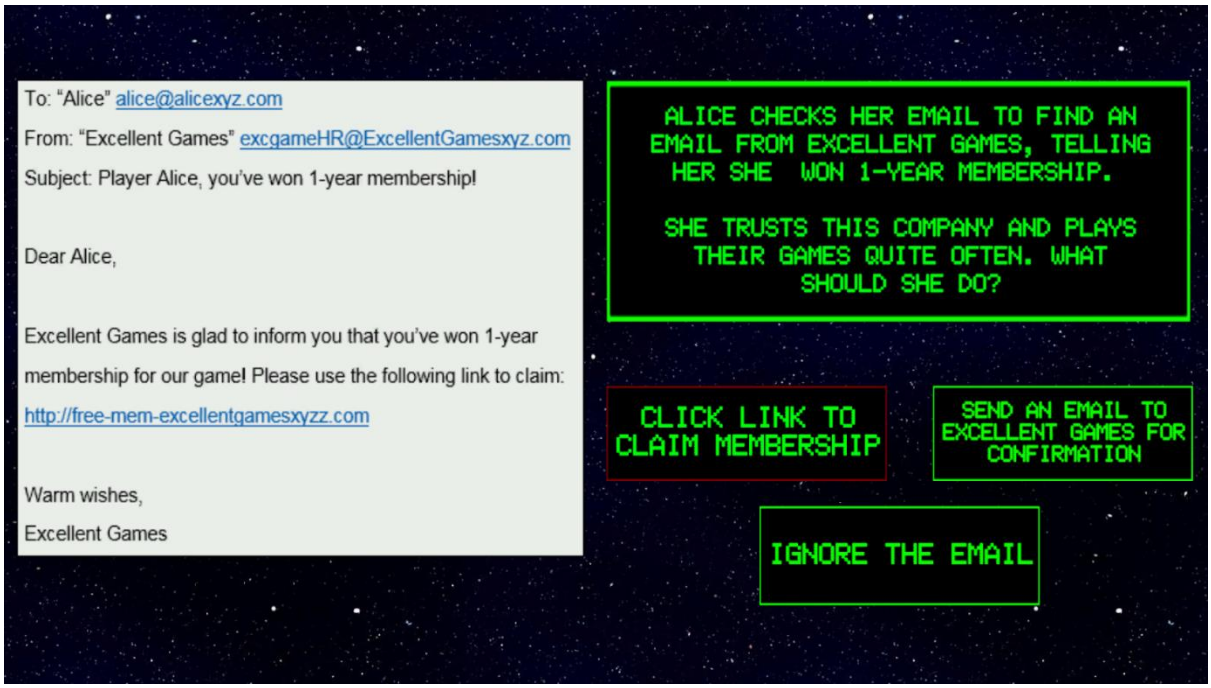

Figure 45: Game Interface, Education - (Part 2 - Scenario Example)

Different scenarios will be displayed based on the answer selected. Tips and reminders will also be shown to users to enhance the learning experiences.

Figure 46: Game Interface, Education - (Part 2 - Scenario Correct Choice)

Users will be encouraged to retry the scenario if they got the wrong option.

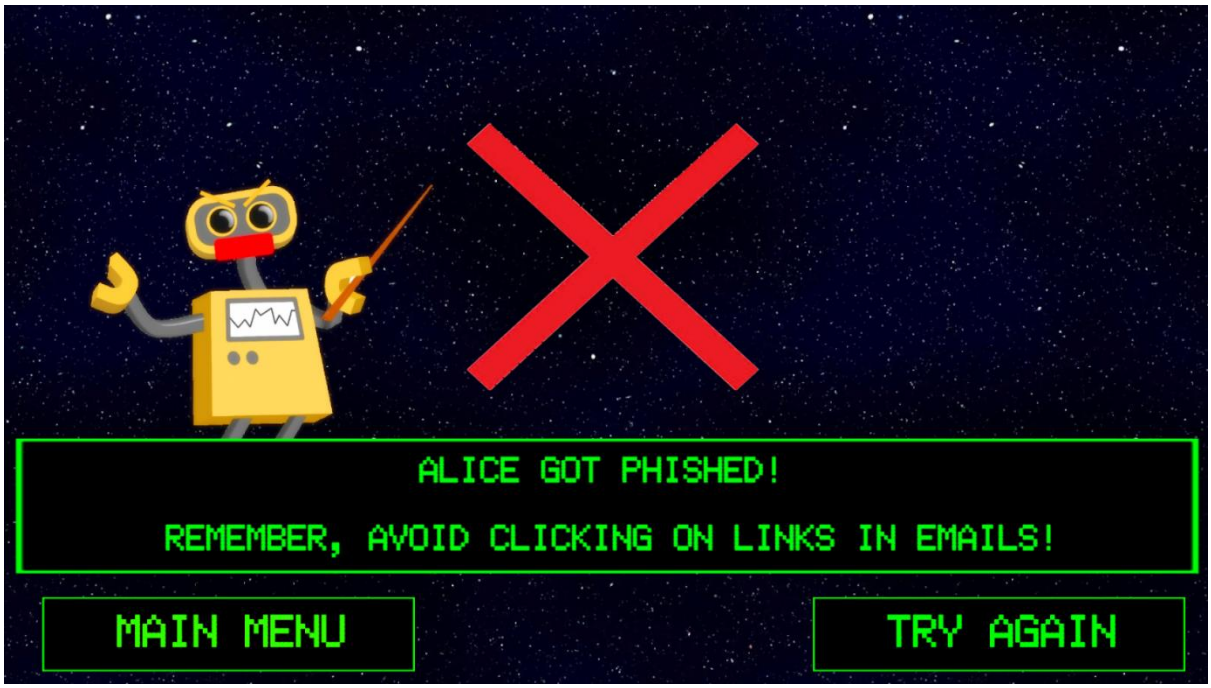

Figure 47: Game Interface, Education - (Part 2 - Scenario Wrong Choice)

When users successfully complete the three scenarios, they will be congratulated. Similarly, they will be awarded a certificate by clicking on the top right corner of the scene.

Figure 48: Game Interface, Education – Congratulatory Scene

Users can then click on the Main Menu button to go back to the Education Main page.

3.5.3.3 Third video: Tech Support Scam

Users will be placed in a situational game whereby the storyline is based on real life example, therefore giving a more realistic feel to it. Depending on the choices made by the user, it will bring them to different scenarios. Advice and information on how to tackle scams are also placed in this game. In this story, the user will be calling a person, “Marcus” for tech support due to issues with their computer.

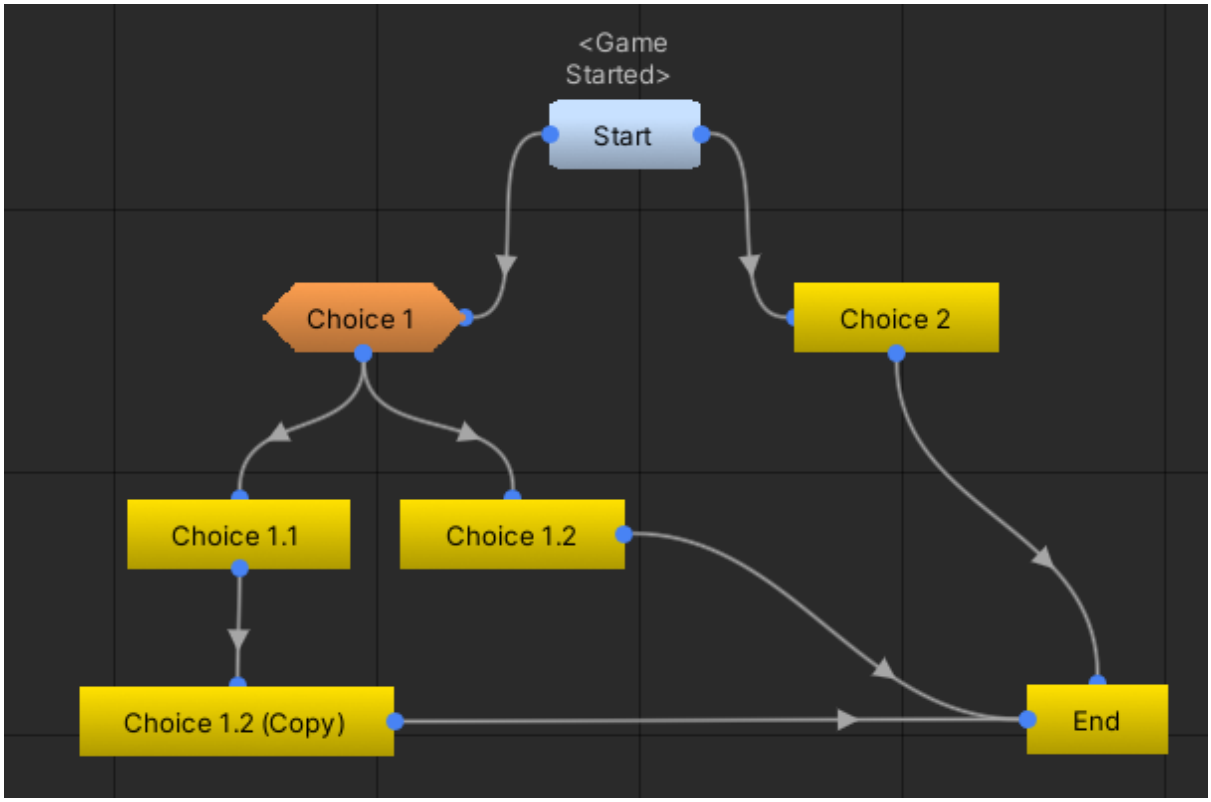

Figure 49: Game Interface, Education - (Part 3 - Overview Flowchart)

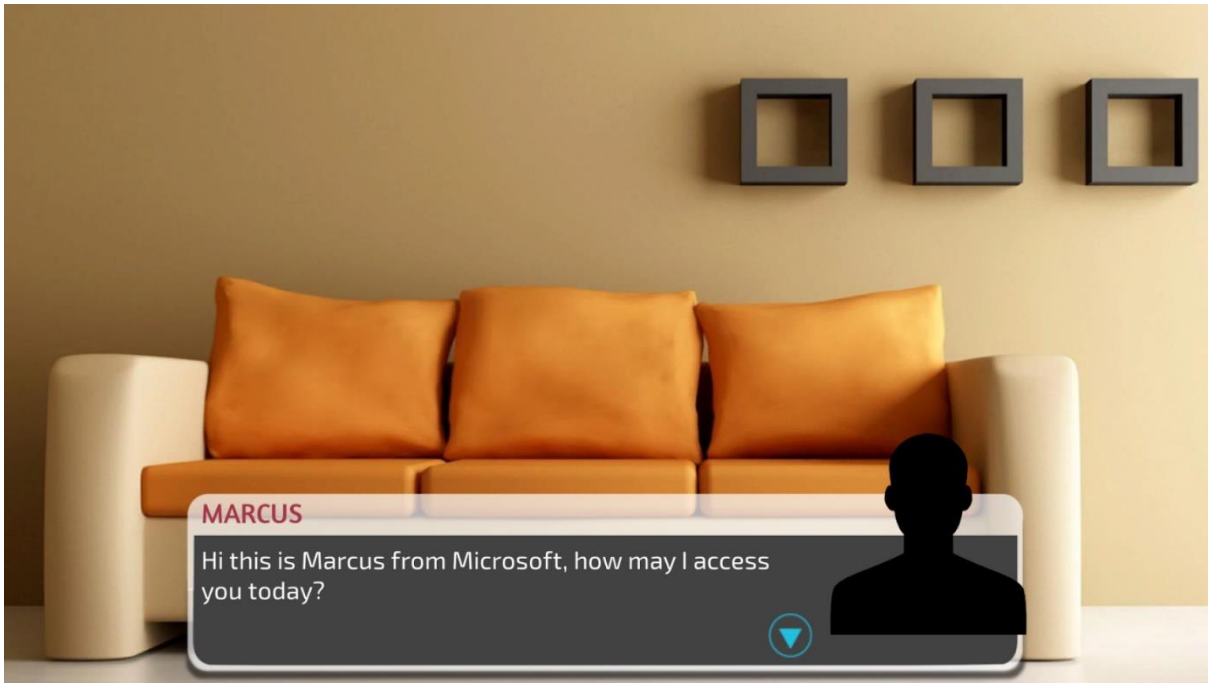

Figure 50: Game Interface, Education - (Part 3- Scenario Example 1)

Information on such scams will be dissipated in the storyline. This will enable the user to identify similar scams in the future as they have experienced such scams through this situational game.

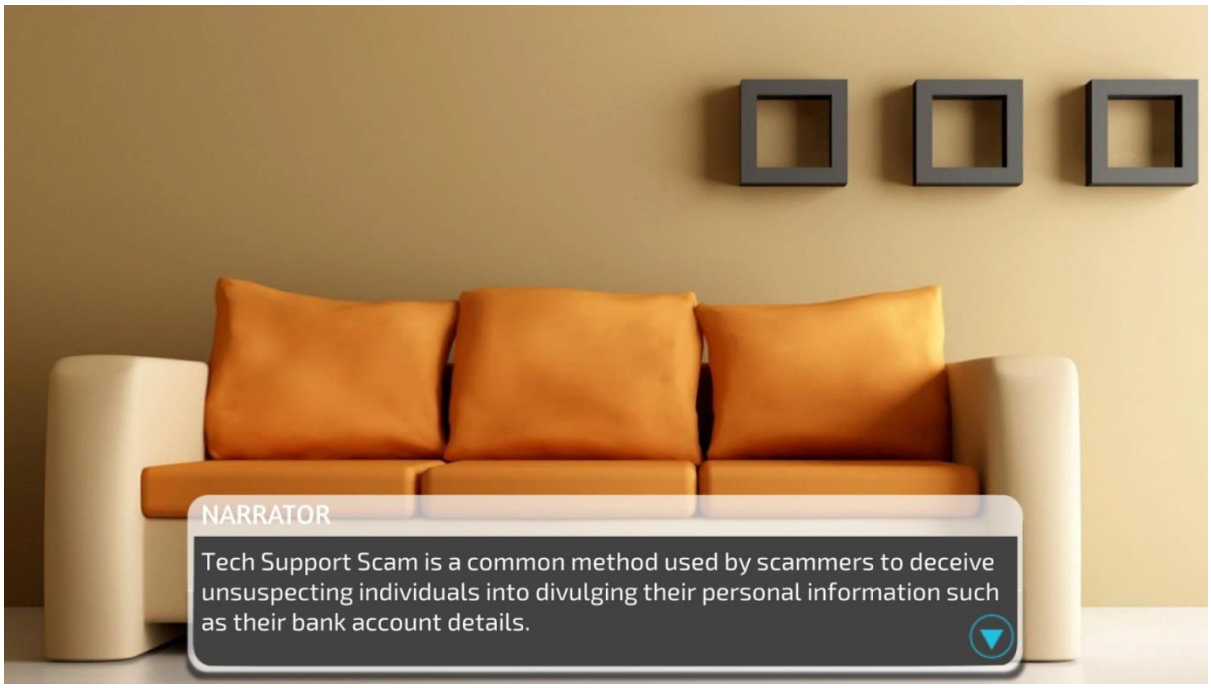

Figure 51: Game Interface, Education - (Part 3- Scenario Example 2)

Users will be given choices in this interactive gameplay. The storyline will evolve into different scenarios according to the options chosen by the user.

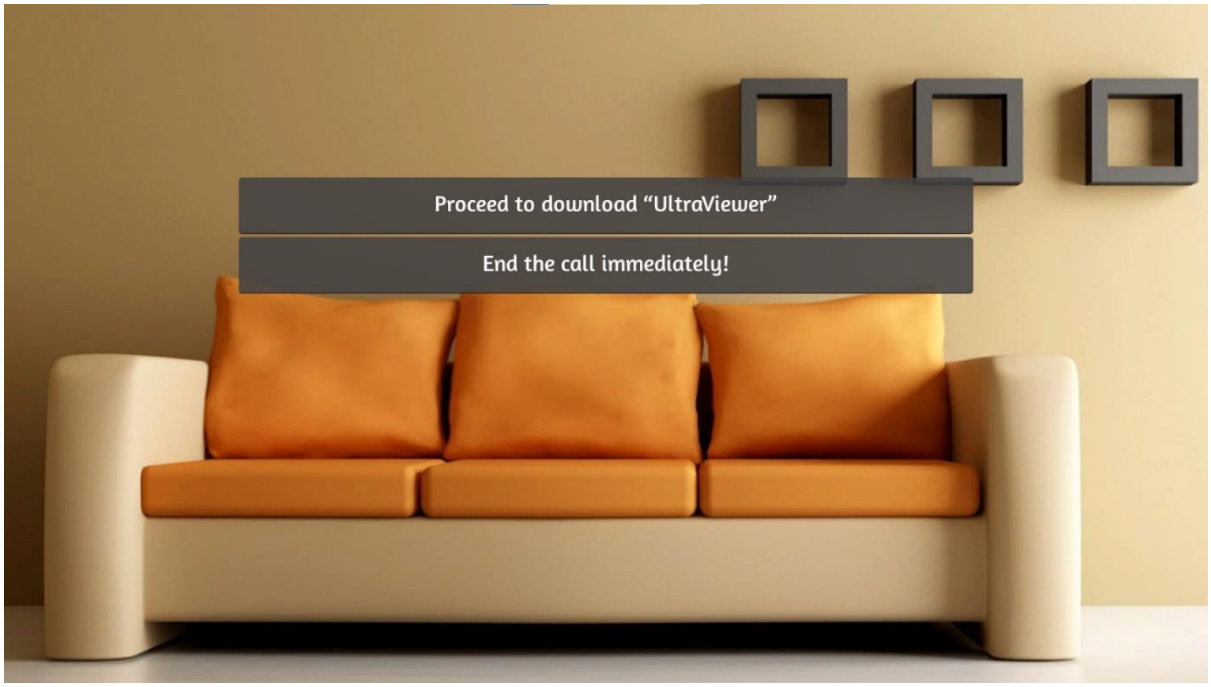

Figure 52: Game Interface, Education - (Part 3- Scenario Example 3)

After the user has gone through the storyline, additional tips will also be shown to teach users how to mitigate the situation. In addition, statistics on Online Tech Support Scam will also be shown to the user. This is to let the user know the severity of this issue and be more wary about it.

Prove of Certification

Figure 53: Game Interface, Prove of Certification

The user will be able to save the game by clicking on the floppy disk. The certificate is programmed in such a way that the “Date of Issue” will change according to the current date.

3.5.4 Credits

Users can also click on the “Credits” button, accessible under the Main Menu or Content screens to view the sources that are used in the game, as well as the producers of the game. This is also the section where we credit the sources used in the game that were gathered online, such as first and last educational videos.

Figure 54: Main Menu Interface, with Credits button at the left

Figure 55: Content Menu Interface, with Credits button at the bottom left corner

Figure 56: Credits Interface

3.6 Initial Drafts

3.6.1 Draft 1

In the initial stages of the project we did not specify on different segments for the game. We intended to combine both the games and the educational resources together. We also did not have a requirement for the users to follow a specific flow when they are using this interactive platform. When they choose to start the game, they will be given the choice to start on any game of their choice. Each game would then end with the educational resources and a quiz. The general flow of the interactive platform for Draft 1 is better illustrated below.

3.6.1.1 Changes made to Draft 1

We realized that splitting the educational resources and the games into two different segments would be better since it would prevent each game from being too lengthy. Having games that were too lengthy might reduce the motivation for the users

to complete each game. By not having any form of points system, there will also be less motivation for the users to complete all the games.

3.6.2 Draft 2

We then decided to split the platform into two main segments, the ‘Education’ and ‘Game’ segments. This way, users will be able to have more freedom to choose the section which they would be more interested in trying first. The attached educational resources based on the three types of scams will end with quizzes.

For the games segment, we removed the different levels for each game since it was not very feasible given our time constraints. The games did not have any specific sequence as well and the users were able to choose the games which they would like to try. The general breakdown of the interactive platform for this draft is shown below.

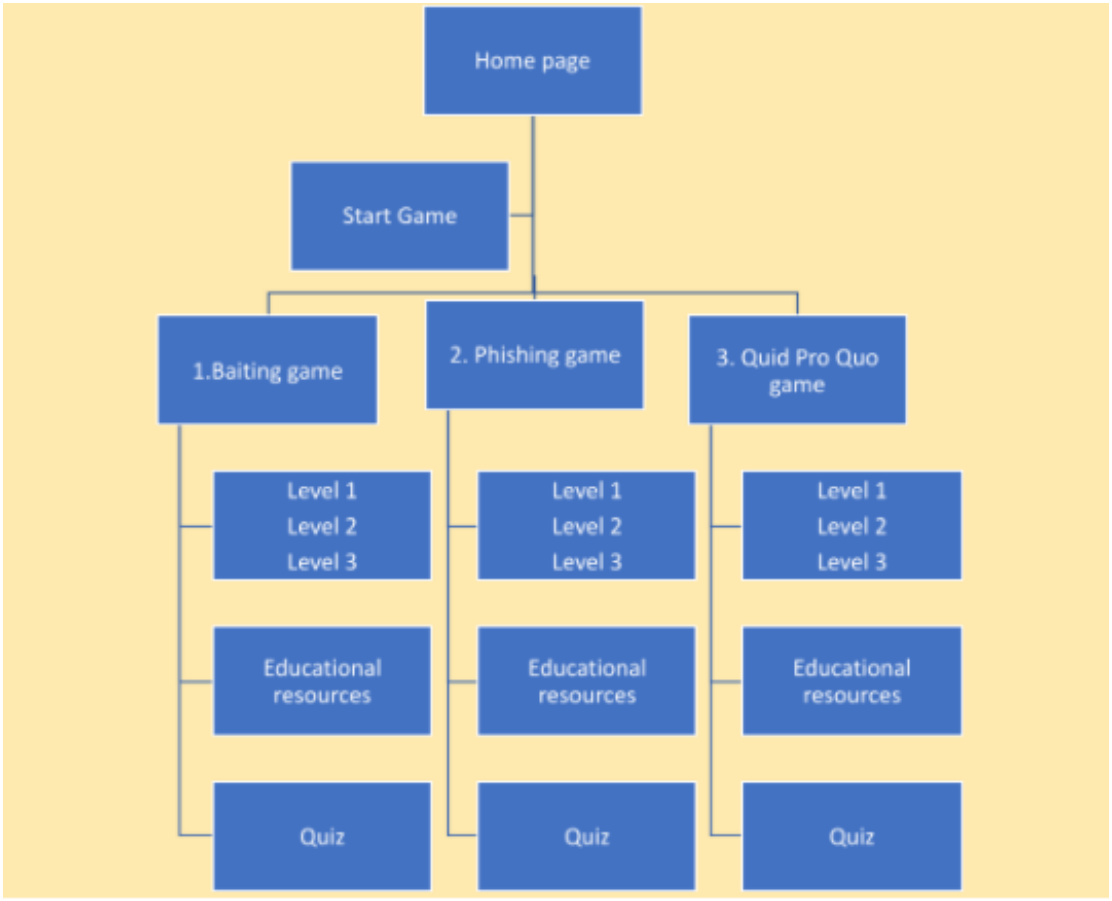

Figure 57: Flowchart - Draft 1

3.6.2.1 Changes made to Draft 2

We realized that our interactive platform is missing out on a motivational factor. Without a proper sequence for the users to follow, chances of the users completing all the games will definitely be much lower. Hence we have decided on arranging the different games in an order of increasing difficulty. Users will also be unable to proceed to the more difficult levels if they are unable to complete the current level which they are on. To increase the challenging aspect of each game, we also decided to relocate the quizzes. Instead of having them grouped with the educational resources, we decided to place quizzes after every game. With the users being required to answer all the questions correctly, they will be able to proceed to the next level. Not being able to have a preview of the next level also contributes to the suspense of the entire interactive platform

In order to increase competitiveness, we also decided to incorporate a points system on top of the above-mentioned content. Mistakes will result in points deductions and successful completion of games and quizzes will lead to point additions. A login page is included to allow users to save their previous high scores. This way, the users will be more motivated to complete all the different segments of the interactive platform

Figure 58: Flowchart - Final

3.6.3 Conclusion

After making the necessary changes to the game structure, we were able to achieve an interactive platform that not only provided a unique and effective learning experience through games, but also provided educational resources for users to access at their own time.

4. Schedule

PHASE	Planned Milestone Date	Actual Milestone Date
Initiating Phase	Week 1 – 2	Week 1 – 2
Planning Phase	Week 3 – 4	Week 3 – 4
Execution Phase	Week 5 – 11	Week 5 – 11

Closing Phase	Week 12 – 13	Week 12
Project End Date	Week 13	Week 13

Table 1: Overall Project Schedule

As seen from the table above, we were able to keep up to our schedule, and was in fact ahead of the plan. This was because everyone was able to complete their designated tasks on time. We also held meetings every week to discuss about each other's workload and seek for help among the teammates whenever needed.

5. Costs

As our product mainly uses a free software known as Unity, we did not incur any sort of monetary costs in this project.

6. Recommended for Future Work

In future work, we hope to code a workable online leader board that can constantly update itself everyday in order to increase the competitiveness of the game. We also want to increase more levels and difficulties for the three respective games. In order to increase the attractiveness of the game, we could also let users dress up their E057 robots with clothes that could be bought with coins that are earned from the games. Another possible idea that we could place into the game is a monitored chat box, or a forum that allows players to communicate with each other. Without any time constraints, we believe that these functions are possible to be featured in our game in the future if we choose to continue to work on the project.

7. Reflection

7.1 Engineering Knowledge

Even though many social engineering scams do not include elaborate tactics, this project still utilized much of the engineering knowledge and skill sets that were imparted to us through the course. Debugging and good coding habits allowed for us

to be able to troubleshoot in a more efficient and organized manner. By having prior knowledge to basic coding, we were also able to develop the game more smoothly.

We also made use of many online resources and tutorials to assist us in the understanding of Unity. We can better understand the issues we faced with designing the platform and were also able to plan for future drafts of the project more holistically.

For email spoofing, we used Virtual Machines with Oracle VM VirtualBox to send spoofed emails to each other, connected via a local server. We used Ubuntu as OS for the VMs and set up email servers in each of the VMs to simulate actual spoofed emails.

7.2 Problem Analysis

There were many challenges which we encountered along the way, many of which we were able to overcome through more careful planning of the platform structure and the objective which we wanted to achieve.

For instance, the initial drafts of the interactive platform would be able to run smoothly in theory. However, in practice the platform did not have a motivational factor or fun element which would encourage users to fully experience the platform. Since our objective is to raise awareness about such social engineering attacks in a unique way, our platform must be structured and planned well. Without doing so the interactive platform would only be an information site with some scenarios being included. By analysing other games and interactive platforms, we were able to identify the various changes that were required to be made.

8. References

Chee, K. (17 September, 2021). *More tech support scams targeting Singapore consumers: Microsoft*. Retrieved from The Straits Times: https://www.straitstimes.com/tech/tech-news/more-tech-support-scams-targeting-singapore-consumers-microsoft

Davis, J. (7 July, 2020). *Magellan Health Data Breach Victim Tally Reaches 365K Patients*. Retrieved from Health IT Security: https://healthitsecurity.com/news/magellan-health-data-breach-victim-tally-reaches-365k-patients

Leswing, K. (15 July, 2020). *Hackers targeted Twitter employees to hijack accounts of Elon Musk, Joe Biden and others in digital currency scam*. Retrieved from CNBC: https://www.cnbc.com/2020/07/15/hackers-appear-to-target-twitter-accounts-of-elon-musk-bill-gates-others-in-digital-currency-scam.html

Sethi, S. S., & Pek, C. (22 July, 2021). *Tech support scams remain a threat globally and in Asia Pacific despite drop in encounters: Microsoft survey*. Retrieved from Microsoft: https://news.microsoft.com/apac/2021/07/22/tech-support-scams-remain-a-threat-globally-and-in-asia-pacific-despite-drop-in-encounters-microsoft-survey/

Ward, C., & Pritam, N. (19 May, 2020). *Money makes the cyber-crime world go round - Verizon Business 2020 Data Breach Investigations Report*. Retrieved from Verizon: https://www.verizon.com/about/news/verizon-2020-data-breach-investigations-report

Yik, W., & Woo, J. (17 September, 2021). *Six in ten consumers in Singapore have been targeted by tech support scams in the last 12 months: Microsoft survey*. Retrieved from Microsoft: https://news.microsoft.com/en-sg/2021/09/17/six-in-ten-consumers-in-singapore-have-been-targeted-by-tech-support-scams-in-the-last-12-months-microsoft-survey/

Appendices

Appendix A - Project Members Information

	Name	Project contributions	Report Contribution
1	Jolene Chng Li Jie	Group Leader, Game Developer, UI Designer, Final Project Integration, Group Report Editor, Simulation, Group Blog	1. Formatting of the report, adding section numbers, page numbers. 2. Scope (Chapt 3.5.3.1, Pg 29, 32-35. Chapt 3.5.3.2, Pg 36. Chapt 3.5.4, Pg 42-44) 3. Schedule (Chapt 4, Pg 47-48) 4. Recommended for Future Works (Chapt 5, 6 Pg 48) 5. Appendices A & B (Pg 52)
2	Pang Yi Wei	Treasurer, Game Developer, UI Designer, Group Report Editor, Simulation, Group Blog	1. Scope (Chapt 3.5.3.3, Pg 39-42) 2. Formatting of figure numbers from Figure 1 to Figure 58
3	Kuan Soon Yee	Virtual Machine Developer, Video Developer, Story Developer, Simulation, Group Report Editor, Group Blog	1. Reflection (Chapt 7, Pg 49) 2. Codes Submission (Appendix C, GitHub codes in Pg 51)
4	Lee Lin Sophia	Group Report Leader, Story Developer, Trade Studies, Researcher, Group Blog	1. Oversees the flow and soundness of the report 2. Purpose (Chapt 1, Pg 3-5) 3. Project Summary (Chapt 2, Pg 6) 4. Scope (Chapt 3.1, 3.2, 3.3, 3.4, Pg 7-11) 5. Reflection (Chapt 7, Pg 48-49) 6. References (Chapt 8, Pg 50)
5	Phang Rei Xuan Rachel	Game Developer, Simulation, Story Developer, Group Report Editor, Group Blog	1. Scope (Chapt 3.5.1, 3.5.2, 3.5.3, 3.5, 3.6, Pg 13-31, 37-39 & Chapt 3.6, Pg 44-47) 2. Crafting out of Draft Plans 1 and 2 in Flowchart, Pg 45, 47 (Figs 57, 58)

Appendix B – Subgroup Members List

Team A: Script Writers, Story Developers	Kuan Soon Yee, Lee Lin Sophia, Phang Rei Xuan Rachel
Team B: Game Developers, Animators	Jolene Chng Li Jie, Pang Yi Wei

Appendix C – Game Codes

1. Email Spoofing – ttps://github.com/lunarca/SimpleEmailSpoofer
2. E057 Project - https://github.com/nubc4kez/E057