

**A Preliminary Propagation Tool in Social Engineering Attacks**

BY

Peggy Hoong

A REPORT

SUBMITTED TO

Universiti Tunku Abdul Rahman

In partial fulfillment of the requirements

for the degree of

BACHELOR OF INFORMATION SYSTEMS (HONOURS)

COMMUNICATION AND NETWORKING

Faculty of Information and Communication Technology

(Kampar Campus)

JAN 2021

UNIVERSITI TUNKU ABDUL RAHMAN

**REPORT STATUS DECLARATION FORM**

**Title:** A Preliminary Propagation Tool in Social Engineering Attacks

\_\_\_\_\_  
\_\_\_\_\_

**Academic Session:** JAN2021

\_\_\_\_\_  
PEGGY HOONG

(CAPITAL LETTER)

declare that I allow this Final Year Project Report to be kept in  
Universiti Tunku Abdul Rahman Library subject to the regulations as follows:

1. The dissertation is a property of the Library.
2. The Library is allowed to make copies of this dissertation for academic purposes.

Verified by,



\_\_\_\_\_  
(Author's signature)



\_\_\_\_\_  
(Supervisor's signature)

**Address:**

28, Lorong Simpang Bersatu 8,  
Taman Simpang Bersatu  
34700 Simpang Perak.

Dr Vasaki a/p Ponnusamy

\_\_\_\_\_  
Supervisor's name

**Date:** 6<sup>th</sup> April 2021

**Date:** 6<sup>th</sup> April 2021

**A Preliminary Propagation Tool in Social Engineering Attacks**

BY

Peggy Hoong

A REPORT

SUBMITTED TO

Universiti Tunku Abdul Rahman

In partial fulfillment of the requirements

for the degree of

BACHELOR OF INFORMATION SYSTEMS (HONOURS)

COMMUNICATION AND NETWORKING


Faculty of Information and Communication Technology

(Kampar Campus)

JAN 2021

## DECLARATION OF ORIGINALITY

I declare that this report entitled “**A Preliminary Propagation Tool in Social Engineering Attacks**” is my own work except as cited in the references. The report has not been accepted for any degree and is not being submitted concurrently in candidature for any degree or other award.

Signature :  \_\_\_\_\_

Name : Peggy Hoong

Date : 5<sup>th</sup> April 2021

## **ACKNOWLEDGEMENTS**

I would like to express my sincere thanks and appreciation to my supervisor, Ts Dr Vasaki a/p Ponnusamy and my moderator Dr Robithoh Annur who has given me this bright opportunity to engage in this project involves Social Engineering Attack Awareness tool project. It is my first step to establish a career in AI field. A million thanks to both.

Special thanks to Ts Dr Vasaki a/p Ponnusamy, for her patience, and passionate in teaching and unconditional support, and advising and guiding me throughout this project. Besides that, she has given me a lot of encouragement and motivation during the development of project. This is important to me when I feel stressful or loss direction, she is the one who always support me and guide me to the correct direction.

Finally, I must say thanks to my parents and my family for their love, unconditional support and continuous encouragement throughout the course.

## **ABSTRACT**

Information security is one of the growing sources of concern and should know how dealing with today. Levels of sophistication of social engineering threats and the exploits from such attacks are evolving. In particular, the lack of social engineering awareness is a concern in the context of human cyber security risks. There are some of the challenges that encounter in the process of developing the human knowledge to fight against social engineering attacks. A detailed literature review is provided to support these arguments with analysis of contemporary approaches. Based on literature review, strengths and weaknesses of different method of awareness had been carried out. This study highlights the weaknesses of previous projects, the project plan is to develop a tool to let user able to understand the social engineering with some fun games. In the market, there are many SEAP but there do not have such social engineering attack awareness tool. There is limitation for people in different countries to purposely travel just to join the awareness program. As social engineering is gaining popularity there days, the awareness of the security breaches is significant in order to decrease the cyber security cases, avoid been target as victim with resulting huge financial and human losses. Awareness tools which provide the same working strategies as SEAP but in different form to carry out by make use of this advance technology nowadays.

## TABLE OF CONTENTS

**TITLE PAGE**

**DECLARATION OF ORIGINALITY**

**ACKNOWLEDGEMENTS**

**ABSTRACT**

**TABLE OF CONTENTS** **i**

**LIST OF FIGURES** **iii**

**LIST OF TABLES** **x**

**LIST OF ABBREVIATIONS** **xi**

**CHAPTER 1 INTRODUCTION** **1**

**1.1 Problem Statement** **1**

**1.2 Background and Motivation** **2**

**1.3 Project Objectives** **5**

**1.4 Proposed Approach/Study** **6**

**1.5 Highlight of what have been achieved** **6**

**1.6 Report Organization** **7**

**CHAPTER 2 LITERATURE REVIEW** **8**

**2.1 Chapter Overview** **8**

**2.2.1 A Serious Game for Eliciting Social Engineering Security Requirements** **8**

**2.2.2 Security awareness escape room – a possible new method in improving security awareness of users** **17**

**2.2.3 A model for social engineering awareness program for schools** **21**

**CHAPTER 3 SYSTEM DESIGN** **30**

**3.1 Chapter Overview** **30**

**3.2 Design Specifications** **30**

**3.2.1 Propose Method** **30**

**3.2.2 Tools to use** **34**

**3.2.3 System Performance Definition** **34**

**3.2.4 Verification Plan** **35**

**3.3 System Design** **42**

**3.4 Implementation Issues and Challenges** **49**

<b>CHAPTER 4 PRELIMINARY WORK</b>	<b>50</b>
<b>4.1 Chapter Overview</b>	<b>50</b>
<b>4.2 Design Game Scenario</b>	<b>50</b>
<b>4.2.1 Scene 1: Phishing Attack</b>	<b>52</b>
<b>4.2.2 Scene 2:Smishing Attack</b>	<b>56</b>
<b>CHAPTER 5 SYSTEM IMPLEMENTAION</b>	<b>61</b>
<b>5.1 Development of Main scene</b>	<b>61</b>
<b>5.2 Development of Introduction scene</b>	<b>62</b>
<b>5.3 Development of Menu scene</b>	<b>64</b>
<b>5.4 Development of Quiz scene</b>	<b>66</b>
<b>5.5 Development of Game scene</b>	<b>68</b>
<b>5.6 Development of Study scene</b>	<b>70</b>
<b>5.7 Development of Video scene</b>	<b>72</b>
<b>5.8 Design Game Scenario</b>	<b>74</b>
<b>5.8.1 Scene 3 Password Exploitation Attack</b>	<b>75</b>
<b>5.8.2 Scene 4 Baiting Attack</b>	<b>79</b>
<b>5.8.3 Scene 5 Tailgating Attack</b>	<b>83</b>
<b>5.8.4 Scene 6 Shoulder Surfing Attack</b>	<b>89</b>
<b>5.8.5 Scene 7 Quiz</b>	<b>92</b>
<b>5.8.6 Scene 8 Video</b>	<b>98</b>
<b>5.8.7 Dicussion</b>	<b>103</b>
<b>CHAPTER 6 CONCLUSION</b>	<b>106</b>
<b>BIBLIOGRAPHY</b>	<b>107</b>



## LIST OF FIGURES

<b>Figure Number</b>	<b>Title</b>	<b>Page</b>
Figure 2.1	Serious game for Social Engineering	10
Figure 2.2	The cards for Social Engineering game	10
Figure 2.3	Overview plan	12
Figure 2.4	Type of card: principle (left), attack scenario (middle), attack technique (right)	13
Figure 2.5	Attacker card (front and back side)	13
Figure 2.6	Life cycle of Social Engineering Attacks	21
Figure 2.7	Rich picture showing information flow in a typical school	22
Figure 2.8	The model of the SEAP within a capability maturity model	23
Figure 2.9	SEAP conceptual model for schools	24
Figure 3.1	Overview of Social engineering attack awareness tool.	30
Figure 3.2	Overview of Phishing Attack.	42
Figure 3.3	Overview of Smishing Attack.	43
Figure 3.4	Overview of Password Exploitation Attack.	44
Figure 3.5	Overview of Baiting Attack.	45
Figure 3.6	Overview of Tailgating Attack.	46
Figure 3.7	Overview of Shoulder surfing Attack	48

Figure 3.8	Overview of Quiz.	49
Figure 3.9	Overview of Video.	50
Figure 4.1	Main interface of the awareness tool game.	52
Figure 4.2	Main interface of the game scenario.	53
Figure 4.3	Main interface of the Phishing attack scenario.	54
Figure 4.4	Phishing mail with malicious link.	55
Figure 4.5	When user click at the link will prompt user a message to select whether click this link with two option “Yes” and “No”.	55
Figure 4.6	If user select “Yes”, will pop this message to user, user can click on the “more info” button to understand which attack and relevant information.	56
Figure 4.7	When user click on “more info” button, will show this information.	56
Figure 4.8	When user click on “example” button, will show some the previous malicious mail and highlighted information for user to aware some details can distinguish the real email or malicious email.	57
Figure 4.9	If user select “No”, will pop congrats message to user, user can click on the “more info” button to understand which attack and relevant information or click the back button to continue the game.	57
Figure 4.10	Main interface of the Smishing attack scenario.	58

Figure 4.11	Smishing attack with malicious number.	58
Figure 4.12	When user click at the link will prompt user a message to select whether click this link with two option “Yes” and “No”.	59
Figure 4.13	If user select “Yes”, will pop this message to user, user can click on the “more info” button to understand which attack and relevant information.	59
Figure 4.14	When user click on “more info” button, will show this information.	60
Figure 4.15	When user click on “example” button, will some the previous malicious SMS and highlighted information for user to aware some details can distinguish the real SMS or malicious SMS.	60
Figure 4.16	If user select “No”, will pop congrats message to user, user can click on the “more info” button to understand which attack and relevant information or click the back button to continue the game.	61
Figure 5.1	Develop the whole game by using Unity	63
Figure 5.2	Hierarchy of Main scene	63
Figure 5.3	Hierarchy of Introduction scene	64
Figure 5.4	Hierarchy of Menu scene	66
Figure 5.5	Hierarchy of Quiz scene	68
Figure 5.6	Hierarchy of Game scene	70

Figure 5.7	Hierarchy of Study scene	72
Figure 5.8	Hierarchy of Video scene	74
Figure 5.9	Introduction scene of awareness tool	76
Figure 5.10	This is the menu scene of the awareness tool	76
Figure 5.11	This is the game scene of the awareness tool	77
Figure 5.12	Main interface of the Phishing attack and password exploitation attack scenario.	77
Figure 5.13	Main interface of the password exploitation attack scenario	78
Figure 5.14	This is an example of Password exploitation attack scenario	78
Figure 5.15	This is an example of Password exploitation attack scenario when user click submit, then will pop up a message “You had been hack!! Your email is abc@email.com Your password is 123abc”	79
Figure 5.16	When user click on “more info” button, will show this information	80
Figure 5.17	Main interface of the Phishing attack and password exploitation attack scenario	81
Figure 5.18	Main interface of the Baiting attack scenario	81
Figure 5.19	When user click at the USB will prompt user a message to select whether pick up and plug into your laptop with two option “Yes” and “No’.	82

Figure 5.20	If user select “Yes”, will pop this message to user, user can click on the “more info” button to understand which attack and relevant information	83
Figure 5.21	When user click on “more info” button, will show this information	83
Figure 5.22	When user click on “example” button, will show the previous parking slot and highlighted information for user to aware some details can distinguish the baiting attack.	84
Figure 5.23	If user select “No”, will pop congrats message to user, user can click on the “more info” button to understand which attack and relevant information or click the back button to continue the game	84
Figure 5.24	Main interface of the Tailgating attack scenario. System will prompt user a message to select whether allow the person follow you go in “Yes” and “No”.	85
Figure 5.25	If user select “Yes”, will pop this message to user, user can click on the “more info” button to understand which attack and relevant information	86
Figure 5.26	When user click on “more” button, will show this information	86
Figure 5.27	When user click on “example” button, will provide some highlighted information for user to aware some details can distinguish the tailgating attack	87

Figure 5.28	If user select “No”, will pop congrats message to user, user can click on the “more info” button to understand which attack and relevant information or click the back button to continue the game	88
Figure 5.29	Main interface of the Shoulder Surfing attack scenario. System will prompt user a message to select whether enter your password when a person standing behind “Yes” and “No’	89
Figure 5.30	If user select “Yes”, will pop this message to user, user can click on the “more info” button to understand which attack and relevant information	89
Figure 5.31	When user click on “more” button, will show this information	90
Figure 5.32	When user click on “example” button, will provide some highlighted information for user to aware some details can distinguish the shoulder surfing attack	90
Figure 5.33	If user select “No”, will pop congrats message to user, user can click on the “more info” button to understand which attack and relevant information or click the back button to continue the game	91
Figure 5.34	This is the first quiz question of the awareness tool	92
Figure 5.35	When user answer the first question then will pop the second quiz	92

Figure 5.36	When user answer the second question then will pop the third quiz question of the awareness tool.	93
Figure 5.37	When user answer the third question then will pop the fourth quiz question of the awareness tool	93
Figure 5.38	When user answer the fourth question then will pop the fifth quiz question of the awareness tool	94
Figure 5.39	When user answer the fifth question then will pop the sixth quiz question of the awareness tool	94
Figure 5.40	When user answer the sixth question then will pop the seventh quiz question of the awareness tool	95
Figure 5.41	When user answer the seventh question then will pop the eighth quiz question of the awareness tool	95
Figure 5.42	When user answer the eighth question then will pop the ninth quiz question of the awareness tool	96
Figure 5.43	When user answer the ninth question then will pop the last quiz question of the awareness tool	96
Figure 5.44	After user answer all the social engineering attack quiz will pop the score of the user.	97
Figure 5.45	When user click “more info” will direct user to the study scene with ten study scene.	97
Figure 5.46	This is the video menu scene of the awareness tool	98
Figure 5.47	This is the brute force attack video scene.	99

Figure 5.48	This is the phishing attack video scene	99
Figure 5.49	This is the SET toolkit attack video scene	100
Figure 5.50	This is the SQL Injection attack video scene	100
Figure 5.51	This is the Tailgating attack video scene	101



## LIST OF TABLES

Table Number	Title	Page
Table 2.1	Overall Comparison Between All Approaches	27
Table 3.1	Software tools for development	34
Table 3.2	Computer model for development	34
Table 3.3	Verification plan for phishing attack	35
Table 3.4	Verification plan for smishing attack.	36
Table 3.5	Verification plan for password exploitation attack.	37
Table 3.6	Verification plan for baiting attack.	38
Table 3.7	Verification plan for tailgating attack	39
Table 3.8	Verification plan for Shoulder surfing	40
Table 3.9	Verification plan for Quiz	41
Table 3.10	Verification plan for Video.	42
Table 4.1	Function of Game Scenario Scene features	62
Table 5.1	Main components in Main scene	64
Table 5.2	Main components in Introduction scene	65
Table 5.3	Main components in menu scene	66
Table 5.4	Main components in quiz scene	68
Table 5.5	Main components in game scene	70
Table 5.6	Main components in study scene	72
Table 5.7	Main components in video scene	74
Table 5.8	Function of Game Scenario Scene features	104

## LIST OF ABBREVIATION

<i>IT</i>	Information Technology
<i>TAC</i>	Technical Assistance Center
<i>SMS</i>	Short Message Service
<i>CNBS</i>	Consumer News and Business Channel
<i>STS</i>	Socio-Technical Systems
<i>SEAP</i>	Social Engineering Awareness Program
<i>CATWOE</i>	Customers, Actors, Transformation process, Worldview, Owners and Environmental constraints
<i>OOP</i>	Object-oriented programming
<i>SE</i>	Social Engineering
<i>AI</i>	Artificial Intelligence

### Chapter 1 INTRODUCTION

#### 1.1 Problem Statement

Social engineering comes in diverse forms of reaching the target victims and purposes. A lack of technology or faulty technology will cause many losses, but user prefer human behavior although technological methods of protecting information may be effective in their respective ways. There will have higher chance of falling into social engineering attack if the people's emotion gets manipulated easily. Resulting elder are easier targeted as a victim in social engineering attack. Lesser use of technology and not familiar with the technology knowledge mostly are in the elderly community. The attacker would pretend themselves as their grandchild or threaten them that they have kidnapped their grandchild in an exchange for confidential information such as the bank information. Throughout the interaction, the destructive nature in the elderly community is completely unaware of their action. Teenager also expose in this risk due to this technology advance era, every teenager also will have their own phone if they do not have the awareness about social engineering attack they will be the most target victim for this attack so this awareness tool mainly focus on teenager and above.

The handling of security breaches is forgotten focus by the public as the world pursues the augment of talent in advanced technology such as data analytics, AI and machine learning. In a report by CNBC, it was reported that there were about 2.93 million cyber security positions left open and unfilled around the world. Thus, there are still not enough cyber security knowledge workers, which cause the shortage of talents in cyber security. On the other hand, the threats of SE attacks are raising in the traditional training and awareness programs. To against social engineering attacks mainly the firm will send their employees to attend the traditional training and awareness programs. However, the biggest challenge is time consuming and need a budget to complete most of the programs and training, some expert and professional awareness programs are not available everywhere, so it was inconvenient for anyone who was interested to join the programs.

As social engineering is gaining popularity these days, the awareness of the security breaches is significant to decrease the cases in cyber security, avoid being targeted as victims with resulting human losses and financial loss. Perhaps a tool in digital based, with different features are most likely still not so popular but one day it will become the trending. This tool will bring BIT (HONOURS) Communications and Networking  
Faculty of Information and Communication Technology (Kampar Campus), UTAR.

many advantages which compare to traditional training and programs or physical games. Hence, those traditional ways will be replaced with the innovation of digital technology. The utmost importance, it can reduce the expenditure of organizations which allocate for employees to participate in awareness training and programs. In addition, smart devices with online functionality are available at medium-low cost and a lot of people have their own smart device nowadays. But also, professionals and most of the organization, even schools might profit from such approaches, giving them the chance to reduce the expenditure allocated to participate in the awareness programs and training.

### **1.2 Background and Motivation**

Social Engineering is the art of exploiting the weakest link of information security systems: the people who are using them. A book “The Art of Deception” written by one of the world’s most popular hackers Kevin Mitnick explained the power of social engineering techniques, which combine with hacking to power insidious attacks. While social engineering attacks attempt to exploit the users of these technologies, compared to the traditional hacking aims to compromise the security settings of IT systems and applications.

As the digital era matures, social engineering has become one of the major threats to a country’s economy, an individual's safety or even to an organization. One of the techniques in social engineering is attackers deceiving privileged users into revealing information that compromises data security to gain sensitive information. The process of exploiting human weakness that is inherent to every organization is the simplest methods of social engineering which gather information about a target. ‘Hacking’ is one of the social engineering words that people will often refer to it. Attackers maliciously use their advantage which humans have a trusting nature to them Organizations and Individuals will suffer an immense amount of loss by these attacks. In cyber security context, it is primarily used to induce victims towards disclosing confidential data, or to perform actions that breach security protocols, unknowingly infecting systems or releasing classified information. The basis of a social engineering attack is to avoid cyber security systems through deceit, exploiting the weakest link, the people involved.

## CHAPTER 1: INTRODUCTION

A talented practitioner of this discipline understands and perceives social interaction patterns to manipulate the psychological aspects of the human mind. With this resolution, the attacker is capable of executing an efficient and cheap security compromise, without the need to invest in breaking technical security measures. Nevertheless, an educated social engineer on computer science may also complement technological means to the attack in order to accomplish the malicious intentions. Due to low awareness and lack of proper training, social engineering becomes a threat that is overlooked by people. In essence, social engineering refers to an activity of psychological manipulation that did not depend mainly on the coding part to exploit confidential information for fraudulent purposes.

Generally, social engineering is considered the easiest method to collect information about a target victim through the action of manipulating the mind of the weakest link in the security chain that is the human. The types of information that the attackers are seeking can vary, either is to trick an individual to provide bank information, password or to secretly install malicious software in order to control over the victim's computer and get more information. The most common social engineering such as phishing, pretexting, tailgating, baiting, quid pro quo and water holing. Each attack has almost the same target to achieve which is to exploit the sensitive information for their fraudulent purpose. But overall each attack is implemented in different techniques.

According to Cyber Security Malaysia chief executive officer Datuk Dr Amirudin Abdul Wahab (2020) concurs that the fraudulent use of payment networks and data theft have gone up. There are several forms of cyber-attack where criminals look for vulnerabilities associated with the technology and use it to their advantage to trick people. For instance, Google Wallet was hacked and exposed user PINs which eventually made it available for the perpetrators to login to accounts for their own use in 2012. In another incident, the Starbucks app was hacked in May 2015, which automatically withdrew funds from a user's bank, credit, or PayPal accounts. In Malaysia, there were a few cases reported on users' bank accounts being manipulated. For instance, a user receives a TAC number through SMS, which was generated by someone who had access to the user's account and made an illegal transaction without the user knowing about it. The perpetrator then sends a message to the user explaining that he had accidentally key-in the wrong mobile phone

number belonging to the user and asks the user to share the TAC code with the perpetrator. Right after the TAC number is shared, the money in the user's bank account can be drained out.

Ever since the emergence of social engineering, the Star reported that about 272 criminal cases using SE have been attacked in Malaysia. The people are slowly having some idea of SE attacks but the actual technique of social engineering attack to get confidential data are unknown. However, there are various types of social engineering attacks but the major problem of the people that always trap of social engineering attack because they are less educated on as well as the techniques the attackers are using. Cyber Security Malaysia had recorded in 2019, a total of 10,772 cyber security cases were reported. Online fraud, content-related incidents, malicious codes, denial of service attacks and intrusion are the top five types of cases. According to the Star reported in terms of content-related cases, fake news and incidents involving public sentiments are on the rise, especially in the midst of the Covid-19 outbreak and also the political situation of the countries. Big healthcare data has substantial ability to enhance patient results, predict outbreaks of epidemics, achieve valuable insights, avoid preventable diseases, decrease the expenditure of healthcare delivery and enhance the quality of life in general. However, deciding on the allowable uses of data while preserving security and the patient's right to privacy is a difficult task.

There are few motivations to propose this approach. Research on social engineering attacks awareness programs, there are only program methods help participant think strategically by using general definitions to help them about whether the message is a social engineering attack or not. However, SEAP do not understand each participant individually but just using these simulations are prepared similarly for all participant. The awareness programs do not provide real case scenarios for them to know how the social engineering attacks happen. Furthermore, the goal of implementing SEAP might not be achieve because mostly the training sessions are generalized, it might result in a lack of understanding of multi-faceted SE attacks.

According to Vincent in 2020, in the cyber world with an ever changing landscape, in the next few years the demand for the kinds of cyber protection may not be the same as today. It is vital that cyber security infrastructure is up to date and protected in the industry which need to work closely with solution providers. To mitigate the chances of becoming a victim of social engineering attack, a series of training and policies can be implemented within an organization as BIT (HONOURS) Communications and Networking  
Faculty of Information and Communication Technology (Kampar Campus), UTAR.

well as to an individual. Mostly the firm use traditional training and awareness programs to keep employees updated against socially engineered attacks. Such educative programs include onsite training courses and awareness camps, posters, screensavers, and manual reminders. Even the best information security policies, procedures, or controls are useless if employees are tricked not to follow them. However, the challenge to training and awareness camps and other on-site learning methods are shortage of training budgets of firms. Motivate companies to minimize budgets for training which is the main challenges caused by the worsen of economies. This also create the chances for social engineering based hackers to discover new skills to sabotage the outdated systems of the firm.

In social engineering awareness program explores the defeat of common SE techniques, and the information security awareness training countermeasures. To maximize an organization's investment in information security by empowering and enlisting every employee to help defeat cybercrime. However, according to Ghafir et.Al (2016), the social engineering awareness program is not so effective due to the shortage of training budgets of firms and also inconvenience for people to attend the program. For problems like this, it can easily be solved by using tools with social engineering awareness to remind them of the importance awareness they should have which helps them easily adapt in any situation. Social engineering awareness tools are more convenient for users which can use it anytime and anywhere, not similar to the training or awareness program which needs to schedule a free time to attend it. In short, the awareness tools will ease the user to learn and be aware of social engineering attacks and can refer over and over with flexible time periods.

### **1.3 Project Objectives**

- To design awareness tools that ease users to explore the social engineering attacks rather than attend awareness programs.
- To provide a real case scenario how the social engineering attacks happen to lend them to understand how social engineering attacks are composed.

### **1.4 Proposed Approach/Study**

The project plan is to let users be able to understand the social engineering attacks which provide real case scenarios for them to know how the social engineering attacks happen. For the real case scenario, it will show some examples how they managed to get sensitive information via social engineering. Instead of the traditional boring training and program, they will have different experiences and have real case scenarios for users to understand. In the market nowadays, there are no proper social engineering awareness tools available. The tools or apps in the market just provide definition else do not have any game feature to let users while playing can learn the information in the same way. Hence, social engineering awareness tools will be a blue ocean market.

These tools not just provide basic definitions about social engineering, it will be some fun games to lead users through penetration. By using game features, to generate attention and interest about social engineering. Therefore, the user can enjoy the game and understand and have the concept of social engineering. Users are able to get the knowledge about social engineering attack by using this awareness tool while playing the game. The proposed project scope is developing a grounded theory of the concept of social engineering in the tools. This tool is to elicit and prioritize social engineering security requirements. Users are able to identify and understand some common social engineering. The limitation of this project is it is still a quite new tool for the public, it might need time for the public to accept and replace the awareness programs and training.

### **1.5 Highlight of what have been achieved**

In FYP1, two different type of social engineering attack in this project has been achieved, which is Phishing attack and Smishing attack. For this social engineering awareness tool, Phishing attack are carried out by the laptop in the game scene with phishing email and provide social engineering attack awareness and knowledge. Other than that, Smishing attack are carried out by the phone in the game scene with smishing SMS and provide awareness and knowledge about social engineering attack.



### **1.6 Report Organization**

The detail structure of this report is shown in the following chapters. In Chapter 2, some related approaches are reviewed. Chapter 3 will discuss the system design of this project and system specifications such as user or system requirements, verification plans and the implementation issues during developing this project. Besides that, Chapter 4, have describe the preliminary work before implementation of important features such as design the UI interface and 3D models. Moreover, Chapter 5 has explained about the whole development process of the system in the Unity platform. Lastly, Chapter 6, which is conclusion that summarise the whole report with few simple statements.

## CHAPTER 2 LITERATURE REVIEW

### 2.1 Chapter Overview

After discovering some introductory papers about the Social Engineering attacks awareness with physical card game, escape room there are few approaches to lead the user aware about the social engineering attacks and some of them able to have better understanding about those attacks.

#### 2.2.1 A Serious Game for Eliciting Social Engineering Security Requirements

There were several approaches introduced by different authors which focus on different ways of elicitation requirements of security. It is vital for human threat to evaluate the proper defense tools which involve socio-technical systems (STS) generating SE requirements. To understand the company by gathering knowledge the security engineers from outsider would need to learn about employees' capabilities, the processes, company policies, and attitudes. Modeling aspects of STS is a common theme in security requirements engineering. According to Houmb (2010), as a basis of identifying the security concerns in software documentation which use the common criteria. Behavior of humans does not focus on this approach which might be exploited by software engineers, because as a source for security requirements it builds on existing system and business report. In this model, writing passwords in notes will be described since individual people have different personality traits so if compared with certain approaches can use styles to recognise the threat but is difficult for social engineering. However, security requirements engineering is unable to do it.

To enhance the security awareness, employees need to join security awareness training conducted by companies to talk about the threat of social engineering. Some low cost mandatory security awareness campaigns do not provide long lasting effects to employees. In general, the employees' weaknesses are not well adapted. On the other hand, there are some agencies that attack their own clients and show the weaknesses from the attack by hiring penetration testing companies. The reason these penetration tests are so rare is due to the huge amount of effort that need to be invested before addressing legal issues. For the better, penetration tests are conducted for

## CHAPTER 2 LITERATURE REVIEW

employees who can be educated by the tester which finds the flaws. However, when confronted with the results, humans are easily demotivated, so the experiments are difficult to achieve.

A game for social engineering for employees of a company has benefit from eliciting security requirements. Common employers can base on the past behavior, attitudes and daily routine to gain benefits of knowing how much their co-worker's security knowledge towards security policies or rules. Especially the deviations from provisions they are more aware about business operation and their conditions. Moreover, the human vulnerabilities in a company can be unconsciously aware by the employees in the company. An approach has been introduced by Denning (2013), mainly based on security awareness games with arguments from serious game research. Players do not need to care about consequences when in the game scenario. Besides that, even though physical games can provide role play in contexts, the game is not feasible, desirable nor appropriate in any way.

There are principles in attack scenarios to provide the validity proposed in game (Figure 2.1 and 2.2) lets them become social engineering attack role, in order to explicit the threats. According to Beckers, Pape (2016), as a principle which is "if everyone is doing it, I do it as well" the game scenario provides the necessary information about patterns of human behavior and attack scenarios. While practicing immediately, social engineering can be learned by employees by playing the game while having fun. This statement alone is able to prove games will have lasting effects of learned knowledge. At first, the employees will propose social engineering threats and validity will build based on their knowledge of the context rate by other players. The game works as follows, for instance an employee who is going through the pressure in time for a deadline would most likely fall for phishing mail attack. The ranking of the proposed threats will be affected by the foundation for security requirements that were made to prevent the threats.

## CHAPTER 2 LITERATURE REVIEW



Figure 2.1: Serious game for Social Engineering



Figure 2.2: The cards for Social Engineering game

## CHAPTER 2 LITERATURE REVIEW

According to Klimmt (2009) attention and interest will be generated while they feel enjoyment in the game. In order to elicit, the company policies, processes, employees' attitudes and capabilities to gain professional domain knowledge would need to be understood by security engineer which from outsider. To cultivate the people that understand the task of their work fine in threat analysis will be more cost effective, simpler and surely easier. The "looking out of the window effect" people not experts in security is the highest danger of the participation who always spends their time looking out the window and thinking of other topics that describe the participants' boredom causes them to stop taking part. It aims to create an enjoyable experience for players to keep away from this outcome by engaging. Always think outside the box and use different methods of thinking that will get employees involved. The games surely can be fun and informative at the same time.

Based on their target audience which had considered the tradeoff between generic games for one specific target group or a very general group for the public. In terms of competencies, to determine the correct components of response teams the electricity industry in Norway of IT security preparedness have helped. These exercises are to evaluate new practices in a realistic setting and have the hidden capacity to enhance the recent emergency action to the fullest. According to Beckers, Pape (2016), by applying the department fire escape plan is an overview plan (Figure 2.3). There is some information from the employees that are working in that department which must be expanded the company's assets, such as their locations and communication channels. All players should be involved for the plan completeness in the creation. It is easily available, the bases procedure on the plan of the department, due to it is often publicly hung out to show the routes to get away. Moreover, players can find all the information such as fire alarm button, fire-extinguisher location, and escape ways in an attack for the plan shown. Lastly, instead of the setup if the game is giving attention on the attacks, the natural outcome of the players studying for defects will be the familiarity with it at the beginning of the game and further discussion.

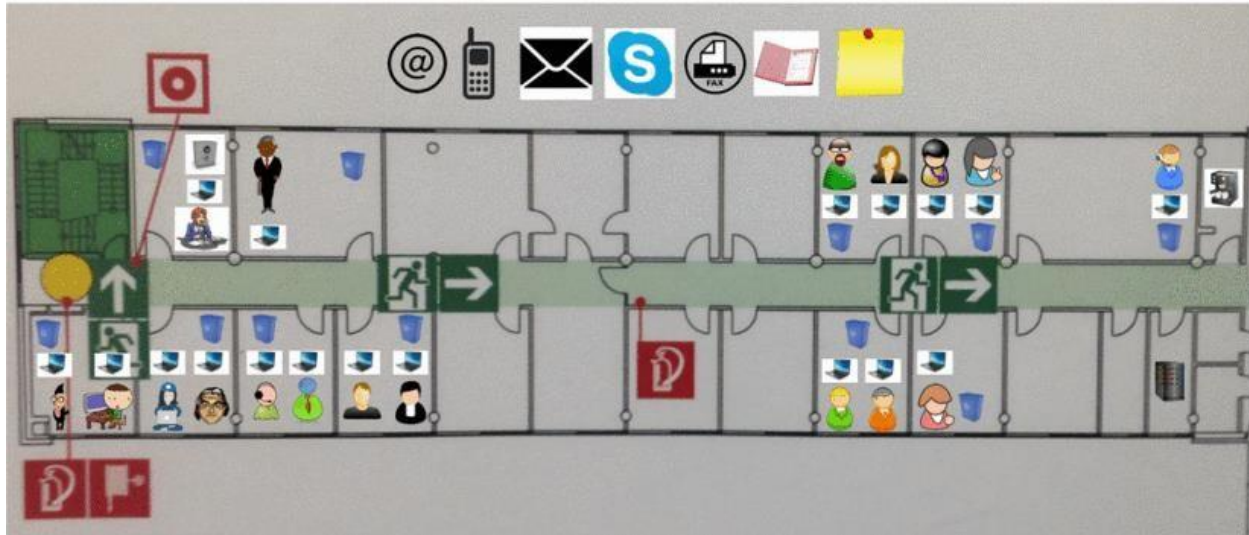


Figure 2.3: Overview plan

Before starting playing the game, each player should draw three different cards which are principle cards, attack scenarios cards and attacker cards. A sample card (Figure 2.4). The deck of human behavioral patterns which are known as principles cards every player takes a card. Based on one of the principles the social engineers need to behave according to exploit it. According to Beckers, Pape (2016), an instance for the patterns will be the principle of Need and Greed that clarify “Your needs and desires make you vulnerable. Once hustlers know what you really want, they can easily manipulate you”. In the next step, every player is given three cards from the deck of the SE attack techniques which are known as attack scenarios cards. The related relationship in a part of the behavioral styles in a proper manner, so the players are only allowed to draw three cards. For example, reverse social engineering which gains trust from the selected person involves creating a problem and solving it for him, asking the victim for a favor.

Next, the card has two sides (Figure 2.5) is an attacker type card which allows each player only to get one. A common staff of the organization is known as an inside attacker. The outside attacker acts as the unknown aspect to the organization members. For insiders are easier to attack because in the organizations they have already build trust. Before the attack execution, the trust between outsiders and organization should be established. The players should come out with what kind of attacker they are and plan their attack accordingly. For instance, an outsider must give a



reason for go in the organization but for an insider just have to cover his paths more precisely or pass the buck to coworkers.



Figure 2.4: Type of card: principle (left), attack scenario (middle), attack technique (right)

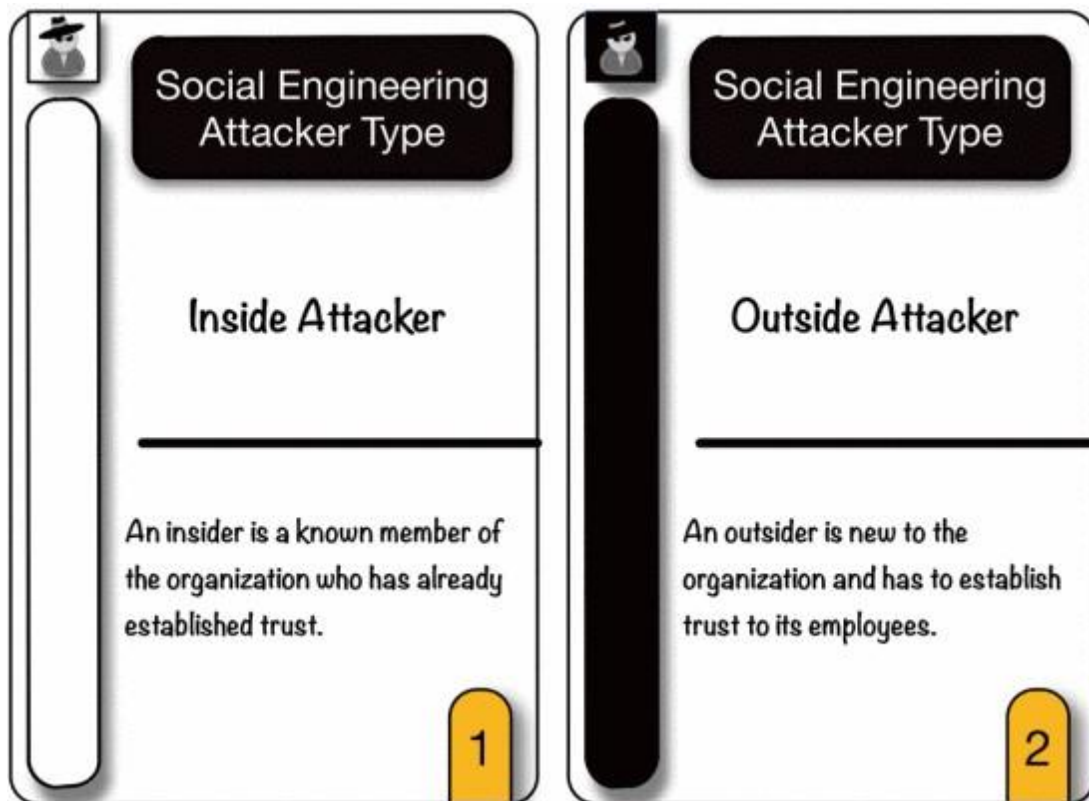


Figure 2.5: Attacker card (front and back side)

## CHAPTER 2 LITERATURE REVIEW

Then, the players adopt the attacker role in the brainstorming phase. To exploit the behavioral pattern of an employee each player needs to think of how to conduct one of the three attacks. In the overview diagram one person is targeted to exploit. Moreover, the player has to choose if she acts a role of an outsider or insider in the organization. Each player needs to think and elaborate their attack in five minutes. They will get distracted easily while having too much time, but the players will frustrate if the time frame is short. Each player proposes an attack until all persons iterate at least twice. As each player presents an attack along with the discussion and getting points consider a round of game which consists of turns of all players. The players restock their cards each round. The time will be shortened in the brainstorming phase if the iterations needed by the players are less time. The active player presents his attack to the group. A principle, an attack scenario, an attacker, a victim, a communication channel and a targeted asset need to be consistent in each attack. When a player has finalized the planning attack, the player has become unchangeable, if the player is allowed to keep changing and always revise their attack to address any risen concerns, it might lead to gaining full points which the game will be endless.

The award points did not embody the players' effort then players were dissatisfied while in the lively discussions. A feasibility reasoning of the proposed threat, if the player obtained help when elaborating the attack or the attack is plausible, but the explanation is infeasible then the player gets one point, for example the attacked person has a special training to resist the described attack. If the proposed attack is not plausible and the round ends immediately, and the player will get zero points. On the other hand, if the attack is feasible with case, the player is able to get two points. For the situation which the player obtained more than one point, a compliance discussion follows. According to Beckers, Pape (2016), for principle: perfect match attack described by the player will get 2 points, gets 1 point if it matches only somehow. The attack description matches the presented attack technique card then the player obtains one point in the scenario. Inside attacker will gain one point while outside attacker will gain two points if the card matches the attacker type in the proposed threat on the attacker side.

In the debriefing phase, the company's security personnel may be supported, and the players reflect their attacks. Based on the potential cause by likelihood to succeed and damage, which this card game is to identify the most relevant threats of social engineers in organization.



## CHAPTER 2 LITERATURE REVIEW

To figure out the probability of some people having a higher chance were attacked but others not at all. It also led to analyze which communication channel and determine why some assets were attacked more often than others. Their variations need to be explored by getting the threat of other players' variations. There is a risk during a security analysis when any missing threat that is not considered and subsequently not protected against.

There are various advantages and disadvantages found in this paper. One of the advantages different facets of social engineering acts can be learned by the employees and becoming an attacker by utilizing the awareness when inside the game. While having fun playing, also learning and applying social engineering will create lasting knowledge on the subject. Besides, by enforcing valuable and precious insights of the domain in their contention the plausibility of the proposed attacks is rated by the employees. Hence, the not plausible attacks in this specific context will be eliminated quickly. Their respective security requirements and prioritization of threats are into the plausible attacks and hopefully, the only feasible ones.

For the disadvantages, the card game can only play physically, and no people guide to ways to play, it does not design as digital based, which means it is not functional on any technology devices. Those who want to play the card game should buy the whole set of games including cards and overview plans. In order to solve this, they should export the game to computer games, build an application that allows users to play together online with different branches of employees and get a wide range of information exchange about social engineering. The employees in the same company with different branches can have better relationships through playing this game together. In the same company, if we keep playing the same game among the same members it would not be effective due to the same employers having the advantage of awaring their daily routine well and they know about their coworkers' attitudes towards policies and security rules, past behavior, and security knowledge. Hence, after they have played iterates until all persons iterated at least several times, then they are well suited to the employees' weaknesses. There is a way to solve it, it can have two different versions combine it in one which can create their own teams or open to the public and allow random players. For those companies who want to play together can create their own teams; for those who not enough players can join for random players. Then, we would not know each other. It would increase the difficulties and would not cause them to avoid taking part

## CHAPTER 2 LITERATURE REVIEW

and spend their time looking out the window and thinking of any other topics. In short, they will not easily get bored with the game because it has a different version for the user to experience and explore it.

### **2.2.2 Security awareness escape room - a possible new method in improving security awareness of users**

According to Kevin Mitnick (2003), these types of attacks technological solutions do not provide complete security against. Security awareness should be improved is the one and only effective countermeasure. Within the company operates every organization independently from the sector are important topic to have the information of security awareness. To ensure organization not targeted for financial loss or to cause disruption. Hence, each employee should have more aware about the security exploit, so most of the organization send their employees to the security awareness training and program. Attacks based on human factor can be prevent from information security, comprehensive information security trainings and programs should be performed. During the security training or program, they are taken away from their usual roles and, for at least a few hours, take part in a workshop which sees an instructor lead them through the ins-and-outs of at least one security topic. For instance, in the training materials have to contain not only these boring descriptions but with physical instruction attacks which exploit human factors. In short, purpose of security awareness training is to inform employees about the security policies and rules of the organization and the necessity of adhering to them.

Security of awareness escape room is another way of informing people about the security awareness through a physical room with furniture such as desk, the chair, the container and all the things on and in this furniture. Six points of views can be identify and explain which are theme, goals, type of exercise, time for a game, number of participants and computer usage but these are main differences between original exit games and information security escape room. The most vital in this kind of escape room is computer, it different with the original escape room or exit game which usage of computer are unnecessary. From the point of view of theme, security awareness escape room should be more reality compare to original escape room. The escape room should be a workplace and office environment. Then the role of players would be office of an assistant, boss, project manager and other “interesting” employee. Compare to the original escape room the type of exercises will be totally different, in the security awareness escape room mainly only focus on the security awareness knowledge instead of the logical, quiz or the slickness. Goals of the security awareness escape room are playing as an attacker who can get access to the computer of the user and opens the appointed file, which totally different compare to the original

BIT (HONOURS) Communications and Networking  
Faculty of Information and Communication Technology (Kampar Campus), UTAR.

## CHAPTER 2 LITERATURE REVIEW

escape room which really escape the room otherwise it will sink or explode or shot down. Besides, without increasing the number of players per group the time for a game should be reduced due to let more people can participate in the game.

The first step can be used general story lines or exercises during the game, which identify the methods, policies and devices used in the company. Provide an environment just same as the common organization office. Then should plan and create the relevant characters, scenario and relevant equipment only start set up the environment. Then, there are few steps to start performing the information security escape room which are registration for the game, instructions and rules before the game, help and supervise then during the game, lastly are photo with the result. For the registration can be in two different based which are paper form based or intranet online form. The form should contain a timetable and slots for the names of the players, most important are their detail and number of players. For instance, if they register through online form should have their name and phone number to guarantee they are not simply register for fun which easy to contact them. The program will not be successful if plan enough time for promoting the program, and sufficient time period to register. Therefore, if use a not suitable to the usual communication and registration channels registration is a very important step, because.

After register successfully, each group of players will be an instructor to provide them some instruction, rules, describe the scenario for each player to lead then to their goals. According to Oroszi (2019), rules of the game:

- Internet is available for all the devices.
- The target file can be found on either the computer or on any external devices.
- These are forbidden if use your private notebook or data travelers.
- Hacking methods is also forbidden.
- The game does no successfully finished if the devices are stolen.
- Try to guess the password according to the conventions or bad habits but not using brute force, password reminder or forgot password function.
- Modify the content of files, papers are forbidden.
- Use of the bin for real trash are forbidden.

## CHAPTER 2 LITERATURE REVIEW

Supervision can be performed in different ways, not necessary physically presence in person supervise also can use more advance way via webcam. The instructor can supervise them and identify the player who break the rule, during the game or end the game. Each group of players should have limit only times to ask for help from the instructor. When the players exceed the time of game, the instructor have the right to stop them or let them continues it depends on the situation. Each group of players will be taken a photo and stated their result time at the end of game. The photo can be a good promotion for next game and a good memory for the players. Moreover, for the players who successful complete the game on time can also have a gift for compliment. For instance, badge, webcam cover, notepad or even a certificate contain their result. These can always remind them they have participate in the game and learned the knowledge. They also can show and share their experience with other, it will motivate more people to participate in this kind of escape room. One of the elements of the information security program or campaign can be prepared for information security escape room. The instructor must reestablish and repair the room before the next group of players. The instructor should check is there any modification element from the previous group of players and if necessary, then should correct them because sometimes there are funny players who modify the password reminder or other elements of the game.

The most obvious advantage of this paper is that the escape room of the awareness of security is another method to let people have the security awareness through game based. According to Van (n.d), “Gamification is the use of game elements and game thinking in non-game environments to increase target behavior and engagement”. Instead of the traditional boring training and program they will be had different experience, and have real life try on how to log in to the target person computer and open an appointed file. They will be more aware how this type of attack to be countermeasures because they have been experiencing and try it.

On the other hand, this paper does have several disadvantages. The first disadvantage is the whole process of the game need at least a person supervises it. If there are quite a lot of rooms which mean need the same amount of supervisor. For this, should be hire more supervisor for the escape room, it will be high cost. Before conduct this escape room should have train them become qualified supervisor, which need more effort on it to train them and they should clearly understand all the steps and the ways to achieve the goals else when the player ask the supervisor question, cannot provide the most accurate answer and detail explanations. The problem can be

BIT (HONOURS) Communications and Networking  
Faculty of Information and Communication Technology (Kampar Campus), UTAR.

## CHAPTER 2 LITERATURE REVIEW

solve by transform this escape room to virtual escape room through digital devices. Through online platform, it will decrease the cost which no need to hire any supervisor or instructor. Moreover, this escape room is not convenience for player from worldwide to join this security awareness escape room. It will be a bit ridiculous for someone who just want join it but from different country, just flight to there for participate it. The timetable and timeslot might be crash, due to different country have different time zone although it allows register via online form but the time stated was their country not applicable for worldwide timeslot. In order to solve this problem, this escape room should be export it to be digital based, build an application that allows users to play together through online and get to access at any time slots at anywhere.

### 2.2.3 A model for social engineering awareness program for schools

A common misconception people have about cyber attackers is that they only use advanced hacking tools and technology to break into computers and networks which is simply not true. One of the easiest ways to steal information or compromise a network is by simply talking to and misleading you by attackers which is social engineering attacks. In short, humans are usually the weakest link in the security chain, so to enhance the awareness of social engineering. For this reason, schools offer various types of human attacks, also known as social engineering awareness programs. According to Elstad (2016), students' learning needs to be improved and communication with parents so that schools assist teachers like many other organizations are now embracing technology and have used it. In today's society, the way teach and learn has transformed this widespread adoption of technology.

According to Poremba (2012), huge financial and human losses are increasing in the school system because viruses and ransomware are attacking school infrastructure and their assets which are caused by social engineering. Firewall, antivirus and encryption have placed it to secure their infrastructure. However, schools are targeted by the human element on cyber criminals and increase focus on more threatening to organizations. For instance, the data will be lost if the staff do not know or understand the procedures. Data needs to be protected by the staff. Schools are the one who do not mainly focus on cyber security, but schools must protect their infrastructure because it also likes an organization so they need to invest in some techniques. Schools are the place mainly focused on educating but not the human element so this provides the chance for Social engineers to have higher chance successfully exploit the human element.

Besides educating the common knowledge, discussing its risks, tactics and countermeasures schools should also educate staff about social engineering attacks. To raise the awareness of SE, schools should evaluate and measure susceptibility of employees to real world SE attacks. An aim tends to reduce the exploit human tendency, a model for SEAP needs to have multiple communication methods to deliver and design to meet all types of learning styles, implemented and used. Schools provide education to human elements which implement the goal of change in behavior of the Social Engineering Awareness Program (SEAP). According to Hadnagy (2014), “A hacker of people, with malicious intent”. Life cycle of SE attacks which focus

BIT (HONOURS) Communications and Networking  
Faculty of Information and Communication Technology (Kampar Campus), UTAR.

on the human element, and how technological infrastructure bypass by social engineers. (Figure 2.6).

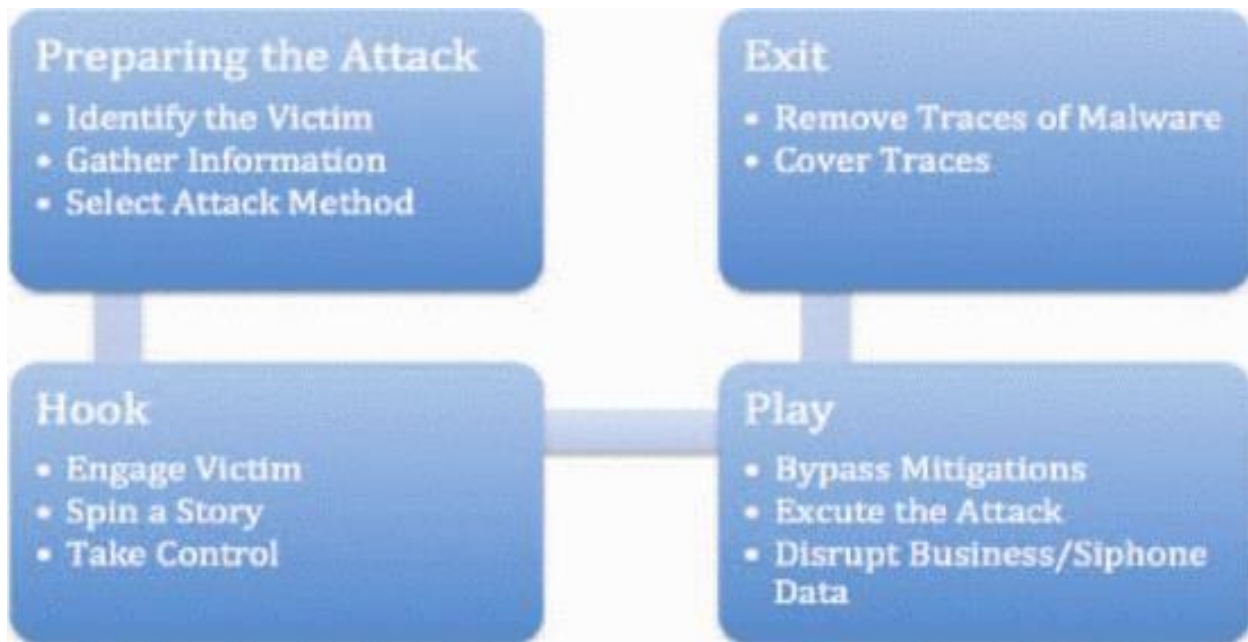


Figure 2.6: Life cycle of Social Engineering Attacks

The first step of this approach is preparing the attack. It is the first stage, needed to identify the target victim then gather the victim's information and select a method to attack. The next stage is a hook which engages the target victim such as spinning a story and trying to take control. Next, play the attacker bypass mitigations, then execute the attack to disrupt business or the data will be siphoned. The last stage is exit, the attacker removes traces of malware and covers the traces to prevent discovery. Implementing SEAP with how to overcome obstacles are the main things that schools need to identify where the obstacles. If mitigate the threats of SE attacks, we need to evaluate the quantitative analysis undertaken and understand the stakeholders' needs.

The goals of identifying the stakeholders to the model of SEAP for schools by design process with data assets which need to analyse the information. According to Basden (2006), methodology was used to obtain (Figure 2.7) and to achieve the subsequent CATWOE.



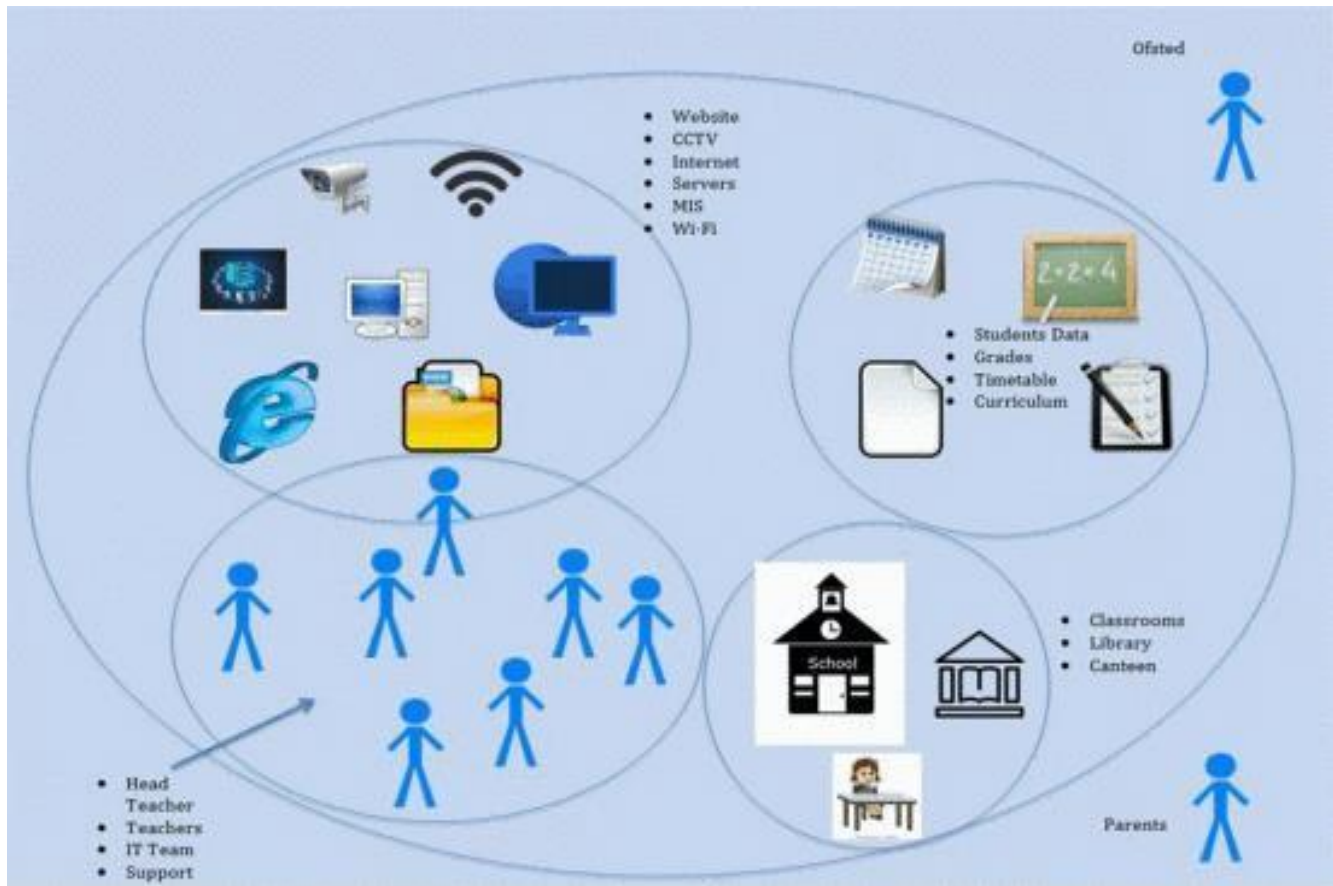


Figure 2.7: Rich picture showing information flow in a typical school

According to Basden (2006), CATWOE obtained in school as follows:

Customers: Students, staffs, teacher

Actors: Offices of SE Awareness

Transformation process: SEAP need to be raising

Worldview: More vigilant staff

Ownership of the system: SEAP officer, Head of Teacher

Environmental constraints: School

BIT (HONOURS) Communications and Networking  
Faculty of Information and Communication Technology (Kampar Campus), UTAR.

## CHAPTER 2 LITERATURE REVIEW

Social engineers attack the human elements which are identified in the (Figure 2.7) which are the vulnerable CATWOE.

CATWOE is an issue from six unique perspectives that is a method of problem solving. This in-depth approach requires that we think about any given problem in a variety of ways, and after doing so have better understanding and appreciation for the issue. Social engineers exploit them such as the school's website and Wi-Fi due to the IT team leaving weakness and the poor implementation of security policies. The basic security such as antivirus, firewall and access controls are implemented by many schools to protect physical security measures and their data assets.

According to Mohammed, Apeh (2016), the process of implementing SEAP which is the model of the SEAP within a capability maturity model is started by evaluating the current level of social engineering awareness. (Figure 2.8)

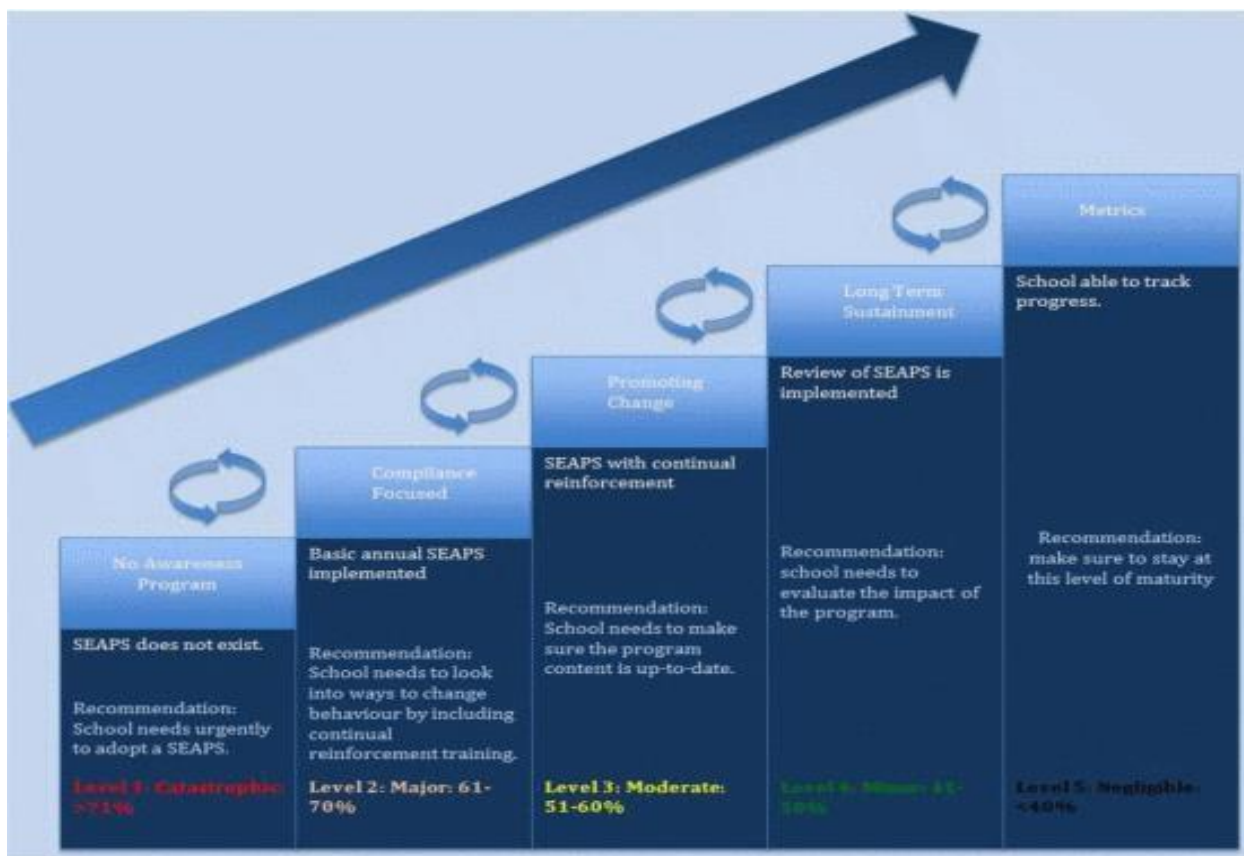


Figure2.8: The model of the SEAP within a capability maturity model

## CHAPTER 2 LITERATURE REVIEW

According to Wilson (2003), SEAP has essentially been designed as a training and education program consisting of a learning continuum which starts with awareness, builds to training and evolves into education. First, the awareness within the SEAP model is focused on the countermeasures for social engineering. Posters and leaflets can be known as different ways to raise awareness in classrooms or offices, which can motivate people to participate in them. Furthermore, training is different with awareness which needs to be demo and hands on practice for staff and children. For the training session, it could be conducted during ICT lessons for children. Awareness and training can be combined in one session to tailor and aware them at the same time. Before the end of section, can evaluate by conducting a test, quizzes or practical to know their ability to recognize and defend against social engineering attacks. The final component in SEAP is education, they can continue further study for some specific courses or degree programs.

□

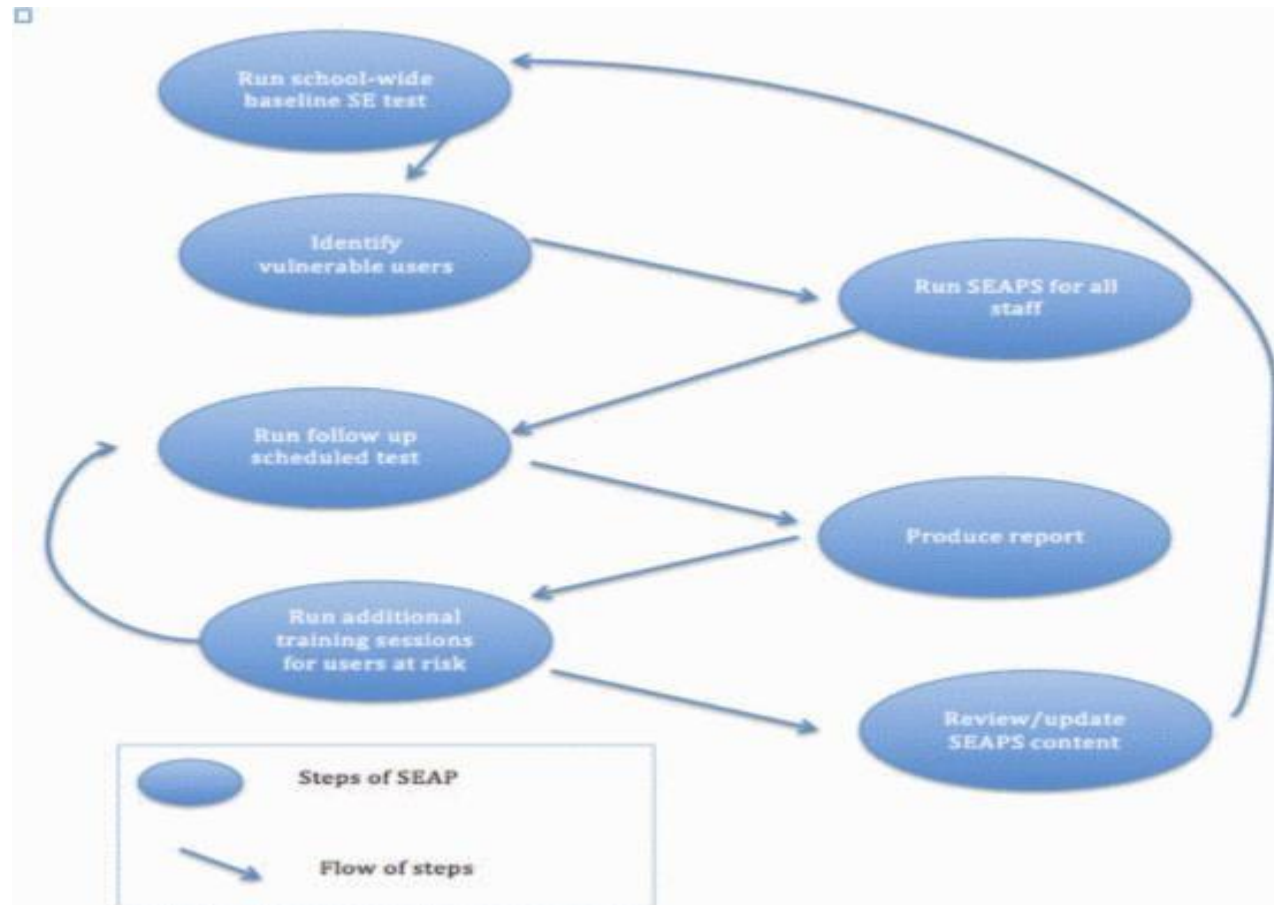


Figure2.9: SEAP conceptual model for schools

## CHAPTER 2 LITERATURE REVIEW

Based on the SEAP conceptual model for schools which should start with run the school; website baseline SE test, then identify the vulnerable users. Provide and run SEAPS for all staff, to ensure all staff have participated in the awareness programs, only run follow up and scheduled tests. The test is to ensure the information has been absorbed, then produce a report. Based on the report, there are two different cases which run additional training sessions for the users at risk to double ensure the risk users can absorb the SE knowledge else proceed to the next steps which is review or update the relevant information in the SEAPS content. On the other hand, follow up and rescheduled tests for users at risk after they participate for additional training. Lastly, run again school website baseline SE test to confirm everything runs smoothly, else if necessary, repeat the whole model.

This awareness program proved to have few advantages. As the age of users of Internet connected devices is lowering more and more, concerns are rising on the security implication of having preteens or even younger children tap into resources and being exposed to the security and privacy risks related to the use of the Internet or sharing of sensitive information online. Firstly, it was a good start for students who participate in awareness programs at an early age, they can know how to be aware and easily adapt in this kind of situation for their future career. Due to the internet it is not a secure environment for beginners such as teens or even earlier age. The younger the user, the more careless he or she might be when using mobile devices or internet connections. Students who have joined the awareness programs and training will be more careful in preventing them from being the easy target of malicious hackers infiltrating systems and accessing information. Besides, students who are really interested in the cyber security field can also have a clearer path for their future which is to continue to study with the courses about cyber security. Cyber security is a national priority and requires a team approach regarding education. After graduation, they can contribute to the public with a high salary because of the current shortage of skilled workers in the sectors.

There are few disadvantages for this awareness program, students who join in the early age of SE knowledge might be outdated when in their future career. The digital world keeps changing, although their susceptibility to the real world social engineering attacks but when the time they work in organization it attacks will be more advanced and sophisticated. Here come the problem,

## CHAPTER 2 LITERATURE REVIEW

it's the same type of attacks that hasn't changed, but cybercriminals decided to use a different tactic exploiting an unpatched vulnerability found in a piece of software used on a global scale. This problem is solving by keep updating social engineering attacks of tactics and countermeasures, which can just explore through social engineering awareness tools. By changing the traditional ways of participating the awareness programs or training, if there a tool which no need scheduled the time to attend it. Just simple steps, students can update their awareness knowledge by exploring via online. To keep on investigating what makes them tick and always have a proactive behavior and react to attacks in a timely manner. On the other hand, if every students and staffs should participate the awareness program it would be huge cost for a school. Ensure students and staffs have the best concept and understand the social engineering attacks should be hire some professional in cyber security to teach and guide them. Therefore, to solve this budget shortage can use an awareness tools through online. Nowadays, mostly everyone will have their own smartdevice, so they can easily explore it without using an amount of money to join the awareness programs and training.

**Table 2.1 Overall Comparison between All Approaches**

	<b>2.2.1 Serious game</b>	<b>2.2.2 Escape room</b>	<b>2.2.3 SEAP</b>
Which based	Card game based	Room based	Training based
Time usage	Depends on number of players, have 4 sessions, each sessions each player has 4 to 5 minutes	15 to 30 minutes	Depends on the report, if the participant in the risk which need additional training
Number of players	2 and above	3 to 5 players	Depends on the class size
How it's work	By drawing different of cards, for players brainstorm then elaborate and describe the attacks. After discuss the plausible and infeasible, then claim with points (0-2 points). Lastly, others player can propose improved version to claim points.	Given a scenario, a role to let player imagine they are in that situation.	Lecture, demo, case study and hands on practice. A test such as quizzes which to ensure the information has been absorbed at the end of session. Based on the report, provide additional training for the players at risk.
Advantages	- While having fun playing, also learn and apply of social engineering it will create lasting knowledge	- With different experience, and have real life try on it	-Participate awareness program at early age - Clearer path for their future
Disadvantages	<u>Problem 1:</u> -No people guide to ways to play	<u>Problem 1:</u> -Need at least a person supervise players	<u>Problem 1:</u> -SE knowledge might be out dated

## CHAPTER 2 LITERATURE REVIEW

	<p>- Only can play physically</p> <p><u>Solution 1:</u></p> <p>-Export the game to computer game, build an application that allows users to play together through online</p> <p>-With different branches of employees and get more wide range of information exchange about social engineering</p> <p><u>Problem 2:</u></p> <p>- know about their coworkers' security knowledge, attitudes towards security rules and policies, and past behavior</p> <p>-well adapted to the employees' weaknesses</p> <p><u>Solution 2:</u></p> <p>- Two different version combine it</p> <p>Version 1: can create their own teams</p> <p>Version 2: open to public allow random player</p>	<p>-If a more escape room need more supervisor due to high cost</p> <p><u>Solution 1:</u></p> <p>- Convert it to virtual escape room through online</p> <p><u>Problem 2:</u></p> <p>- Not convenience for who interested to join it from different country</p> <p><u>Solution 2:</u></p> <p>-Transform it to digital form, virtual escape room.</p>	<p><u>Solution 1:</u></p> <p>- Explore through social engineering awareness tools</p> <p><u>Problem 2:</u></p> <p>- Huge cost for all students and staffs participate SEAP</p> <p><u>Solution 2:</u></p> <p>- Awareness tools through online</p>
--	---	---	--

### CHAPTER 3 SYSTEM DESIGN

#### 3.1 Chapter Overview

This chapter will explain the general methodologies and list down the technologies used in the methodologies step. Furthermore, design the draft of system flow diagram so that the whole system can be illustrated clearly. System requirements such as software and hardware tools that used to develop the application will be discussed in this chapter. Lastly, create a project timeline so that the development of the application can be planned properly.

#### 3.2 Design Specifications

##### 3.2.1 Proposed Method

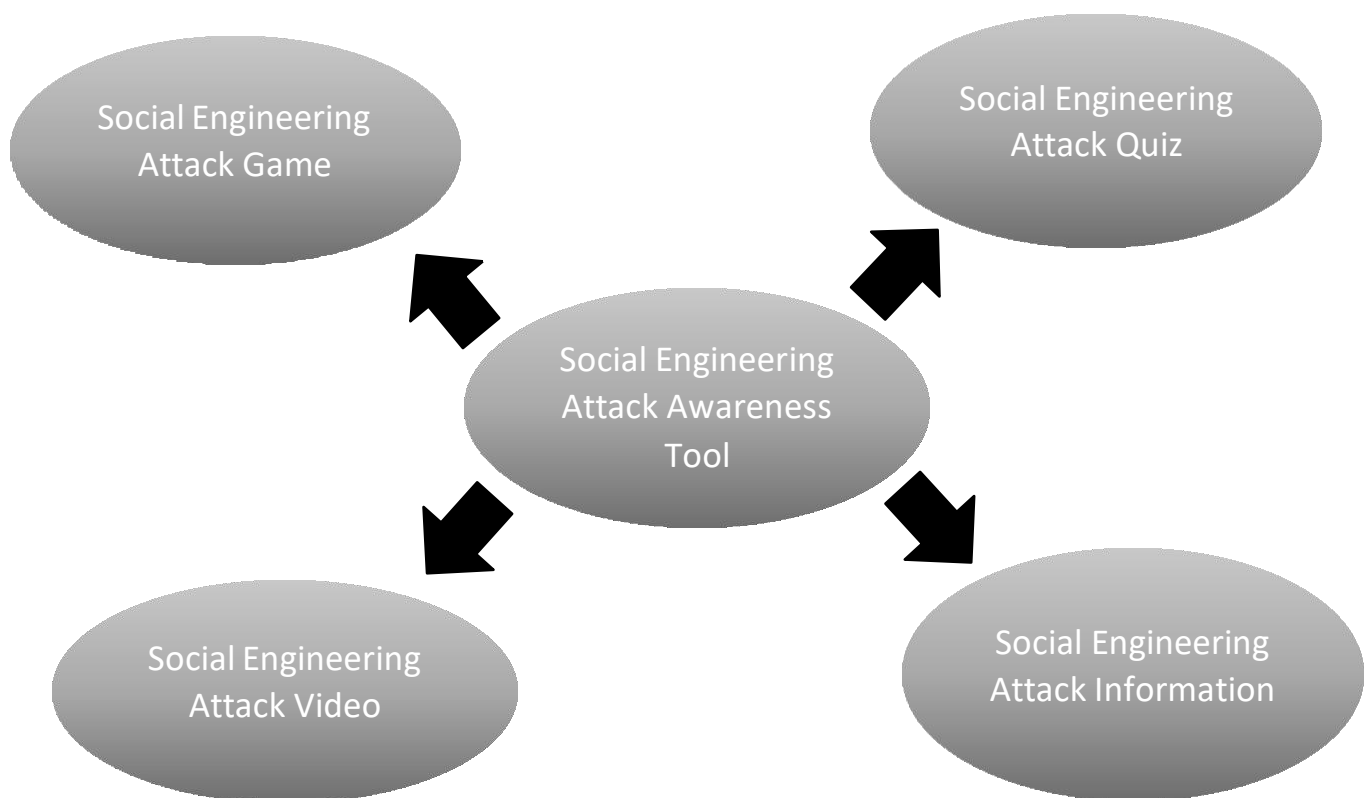


Figure 3.1: Overview of Social engineering attack awareness tool.



## CHAPTER 3 SYSTEM DESIGN

After reading various of papers and journals that related to my project, a general approach is constructed. For the awareness tools, user need to press the button to start the game. It will redirect to a short introduction about this social engineering awareness tools. After click start, will have a menu of this awareness tool which have game, quiz, video and study. Then the game is in room scenario, which have a desktop, smartphone and USB on table some books on the rack, a door and the chair. Based on the game scenario which will have Phishing attack, Smishing attack, Baiting attack, Tailgating attack, Password exploitation attack and Shoulder Surfing attack. For the video will have five different type of social engineering attack video which are Brute force attack, Phishing attack, SET toolkit attack, SQL injection attack and Tailgating attack. Moreover, for the quiz will have ten different question about social engineering attack which different type which have case scenario, theory and others. Then the Information is at study button which provide social engineering knowledge about the quiz.

Firstly, user click the on the laptop it will direct user to the desktop screen which have some icon on the monitor screen such as mail, web browser and some files. The user can randomclick on it. When user click on the mail icon, then will have some email inside the mail box. Usercan read the email and understand the contain of the email. One of the emails contain about Phishing attack. Phishing attack often used to steal user data, including login credentials and creditcard numbers. In this game, it will pop a message ask user whether want to click the link in the email. User can choose either yes or no, if yes then will pop a message to tell user that had been attacked and provide some related information about phishing attack to aware user, if choose no then will pop a message to congrats user have been successfully avoid a phishing attack and withsome related information.

Besides desktop, there is a smart phone on the table. When the user clicks the smart phone then will direct user to the home screen of the smart phone. Then in the home screen of smart phone will have come apps and icon such as call, message, browser, camera and so on. When user click the message icon will have few SMS in the inbox, one of the SMS is about user PayPal account has been suspended due to suspicious activity and request user to contact immediately, then will pop a message which request user to whether call that number if user choose to call this number mean the user had been attacked. Therefore, scammers can easily get their login information and login to their account, else they are successfully avoiding a Smishing attack.

BIT (HONOURS) Communications and Networking  
Faculty of Information and Communication Technology (Kampar Campus), UTAR.

## CHAPTER 3 SYSTEM DESIGN

For the laptop it will have another game with is in the chrome icon. When user click the chrome icon will direct user to the login page which need user fill in the email and password. If user fill in the email and password, then click submit system will prompt a message “You have been hacked! Your email is (the email user key in) and your password is (the password user key in)”. Will have a button for more information to let user know more about this password exploitation attack and have awareness knowledge about it. If user click back will back to the game scene to continue the game.

Moreover, on the table will have USB on the table with beside the smart phone. When the user clicks the USB then will direct user to the car park scene with a lot of USB on the floor. When user click on any USB on the floor will pop a message to ask user whether pick it up and plug it to the laptop. If user choose yes then will pop a message to tell user that had been attacked and provide some related information about baiting attack to aware user, if choose no then will pop a message to congrats user have been successfully avoid a baiting attack and with some related information. Thus, user will know how their password been hacked with different ways.

In addition, there is a door in the game scene which is the tailgating attack scene. When user click the door will direct user to the scene with two people, one person will ask the person can help to scan the access card because his access card not working again. Then will ask user whether “Will you allow the person go in with you?”, if user choose yes then will pop a message to tell user that had been attacked and provide some related information about tailgating attack to aware user, if choose no then will pop a message to congrats user have been successfully avoid a tailgating attack and with some related information.

At the chair in the game scene which contain the shoulder surfing attack. When user click the chair will direct user to the scene with two person one is using the smart device then a person is standing behind the person. Then system will prompt a message for user whether enter your password when a person standing behind you. If user choose yes then will pop a message to tell user that had been attacked and provide some related information about shoulder surfing attack to aware user, if choose no then will pop a message to congrats user have been successfully avoid a shoulder surfing attack and with some related information.

## CHAPTER 3 SYSTEM DESIGN

On the other hand, there is social engineering awareness quiz for user to answer and have more awareness knowledge about social engineering attack. There are ten question which have different types of pattern such as scenario-based question to give user think if they in that scenario what they will do, each question will have four selection for user to select, only can select one for each question. After answered all the question, user will have their score. Besides, there also can click on more information to study more about the social engineering attack and have more awareness knowledge about it.

Next, there are social engineering attack video in this awareness tool which provide user more understand the attack by watching the video and have better visualization about the attack. There are five different attack which is brute force attack, phishing attack, SET toolkit attack, SQL injection attack and tailgating attack. By clicking the name of the attack will direct user to the relevant video of the attack that the user selects. There is the most common attack there will happen, so by watching the video user will clearer and understand this type of social engineering attack then they can avoid it.

## 3.2.2 Tools to use

The following table shows the software tools that will be used to develop the proposed application.

Development Environment	Software Tools
Game Engine	Unity Hub
Programming Languages	Microsoft Visual Studio - C# (code function of modules)

Table 3.1 Software tools for development

The following table shows the hardware tools that will be used to develop the proposed application.

Computer Model: ASUS TUF GAMING A15

System	Information
Operating system	Window 10 Home(64-bit)
Processor	AMD Ryzen 7 4800H Radeon Graphics
Graphic card	NVIDIA GeForce GTX 1650 Ti
CPU	2.90GHz
Memory (RAM)	16GB

Table 3.2 Computer model for development

## 3.2.3 System Performance Definition

In this system, the performance is defined based on the user decision. The reason is if the user chooses “Yes” the will led to different situation, else if the user chooses “No” will have different result too. This is because human have their own way to do decision making. Based on their decision will have different results. Moreover, human have different knowledge about social engineering attack. Different people will also result different. For instance, a user which have cyber security information and user who does not have any cyber security information will also result differently. Hence, this awareness tools are help the user to gain the knowledge about social engineering attack.

## 3.2.4 Verification Plan

Use Case ID	UC001	Version	1.0
Feature	F001 Phishing Attack		
Purpose	To allow user to understand the phishing attack and have awareness.		
Actor	User		
Trigger	User click on the “laptop” on the table in game scenario.		
Precondition	System is at the main menu page.		
Scenario Name	Step	Action	
Main Flow	1	System prompt message for user	
	2	User click on the laptop on the table from the game scenario.	
	3	User is redirected to laptop home screen.	
	4	User click on the mail icon.	
	5	User is redirected to an email.	
	6	User able to view the Phishing email.	
	7	User clicks on the link.	
	8	System requests whether user want to click the link.	
	9	User select “Yes”	
	10	System prompt “You’ve been hacked!” message.	
	11	User click on “more info” will redirect to info about phishing attack.	
	12	User click on “example” will redirect to previous email will highlighted information to let user understand and have awareness.	
	13	User click on “back” will redirect to the game scenario for user to continue the game.	
Alternate Flow – Invalid option	2.1	User click on different thing on the game scenario.	
	2.2	System will redirect to different game scenario.	
	9.1	User select “No”	
	10.1	System prompt congrats message.	
	11.1	User click on “back” will redirect to the game scenario for user to continue the game.	
Rules	Clicked option must be a valid option (Laptop on the table).		

Table 3.3 Verification plan for phishing attack

Use Case ID	UC002	Version	1.0
Feature	F002 Smishing Attack		
Purpose	To allow user to understand the smishing attack and have awareness.		
Actor	User		
Trigger	User click on the “phone” on the table in game scenario.		
Precondition	System is at the main menu page.		
Scenario Name	Step	Action	
Main Flow	1	System prompt message for user	
	2	User click on the phone on the table from the game scenario.	
	3	User is redirected to phone home screen.	
	4	User click on the message icon.	
	5	User is redirected to an SMS.	
	6	User able to view the Smishing SMS.	
	7	User clicks on the phone number.	
	8	System requests whether user want to click the link.	
	9	User select “Yes”	
	10	System prompt “You’ve been hacked!” message.	
	11	User click on “more info” will redirect to info about smishing attack.	
	12	User click on “example” will redirect to previous email will highlighted information to let user understand and have awareness.	
	13	User click on “back” will redirect to the game scenario for user to continue the game.	
Alternate Flow – Invalid option	2.1	User click on different thing on the game scenario.	
	2.2	System will redirect to different game scenario.	
	9.1	User select “No”	
	10.1	System prompt congrats message.	
	11.1	User click on “back” will redirect to the game scenario for user to continue the game.	
Rules	Clicked option must be a valid option (Phone on the table).		

Table 3.4 Verification plan for smishing attack.

Use Case ID	UC003	Version	1.0
Feature	F003 Password exploitation Attack		
Purpose	To allow user to understand the phishing attack and have awareness.		
Actor	User		
Trigger	User click on the “laptop” on the table in game scenario.		
Precondition	System is at the main menu page.		
Scenario Name	Step	Action	
Main Flow	1	System prompt message for user	
	2	User click on the laptop on the table from the game scenario.	
	3	User is redirected to laptop home screen.	
	4	User click on the chrome icon.	
	5	User is redirected to a scene with login page	
	6	User able to choose login with email and password or back to eh game scene	
	7	User click the email column and fill in the email and password	
	8	System prompt “You’ve been hacked!” message.	
	9	User click on “more info” will redirect to info about phishing attack.	
		10	User click on “example” will redirect to a scene with highlighted information to let user understand and have awareness.
	13	User click on “back” will redirect to the game scenario for user to continue the game.	
Alternate Flow – Invalid option	2.1	User click on different thing on the game scenario.	
	2.2	System will redirect to different game scenario.	
	6.1	User click on “back” will redirect to the game scenario for user to continue the game.	
Rules	Clicked option must be a valid option (Laptop on the table).		

Table 3.5 Verification plan for password exploitation attack.

Use Case ID	UC004	Version	1.0
Feature	F004 Baiting Attack		
Purpose	To allow user to understand the baiting attack and have awareness.		
Actor	User		
Trigger	User click on the “USB” on the table in game scenario.		
Precondition	System is at the main menu page.		
Scenario Name	Step	Action	
Main Flow	1	System prompt message for user	
	2	User click on the USB on the table from the game scenario.	
	3	User is redirected to USB home screen.	
	4	User click on the USB icon.	
	5	User is redirected to a parking lot.	
	6	User able to view the many USB on the parking lot.	
	7	User clicks on the any of the USB.	
	8	System requests whether user want to pick up the USB and plug in to the laptop.	
	9	User select “Yes”	
	10	System prompt “You’ve been hacked!” message.	
	11	User click on “more info” will redirect to info about baiting attack.	
	12	User click on “example” will redirect to previous parking lot with highlighted information to let user understand and have awareness.	
	13	User click on “back” will redirect to the game scenario for user to continue the game.	
Alternate Flow – Invalid option	2.1	User click on different thing on the game scenario.	
	2.2	System will redirect to different game scenario.	
	9.1	User select “No”	
	10.1	System prompt congrats message.	
	11.1	User click on “back” will redirect to the game scenario for user to continue the game.	
Rules	Clicked option must be a valid option (USB on the table).		

Table 3.6 Verification plan for baiting attack.



Use Case ID	UC005	Version	1.0
Feature	F005 Tailgating Attack		
Purpose	To allow user to understand the tailaging attack and have awareness.		
Actor	User		
Trigger	User click on the “door” on the table in game scenario.		
Precondition	System is at the main menu page.		
Scenario Name	Step	Action	
Main Flow	1	System prompt message for user	
	2	User click on the door on the table from the game scenario.	
	3	User is redirected to door home screen.	
	4	User click on the door icon.	
	5	User is redirected to the scene.	
	6	User able to view two people at the door side.	
	7	User will get a message.	
	8	System requests whether user want to help the person to scan the access card to allow the person go in.	
	9	User select “Yes”	
	10	System prompt “You’ve been hacked!” message.	
	11	User click on “more” will redirect to info about baiting attack.	
	12	User click on “example” will redirect to an example with highlighted information to let user understand and have awareness.	
	13	User click on “back” will redirect to the game scenario for user to continue the game.	
Alternate Flow – Invalid option	2.1	User click on different thing on the game scenario.	
	2.2	System will redirect to different game scenario.	
	9.1	User select “No”	
	10.1	System prompt congrats message.	
	11.1	User click on “back” will redirect to the game scenario for user to continue the game.	
Rules	Clicked option must be a valid option (Door).		

Table 3.7 Verification plan for tailgating attack.

Use Case ID	UC006	Version	1.0
Feature	F00 Shoulder Surfing Attack		
Purpose	To allow user to understand the Shoulder Surfing attack and have awareness.		
Actor	User		
Trigger	User click on the “chair” on the table in game scenario.		
Precondition	System is at the main menu page.		
Scenario Name	Step	Action	
Main Flow	1	System prompt message for user	
	2	User click on the chair from the game scenario.	
	3	User is redirected to chair home screen.	
	4	User click on the door icon.	
	5	User is redirected to the scene.	
	6	User able to view two people one is using smart device then another person standing behind.	
	7	User will get a message.	
	8	System requests whether user will enter password when people standing behind.	
	9	User select “Yes”	
	10	System prompt “You are giving chance people know your password!” message.	
	11	User click on “more” will redirect to info about Shoulder Surfing attack.	
	12	User click on “example” will redirect to an example with highlighted information to let user understand and have awareness.	
	13	User click on “back” will redirect to the game scenario for user to continue the game.	
Alternate Flow – Invalid option	2.1	User click on different thing on the game scenario.	
	2.2	System will redirect to different game scenario.	
	9.1	User select “No”	
	10.1	System prompt congrats message.	
	11.1	User click on “back” will redirect to the game scenario for user to continue the game.	
Rules	Clicked option must be a valid option (Chair).		

Table 3.8 Verification plan for Shoulder Surfing attack

Use Case ID	UC007	Version	1.0
Feature	F007 Quiz		
Purpose	To allow user to understand the social engineering attack and have awareness.		
Actor	User		
Trigger	User click on the “quiz” on the table in game scenario.		
Precondition	System is at the main menu page.		
Scenario Name	Step	Action	
Main Flow	1	Score will set as default as 0	
	2	System prompt question for user with 4 selections	
	3	User select their answer	
	4	System prompt the next question for user with 4 selections	
	5	User select correct answer	
	6	Score will change by added 1	
	7	After 10 questions	
	8	System will display the score of the user	
	9	System prompt two selection “Retry” and “More Info”	
	10	User click on “More Info” will redirect to information scene of the quiz	
Alternate Flow – Invalid option	5.1	User select correct answer	
	5.2	Score will be remained no change	
	10.1	User click on “Retry” will redirect to quiz question for user	
Rules	Clicked option must be a valid option (Quiz).		

Table 3.9 Verification plan for Quiz.

Use Case ID	UC008	Version	1.0
Feature	F008 Video		
Purpose	To allow user to understand the different types of social engineering attack and have awareness.		
Actor	User		
Trigger	User click on the “Video” button on the menu in game scenario.		
Precondition	System is at the main menu page.		
Scenario Name	Step	Action	
Main Flow	1	System prompt five selection of different type of social engineering attack	
	2	User click on the first selection Brute force attack	
	3	User is redirected to Brute force attack video screen.	
	4	User clicks on the “back” button	
Alternate Flow – Invalid option	2.1	User click on the second selection Phishing attack	
	2.2	User click on the third selection SET toolkit attack	
	2.3	User click on the forth selection SQL Injection attack	
	2.4	User click on the fifth selection Tailagting attack	
	3.1	User is redirected to Phishing attack video screen.	
	3.2	User is redirected to SET toolkit attack video screen.	
	3.3	User is redirected to SQL Injection attack video screen.	
	3.4	User is redirected to Tailgating attack video screen.	
Rules	Clicked option must be a valid option (Video button).		

Table 3.10 Verification plan for Video.

### 3.3 System Design Diagram

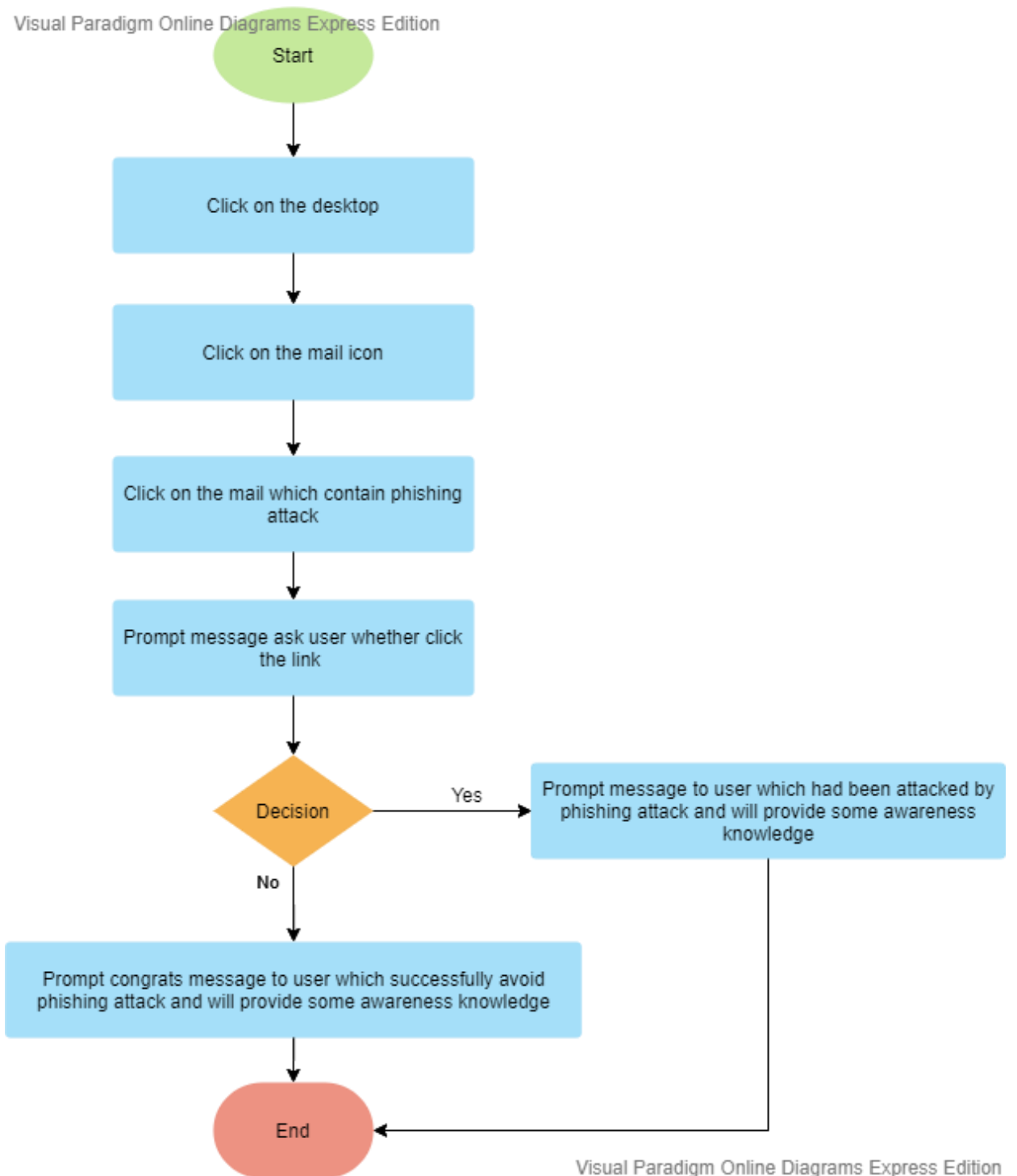


Figure 3.2: Overview of Phishing Attack.

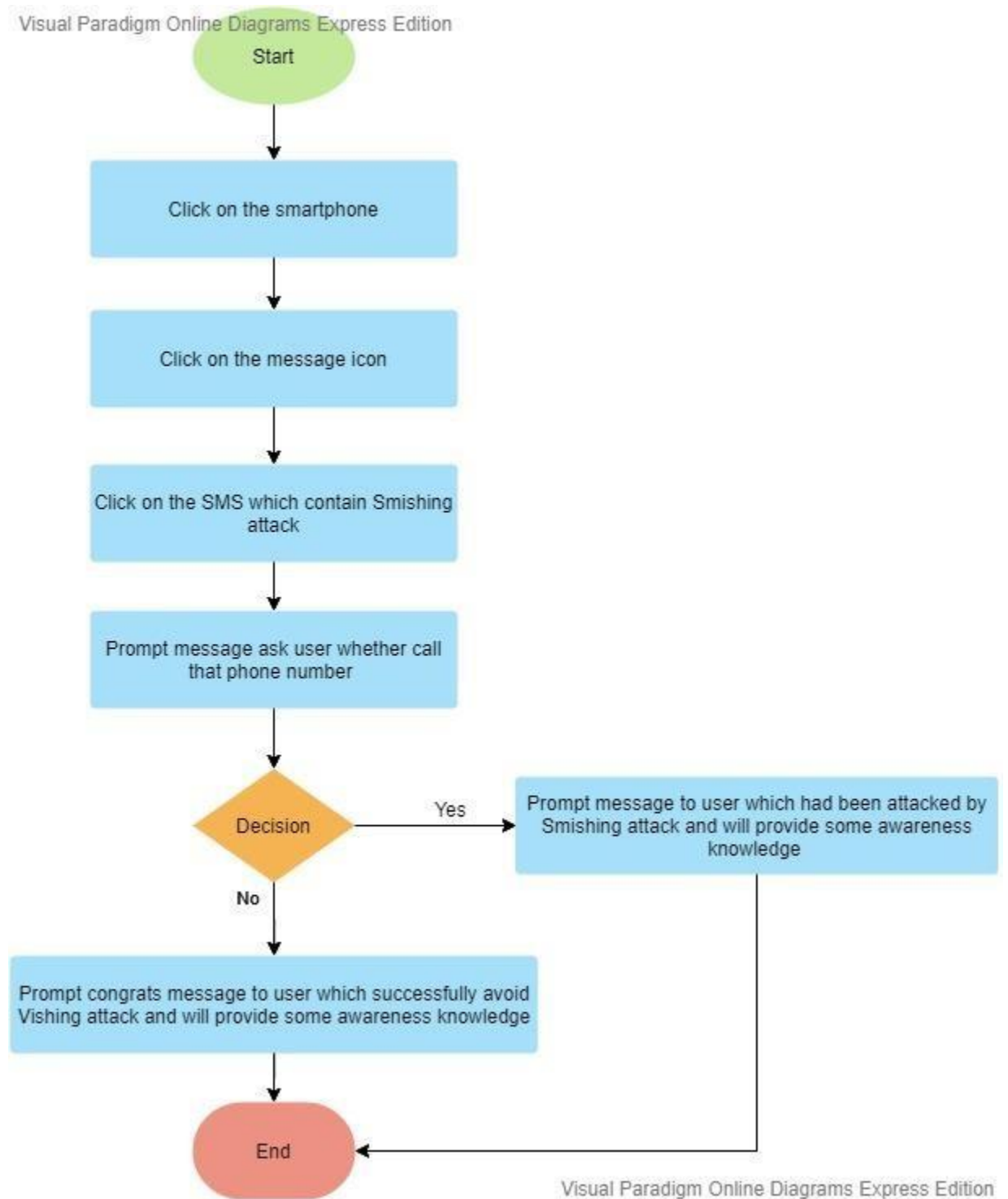


Figure 3.3: Overview of Smishing Attack

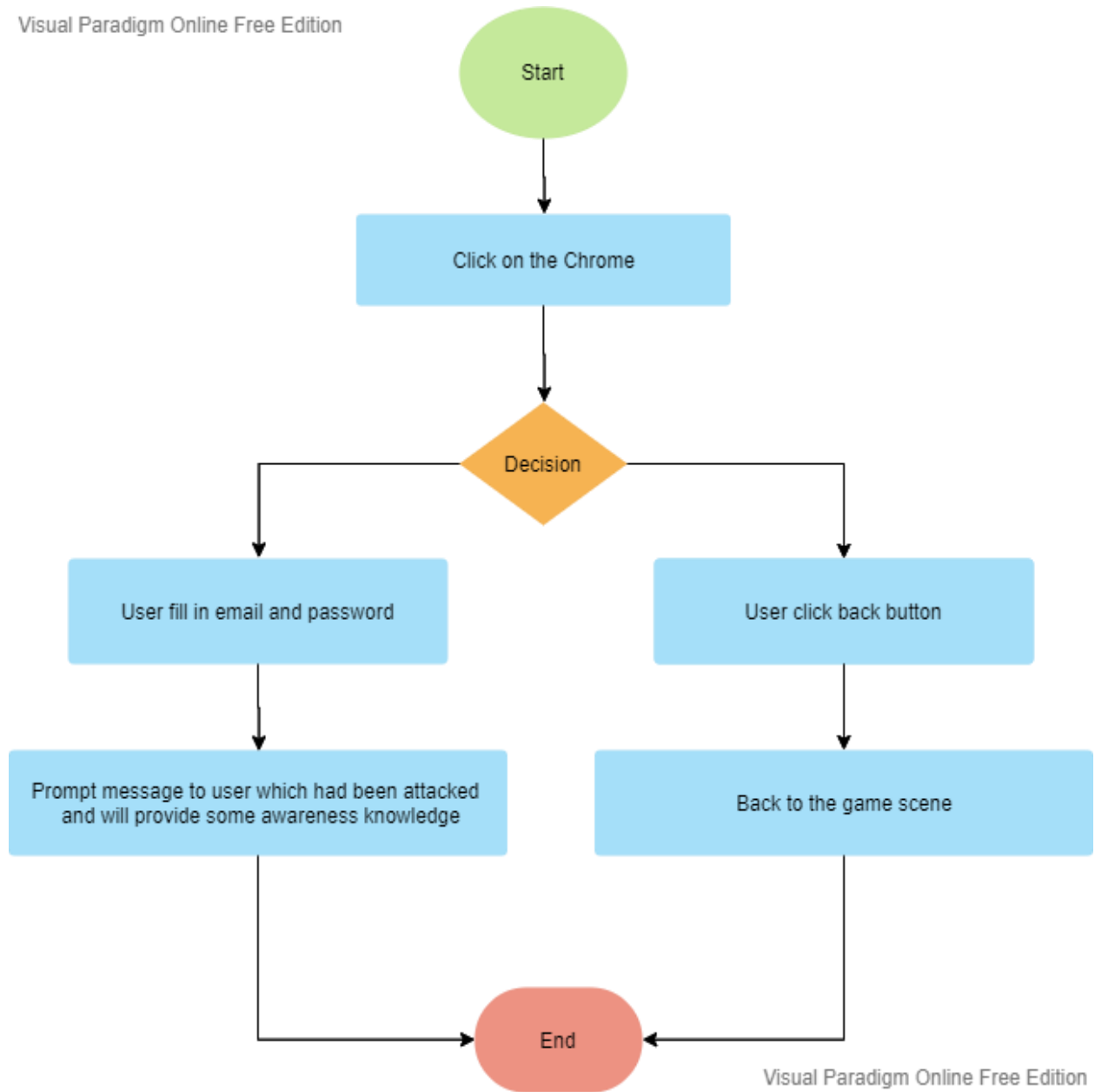


Figure 3.4: Overview of Password Exploitation Attack

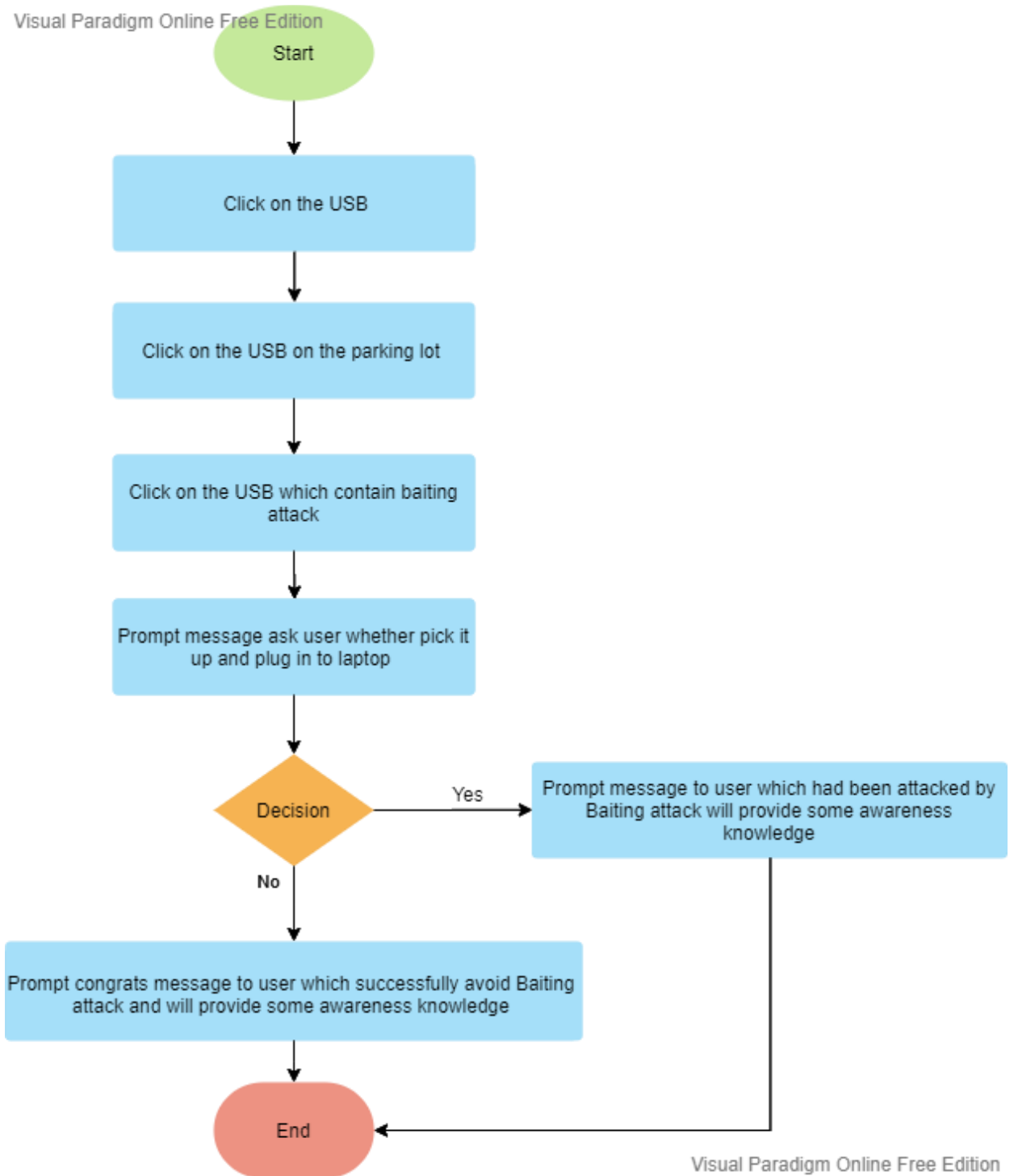


Figure 3.5: Overview of Baiting Attack



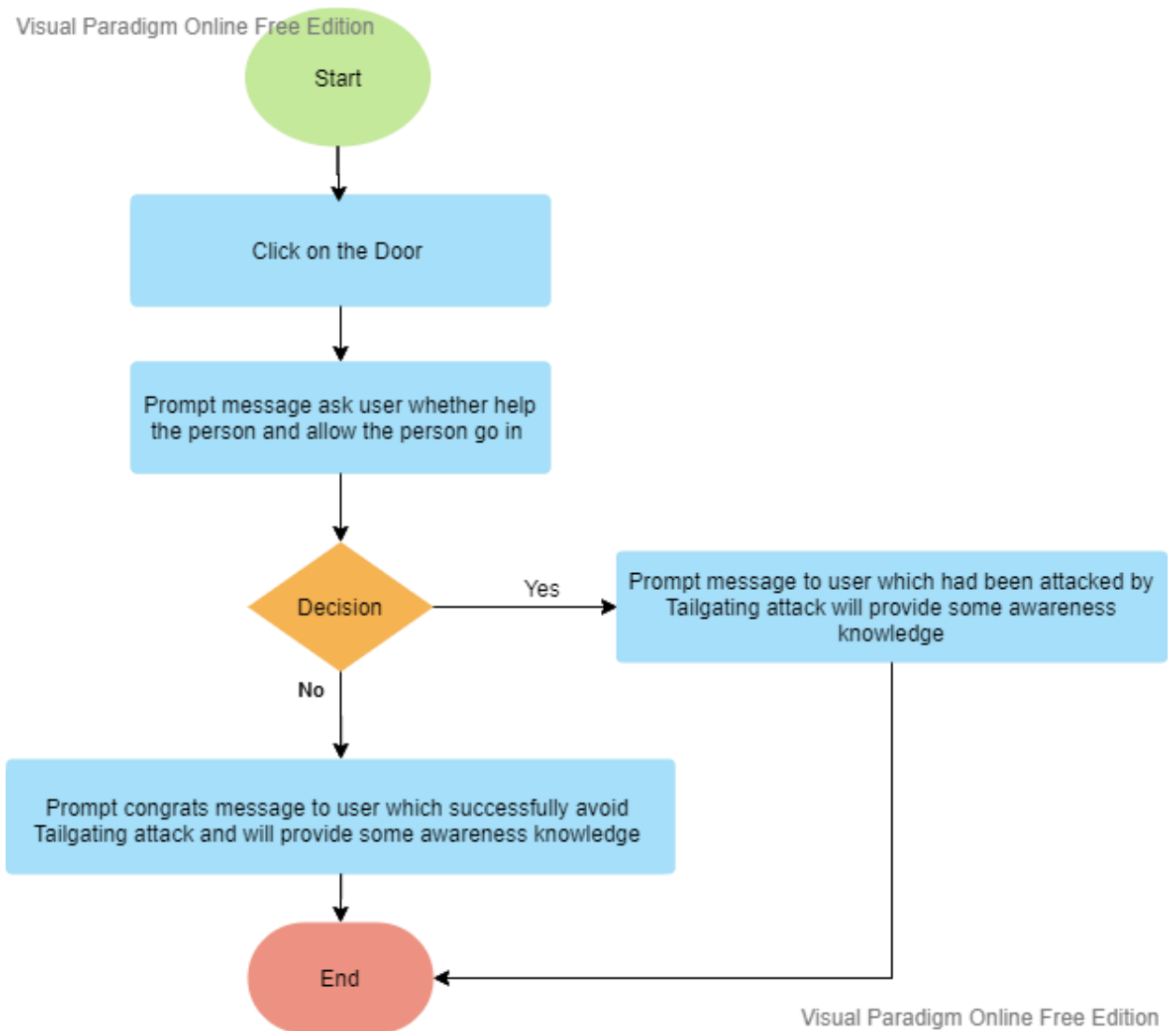


Figure 3.6: Overview of Tailgating Attack

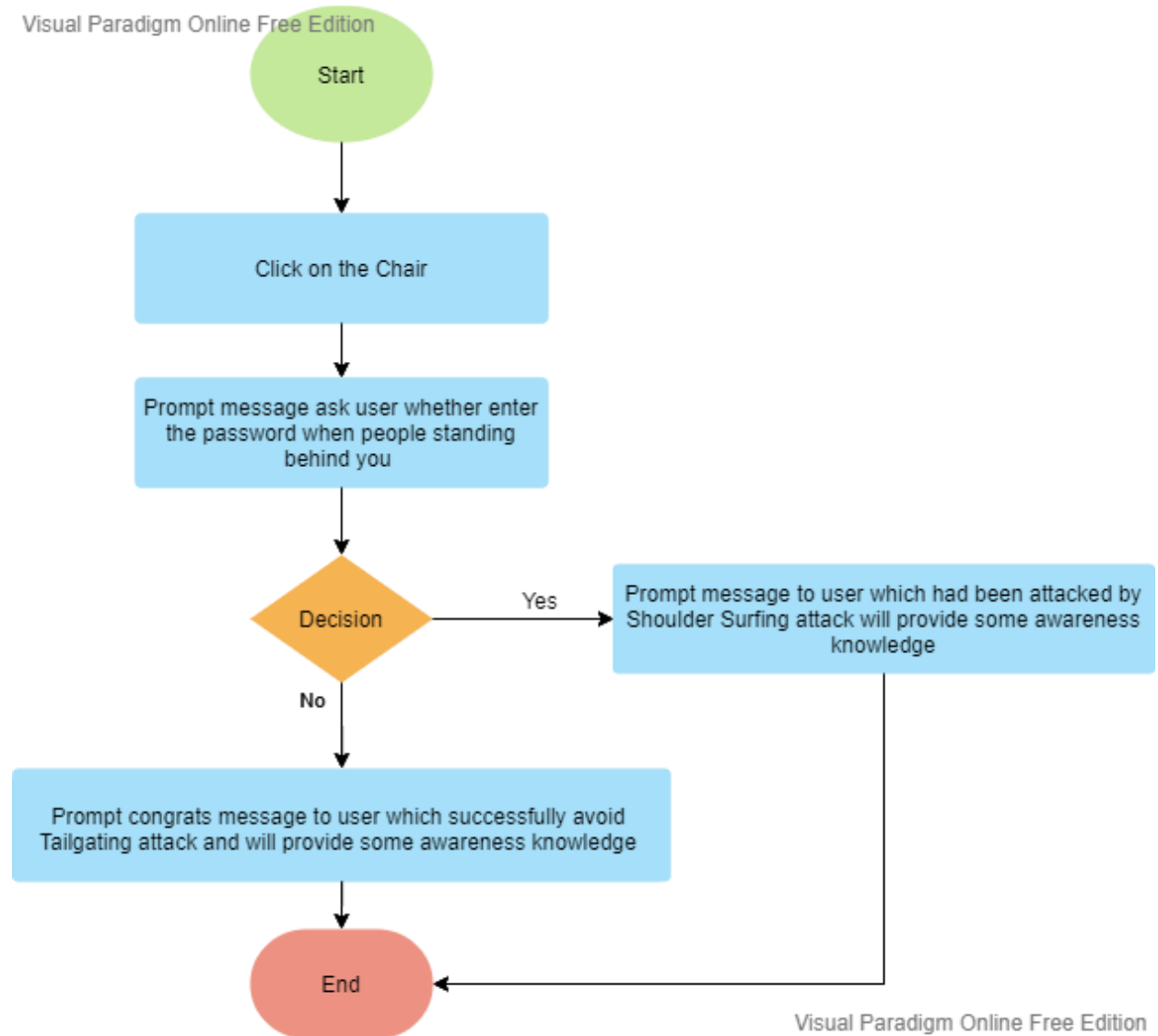
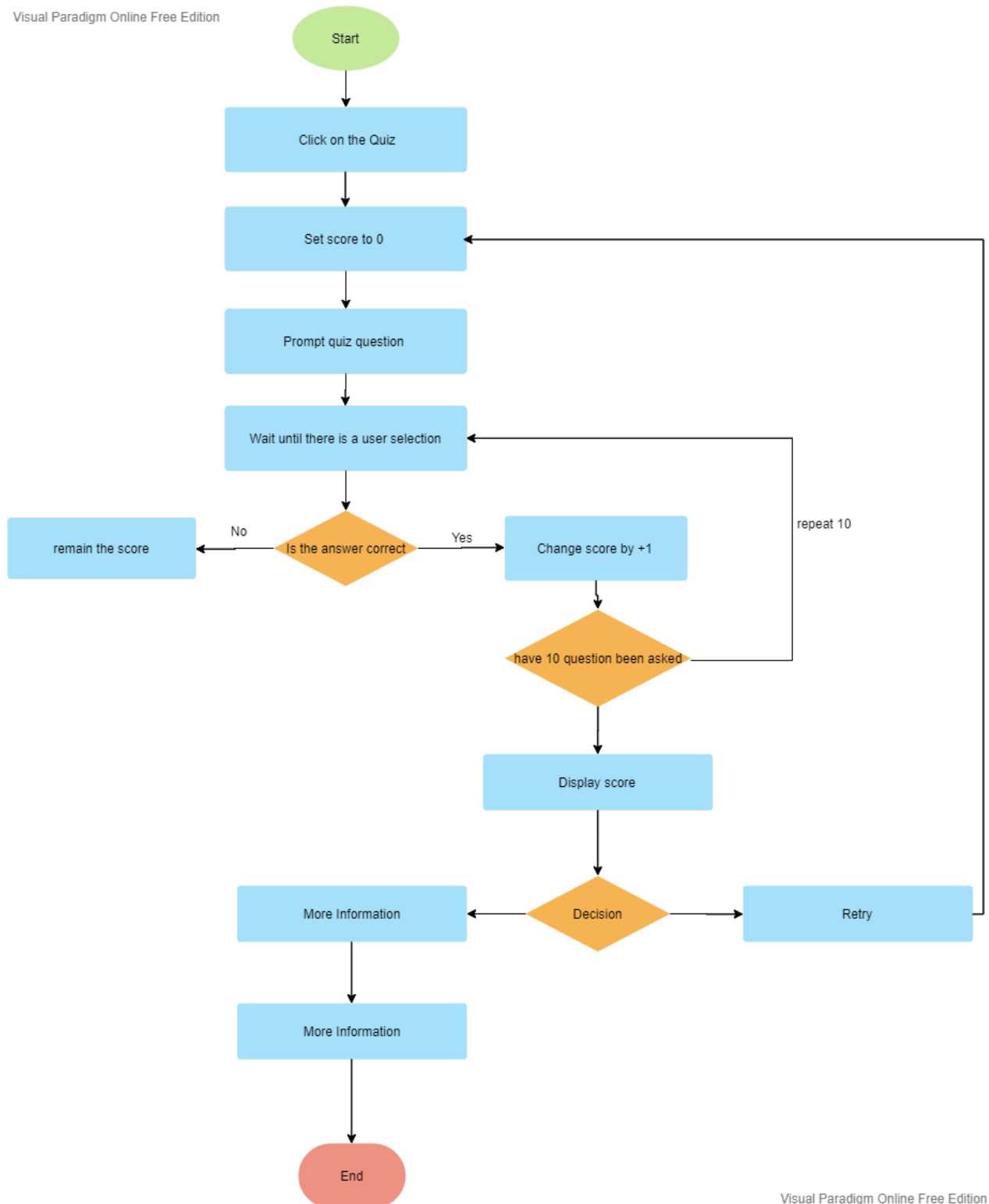


Figure 3.7: Overview of Shoulder surfing Attack

## CHAPTER 3 SYSTEM DESIGN

Visual Paradigm Online Free Edition



Visual Paradigm Online Free Edition

Figure 3.8: Overview of Quiz

Visual Paradigm Online Free Edition

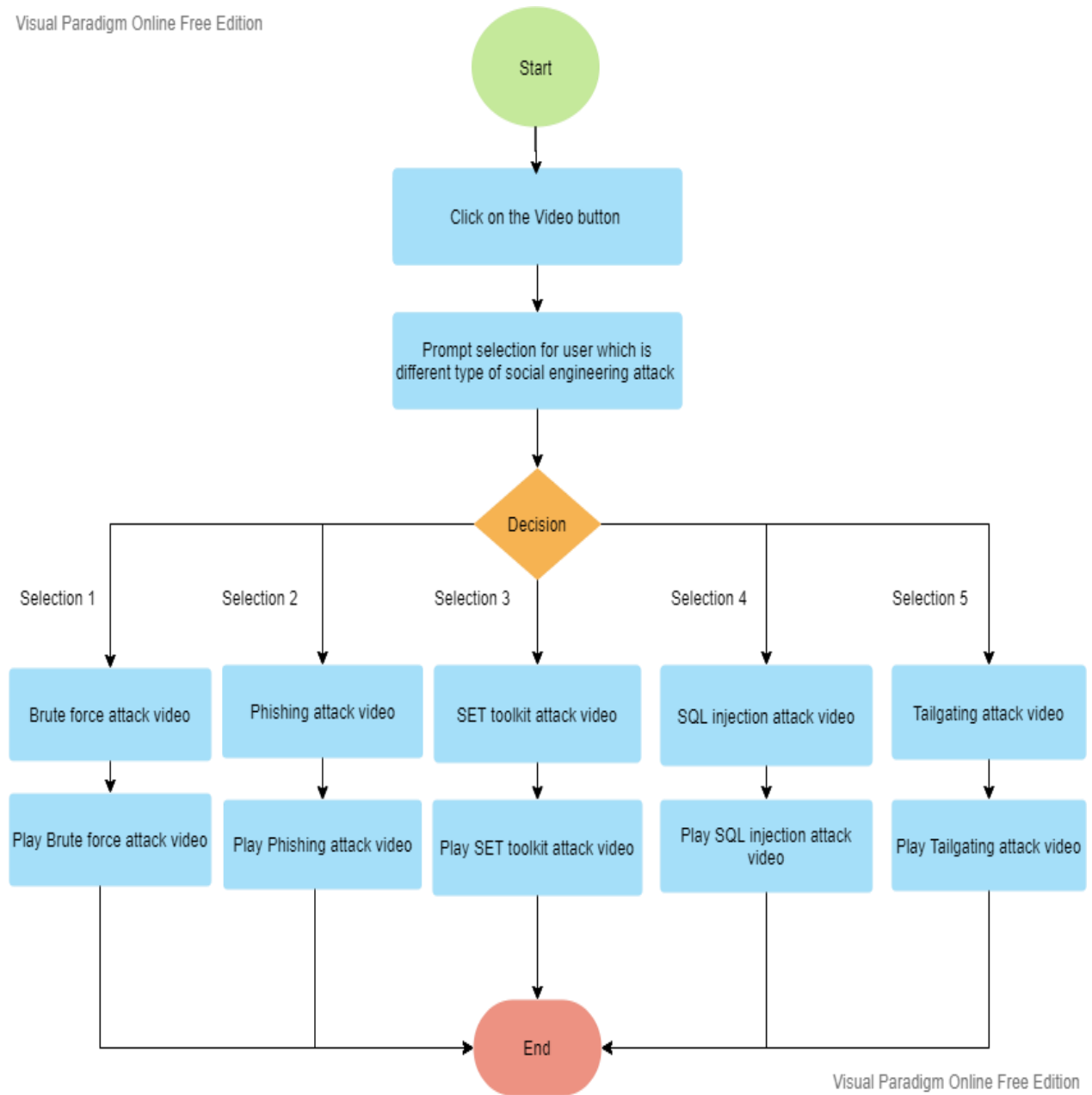


Figure 3.9: Overview of Video

### 3.4 Implementation Issues and Challenges

The major and the biggest issue of this project in implementation is there are lack of similar product in the market which mean lack of resources to implement this tool. There are a lot of different kind of SEAP but do not have any awareness tools to raise awareness and help user to understand the knowledge. Awareness tools still a new thing in the market, unlikely those traditional awareness program which already exist in the market for long period. Besides, there are lack of awareness tools to review or make improvement. Awareness tool become a new challenge for people to adapt it and use it. Perhaps a tool in digital based, with different features are most likely still not so popular but one day it will become the trending. Hence, those traditional ways will be replaced with the innovation of digital technology.

## CHAPTER 4 PRELIMINARY WORK

## CHAPTER 4 PRELIMINARY WORK

### 4.1 Chapter Overview

This chapter will explain the preliminary work done and results obtained according to the proposed method in Chapter 3.

### 4.2 Design Game Scenario

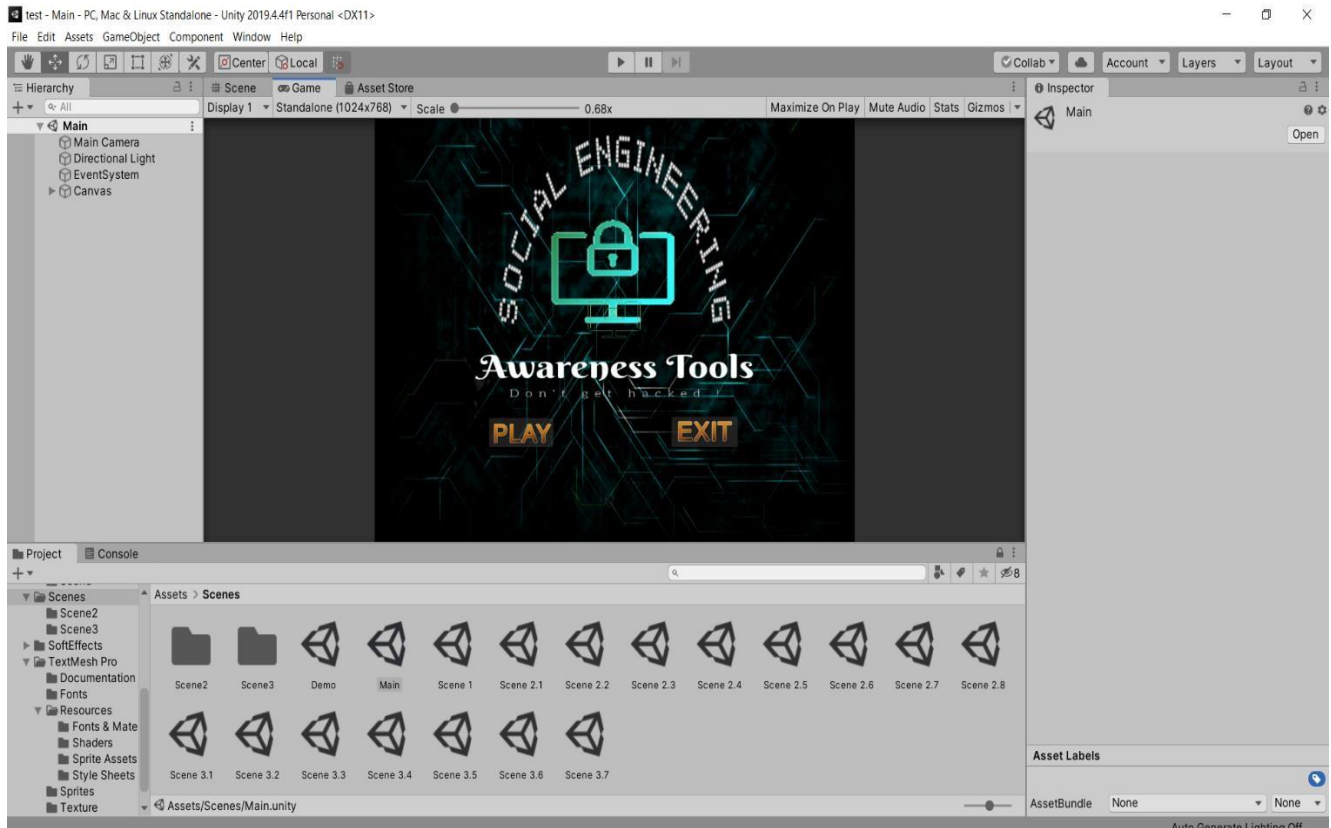


Figure 4.1: Main interface of the awareness tool game.

Unity Hub is a free and open source game creation engine. Unity empowers game designers to make games. It is used when modeling, animation, game creation of objects. This is the main interface of Social Engineering awareness tool it designed using Unity. The appearance of this awareness tool is having two buttons in the main interface which are “play” and “exit”. When user click the play button will redirect user to the main game scenario. In the main scenario, system will prompt message to user and give user some brief explanation before user start play the game. User can click on the dialog box will more description.

BIT (HONOURS) Communications and Networking  
Faculty of Information and Communication Technology (Kampar Campus), UTAR.

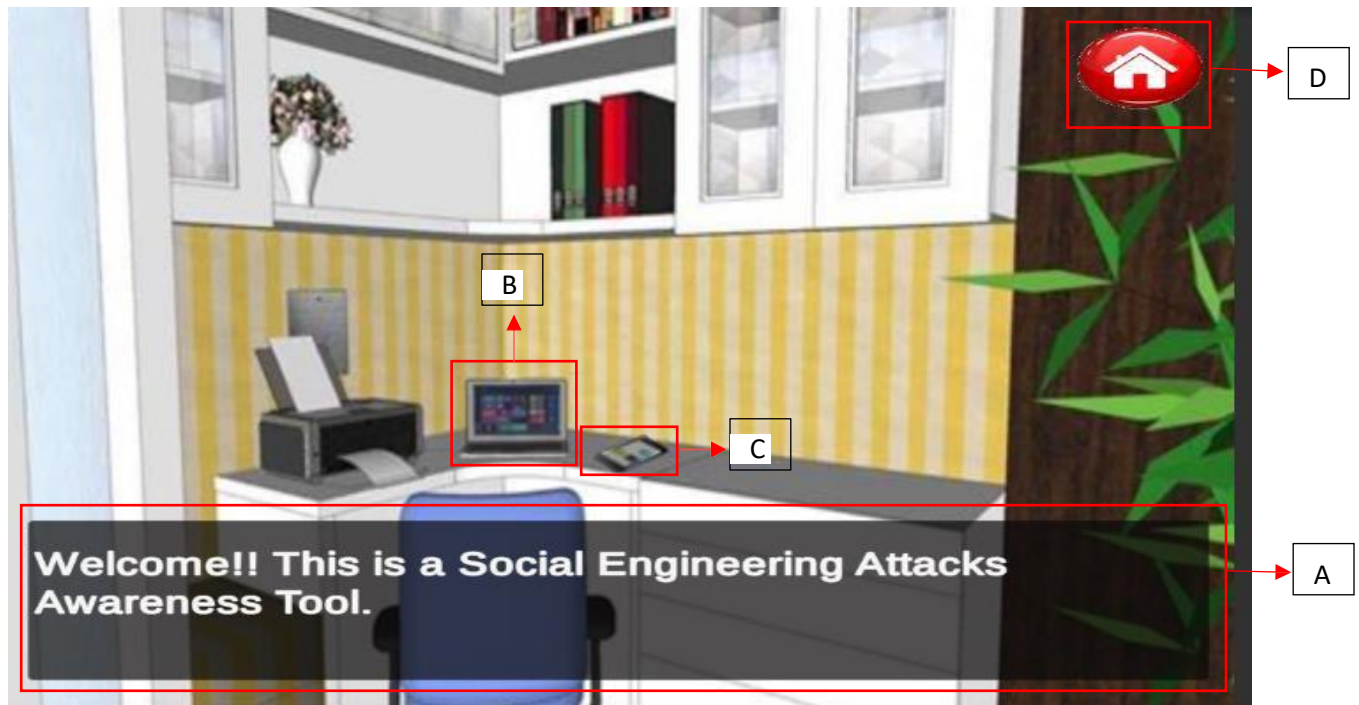


Figure 4.2: Main interface of the game scenario.

After the brief introduction of the game, user can click on the laptop or the phone on the table to start the game. The available game scenario is phishing attack and smishing attack which in different representative in laptop and phone respectively. When user click the “laptop” will redirect user to the different scene which is the home screen of the laptop with different icon. The phishing attack game scenario trigger by clicking the mail icon. There will be a Phishing mail in the game with malicious link attached inside the mail. When user click the link, will prompt message and ask user whether want to click the link. If user select “Yes”, will pop a message “You’ve been hacked!” below with a “more info” button. When user click the “more info” button will redirect user to next scene which show more information such as kind of attack and relevant descriptions of the attack, below have an “example” button. User click the button will show user the previous phishing email with highlighted things for user to aware some details can distinguish the real email or malicious email. On contrary, if user choose “No”, will pop congrats message to user successfully avoid phishing attack. Then, user can choose to know more about the attack or back to the game scene to try others game.

### 4.2.1 Scene1: Phishing attack

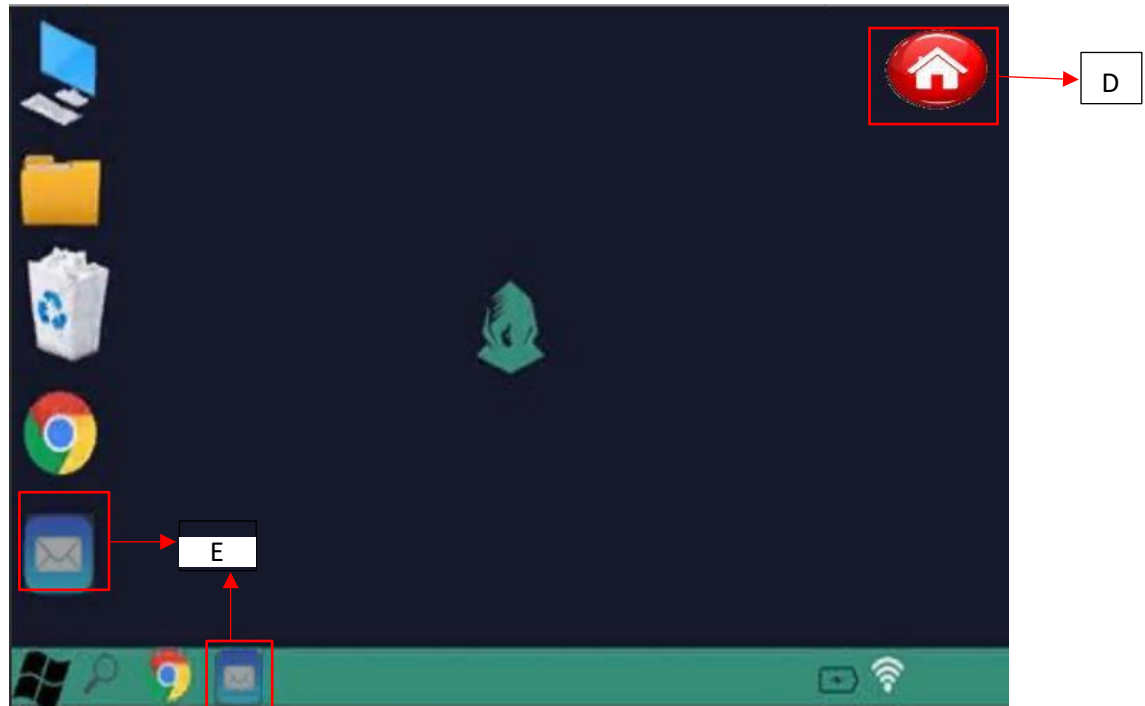


Figure 4.3: Main interface of the Phishing attack scenario.

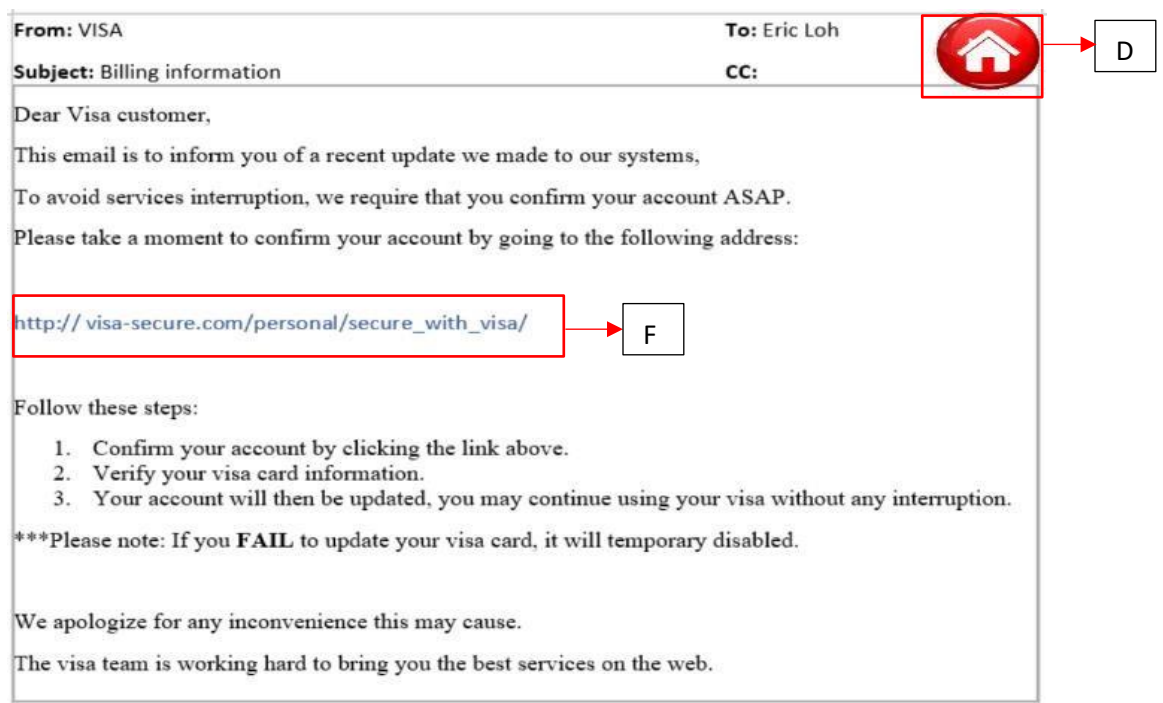


Figure 4.4: Phishing mail with malicious link.



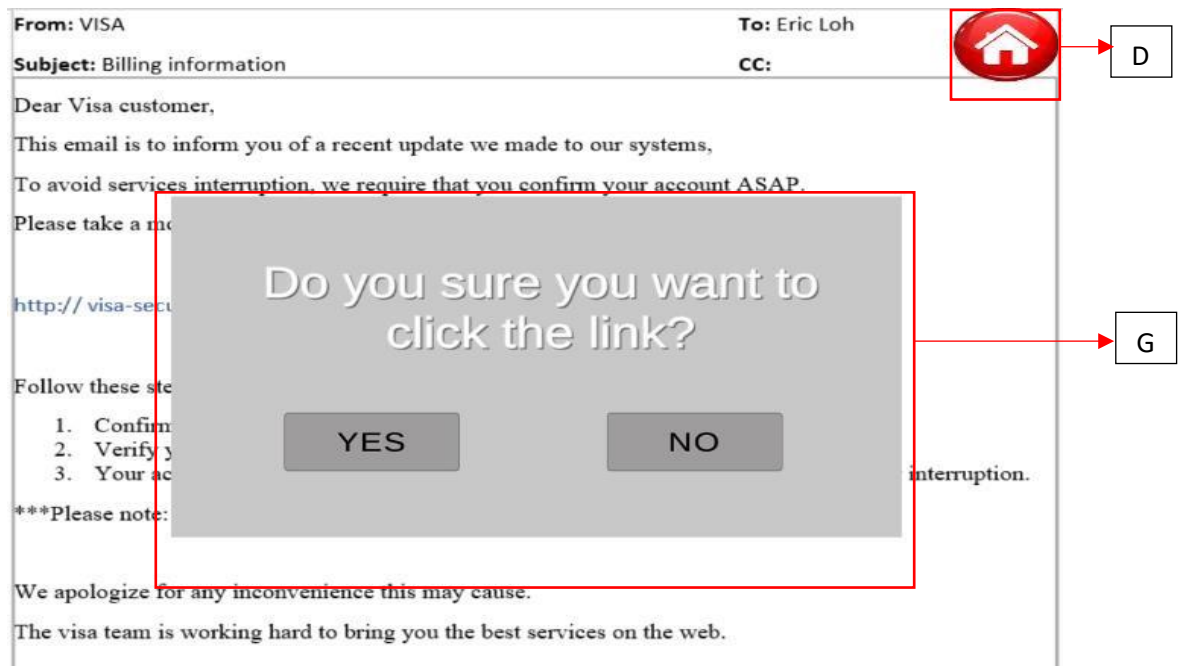


Figure 4.5: When user click at the link will prompt user a message to select whether click this link with two option “Yes” and “No”.

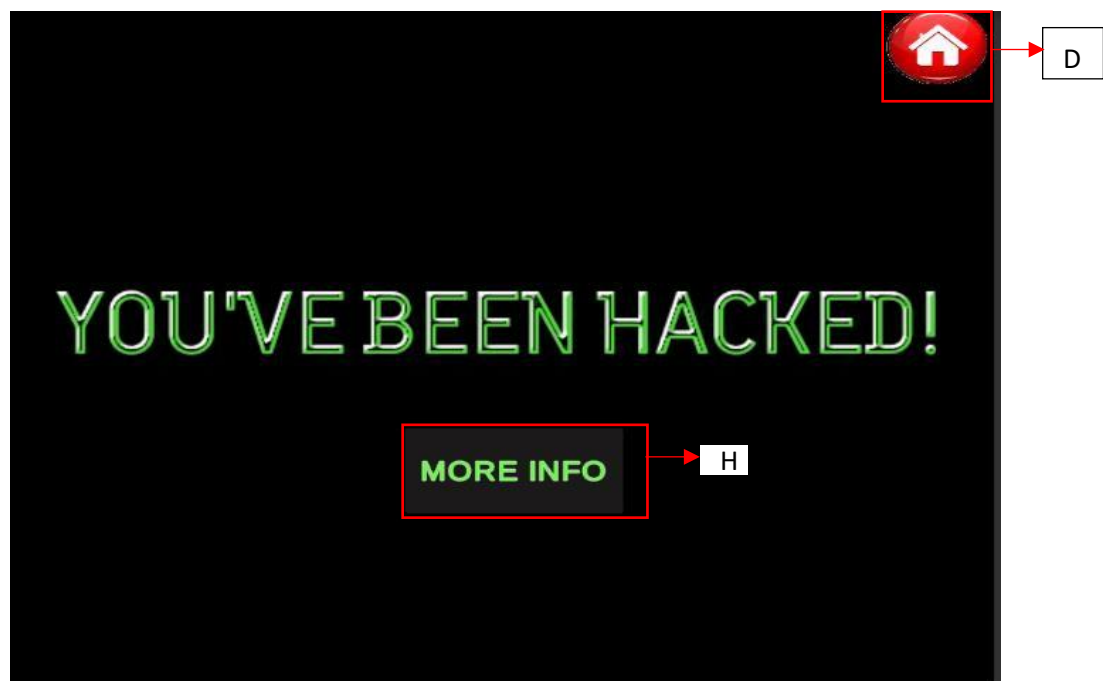


Figure 4.6: If user select “Yes”, will pop this message to user, user can click on the “more info” button to understand which attack and relevant information.



Figure 4.7: When user click on “more info” button, will show this information.

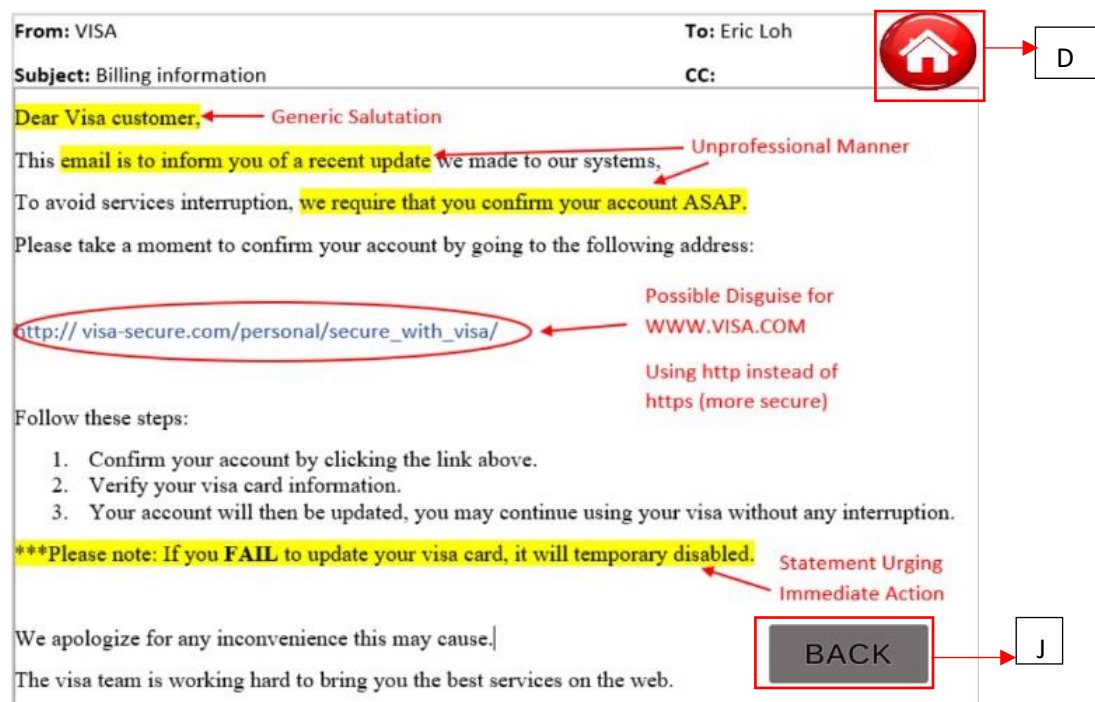


Figure 4.8: When user click on “example” button, will some the previous malicious mail and highlighted information for user to aware some details can distinguish the real email or malicious email.

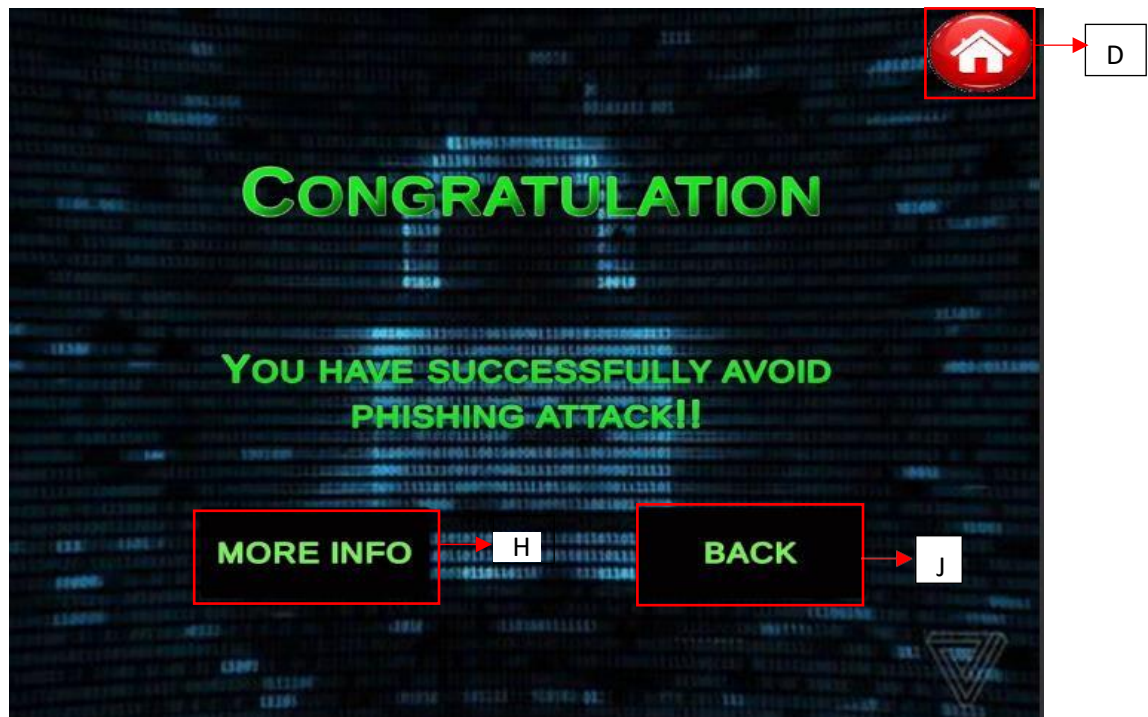


Figure 4.9: If user select “No”, will pop congrats message to user, user can click on the “more info” button to understand which attack and relevant information or click the back button to continue the game.

#### **4.2.2 Scene2 Smishing Attack**



Figure 4.10: Main interface of the Smishing attack scenario.



Figure 4.11: Smishing attack with malicious number.

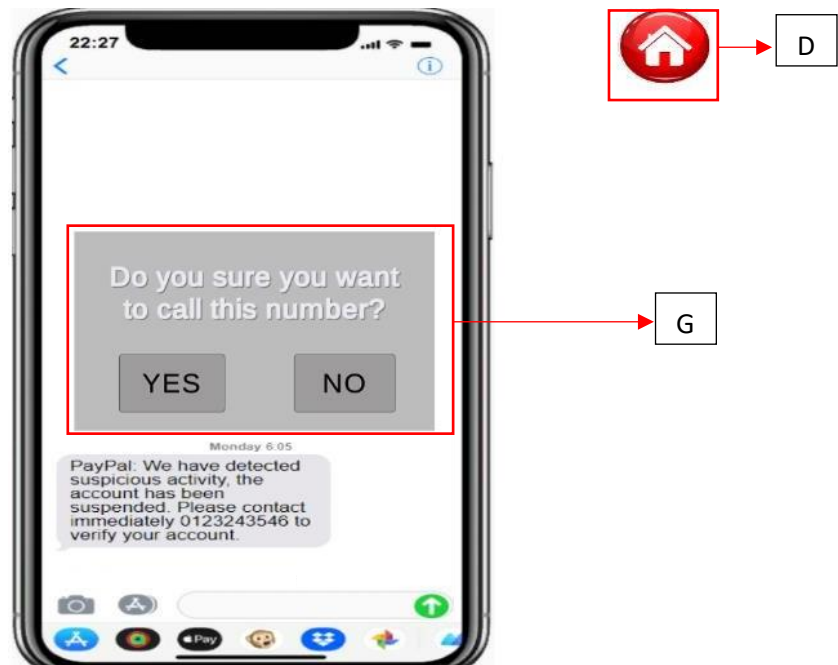


Figure 4.12: When user click at the link will prompt user a message to select whether click this link with two option “Yes” and “No”.

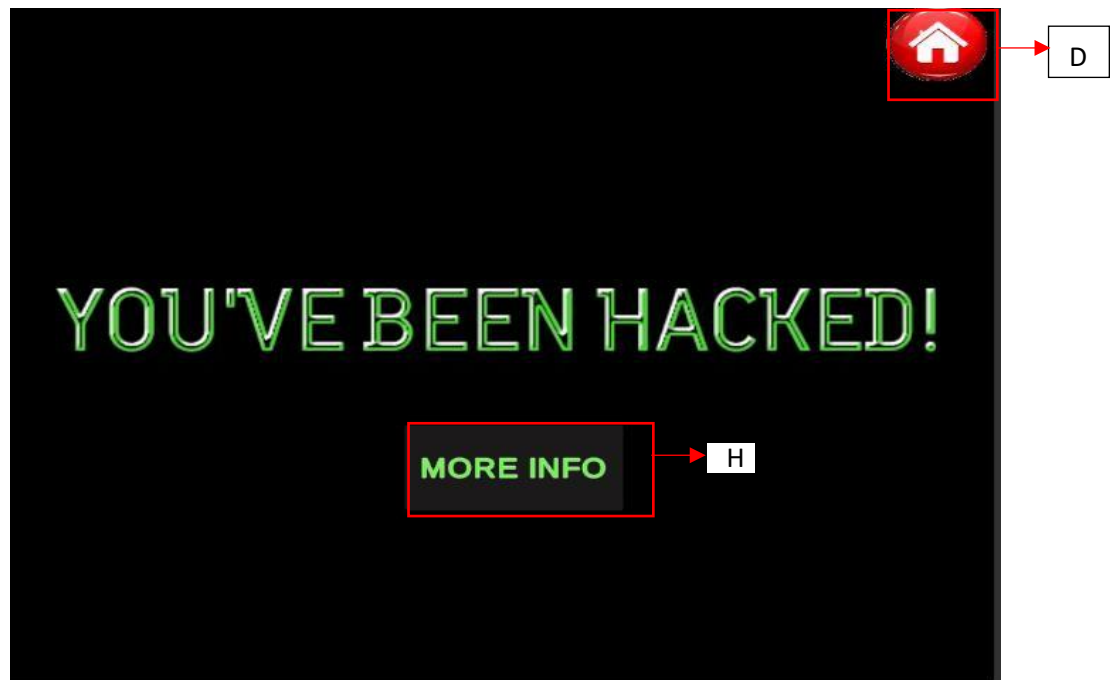


Figure 4.13: If user select “Yes”, will pop this message to user, user can click on the “more info” button to understand which attack and relevant information.

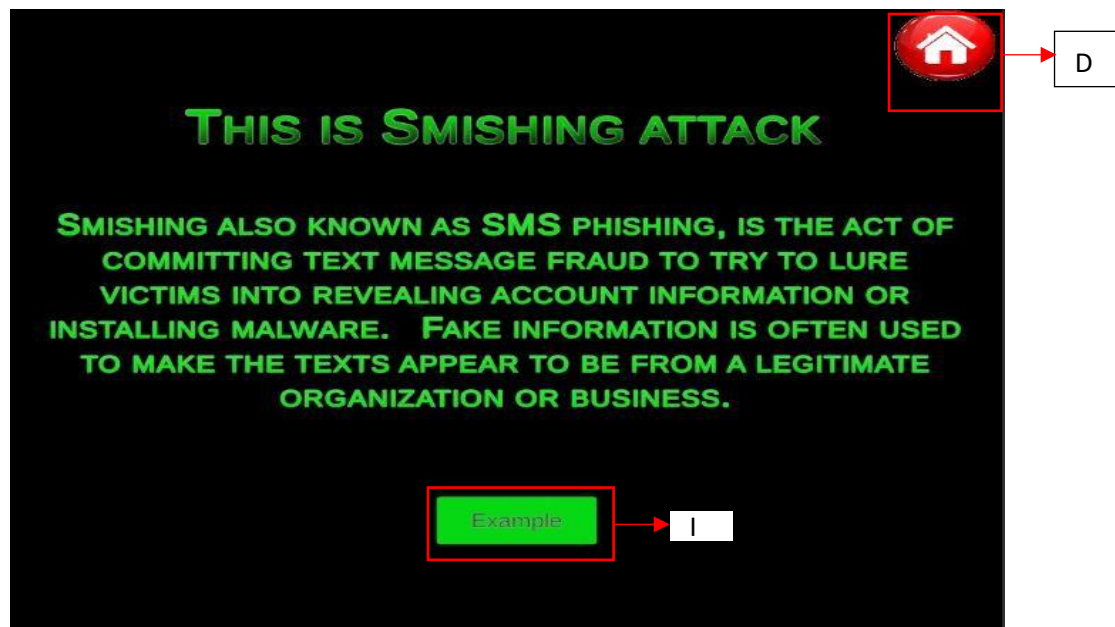


Figure 4.14: When user click on “more info” button, will show this information.





Figure 4.15: When user click on “example” button, will some the previous malicious SMS and highlighted information for user to aware some details can distinguish the real SMS or malicious SMS.



Figure 4.16: If user select “No”, will pop congrats message to user, user can click on the “more info” button to understand which attack and relevant information or click the back button to continue the game.

## CHAPTER 4 PRELIMINARY WORK

Label	Name	Function
A	Dialog box	Brief introduction when clicked this dialog box.
B	Laptop	Phishing attack scene when clicked this button.
C	Phone	Smishing attack scene when clicked this button.
D	Home button	Back to Game scene when clicked this button.
E	Mail icon	Phishing email scene when clicked this link.
F	Malicious link	Phishing attack contain in this link when clicked this link.
G	Selection box	Different selection will have different result.
H	More info button	Relevant information and type of attack when clicked this button.
I	Example button	Relevant example with highlighted information when clicked this button.
J	Back button	Back to Game scene when clicked this button.
K	Message icon	Smishing scene when clicked this link.
L	Malicious number	Smishing attack contain in this link when clicked this link.

Table 4.1 Function of game scenario scene feature.

## CHAPTER 5 SYSTEM IMPLEMENTATION

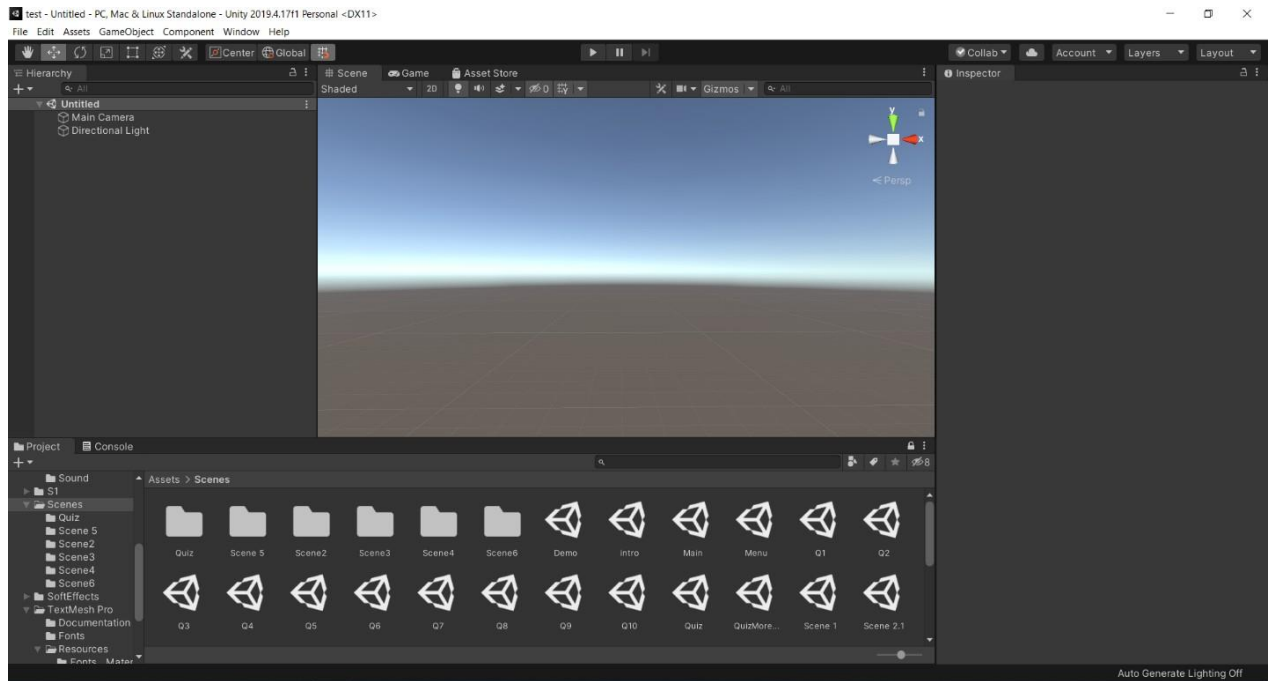


Figure 5.1 Develop the whole game by using Unity

The whole game application includes Quiz, game module and video module are created and designed by using unity as shown as Figure 5.1.

### 5.1 Development of Main scene

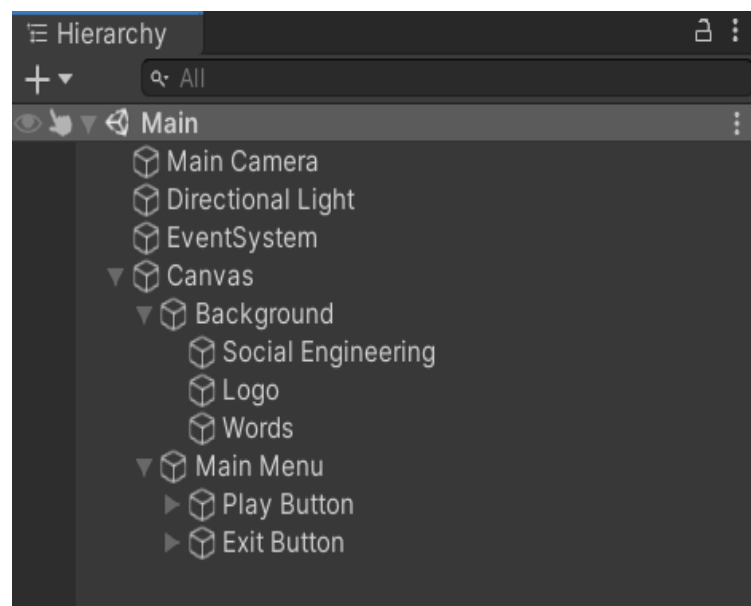


Figure 5.2 Hierarchy of Main scene



Figure 5.2 shows the development of Main scene which is the first scene when the application is started. This scene develops the structure of main scene, built the play and exit buttons. In order to build up this scene, there are some components are required to create main scene of game stimulation. Main components in this scene are stated at the table below.

Main Components	Explanation
Main Camera	The first enabled camera tagged "MainCamera" Therefore, you just change the tag of the camera you want to be it, and the tag of the one that had previously been it.
Directional Light	Create light for the scene.
EventSystem	Sending events to objects in the application based on input.
Canvas	Create UI such as background image, logo, play and exit button and texts.

Table 5.1 Main components in Main scene

## 5.2 Development of Introduction scene

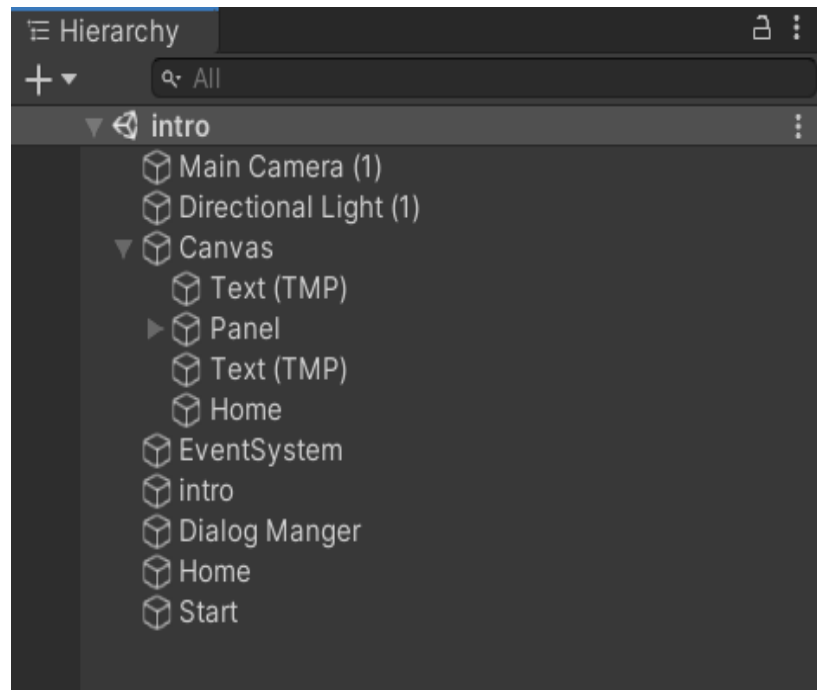


Figure 5.3 Hierarchy of Introduction scene

Figure 5.3 shows the development of Introduction scene which is the second scene when the application clicked the play button. This scene develops the structure of introduction scene, with a short introduction of this application and start button. In order to build up this scene, there are some components are required to create introduction scene of game stimulation. Main components in this scene are stated at the table below.

Main Components	Explanation
Main Camera	The first enabled camera tagged "MainCamera" Therefore, you just change the tag of the camera you want to be it, and the tag of the one that had previously been it.
Directional Light	Create light for the scene.
EventSystem	Sending events to objects in the application based on input.
Canvas	Create UI such as background image, logo, play and exit button and texts.
Panel	Panel is an upper-level UI container in which to arrange widgets. Layout object that controls how its widgets are arranged on the screen.
Text(TMP)	TMP is TextMesh Pro which is a replacement for Unity's existing text components. TextMesh Pro uses Signed Distance Field (SDF) as its primary text rendering pipeline making it possible to render text cleanly at any point size and resolution.
Dialog Manger	This contains introduction script
Home	This is used to go back the main scene
Start	This is used to go enter the menu scene

Table 5.2 Main components in Introduction scene

### 5.3 Development of Menu scene

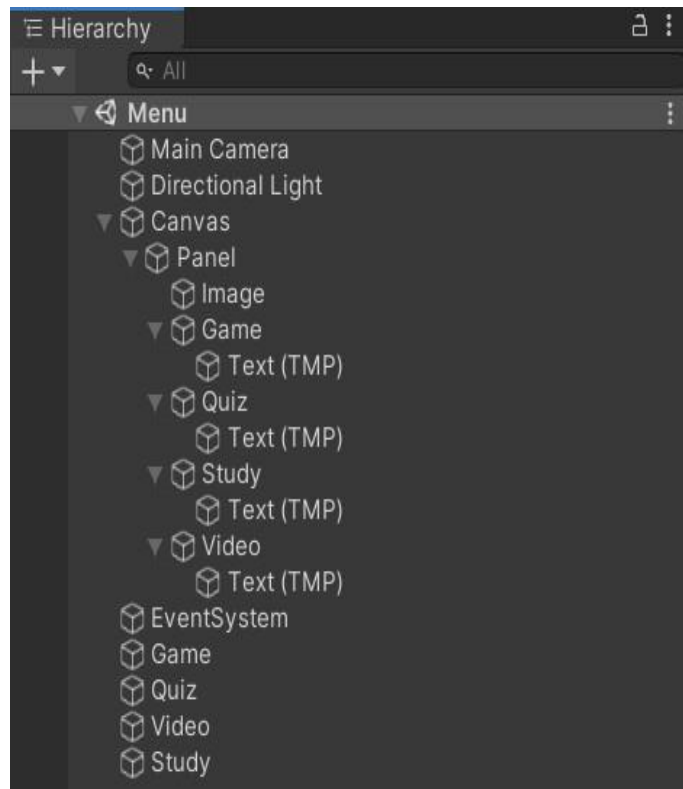


Figure 5.4 Hierarchy of Menu scene

Figure 5.4 shows the development of Menu scene which is the third scene when the application clicked the start button. This scene develops the structure of menu scene, with four different buttons which are game, quiz, video and study of this application. In order to build up this scene, there are some components are required to create introduction scene of game stimulation. Main components in this scene are stated at the table below.

Main Components	Explanation
Main Camera	The first enabled camera tagged "MainCamera" Therefore, you just change the tag of the camera you want to be it, and the tag of the one that had previously been it.
Directional Light	Create light for the scene.
EventSystem	Sending events to objects in the application based on input.

Canvas	Create UI such as background image, logo, play and exit button and texts.
Panel	Panel is an upper-level UI container in which to arrange widgets. Layout object that controls how its widgets are arranged on the screen.
Image	This is the background image
Game	This is used to go enter the game scene
Quiz	This is used to go enter the quiz scene
Study	This is used to go enter the study scene
Video	This is used to go enter the video scene
Text(TMP)	TMP is TextMesh Pro which is a replacement for Unity's existing text components. TextMesh Pro uses Signed Distance Field (SDF) as its primary text rendering pipeline making it possible to render text cleanly at any point size and resolution.
Home	This is used to go back the main scene

Table 5.3 Main components in menu scene

### 5.4 Development of Quiz scene

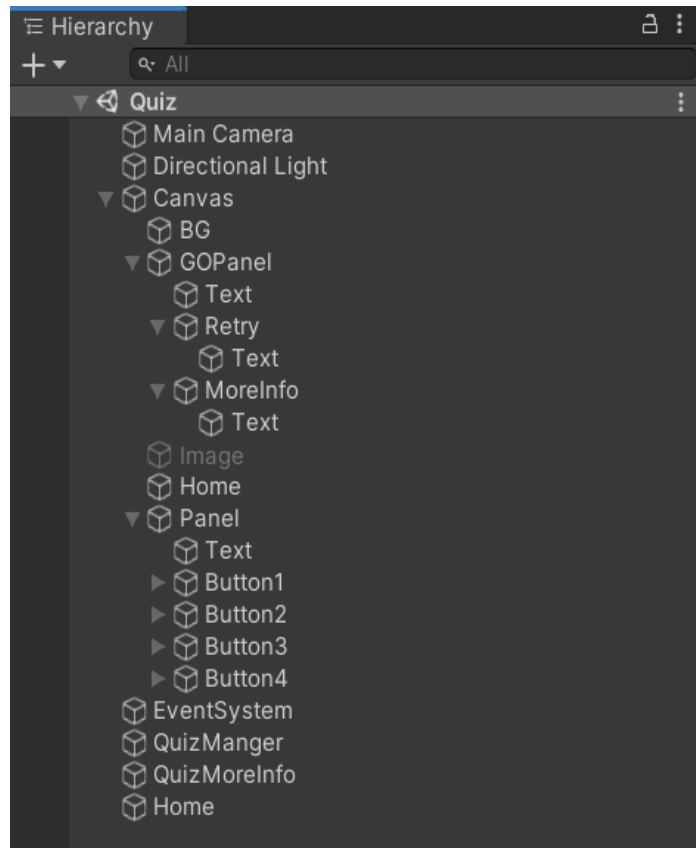


Figure 5.5 Hierarchy of Quiz scene

Figure 5.5 shows the development of Quiz scene is the scene when the application clicked the quiz button. This scene develops the structure of quiz scene, with four option buttons which for the quiz selection and each question of this application. In order to build up this scene, there are some components are required to create introduction scene of game stimulation. Main components in this scene are stated at the table below.

Main Components	Explanation
Main Camera	The first enabled camera tagged "MainCamera" Therefore, you just change the tag of the camera you want to be it, and the tag of the one that had previously been it.
Directional Light	Create light for the scene.
EventSystem	Sending events to objects in the application based on input.

Canvas	Create UI such as background image, logo, play and exit button and texts.
Panel	Panel is an upper-level UI container in which to arrange widgets. Layout object that controls how its widgets are arranged on the screen.
GOPanel	GOPanel is Game Over Panel when end of the game will pop up the score for user.
BG	This is the background image
Retry	This is used to go try again the quiz
MoreInfo	This is used to go enter the more information scene
Text	Text is the text components every words in this scene
Button 1	This is the selection 1
Button 2	This is the selection 2
Button 3	This is the selection 3
Button 4	This is the selection 4
QuizManager	This contains every question of the quiz
QuizMoreInfo	This contains more information of the quiz
Home	This is used to go back the main scene

Table 5.4 Main components in quiz scene

### 5.5 Development of Game scene

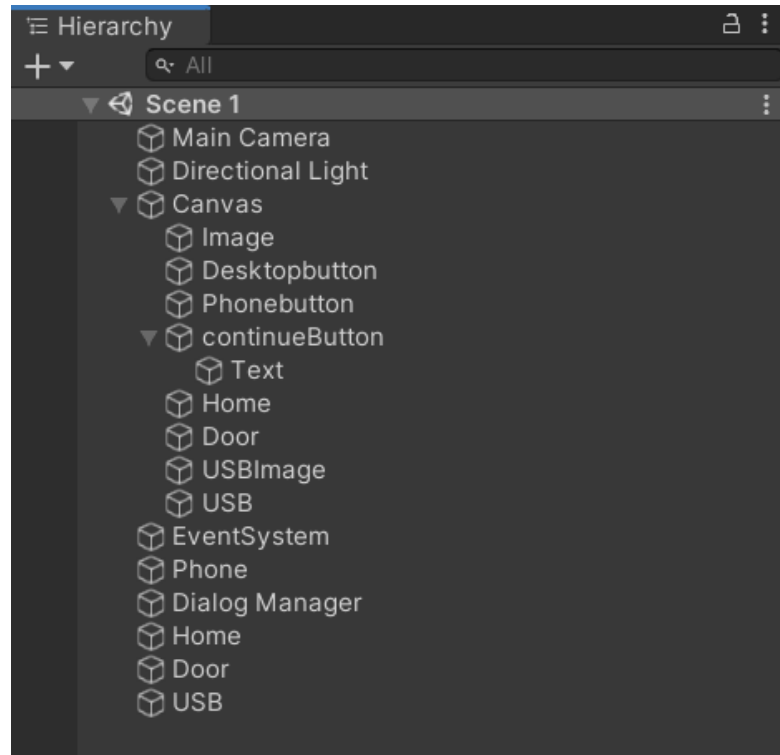


Figure 5.6 Hierarchy of Game scene

Figure 5.6 shows the development of Game scene is the scene when the application clicked the game button. This scene develops the structure of game scene, with varies option buttons which for the different social engineering attack game of this application. In order to build up this scene, there are some components are required to create introduction scene of game stimulation. Main components in this scene are stated at the table below.

Main Components	Explanation
Main Camera	The first enabled camera tagged "MainCamera" Therefore, you just change the tag of the camera you want to be it, and the tag of the one that had previously been it.
Directional Light	Create light for the scene.
EventSystem	Sending events to objects in the application based on input.

Canvas	Create UI such as background image, logo, play and exit button and texts.
Panel	Panel is an upper-level UI container in which to arrange widgets. Layout object that controls how its widgets are arranged on the screen.
Text	Text is the text components every word in this scene
Desktopbutton	This is the Desktop on the table
Phonebutton	This is the Phone on the table
Continuebutton	This is the dialog to welcome user n short introduction for user
USB	This is the Desktop on the table
Door	This is the door in the game
Dialog Manger	This contains introduction script
Home	This is used to go back the main scene

Table 5.5 Main components in game scene



## 5.6 Development of Study scene

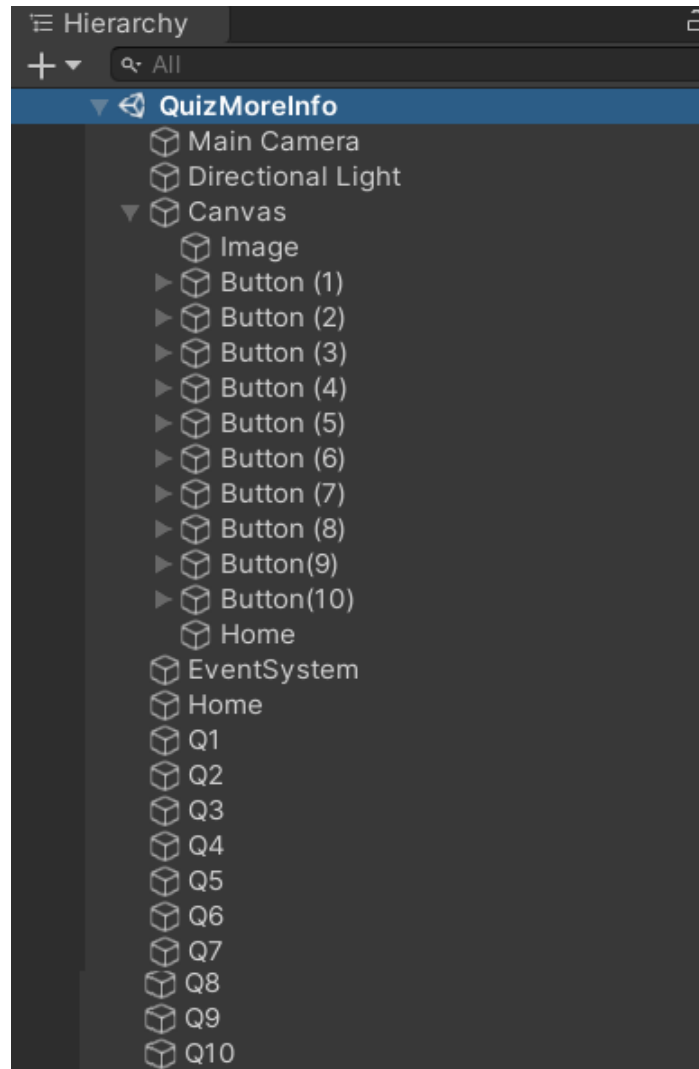


Figure 5.7 Hierarchy of Study scene

Figure 5.7 shows the development of Study scene is the scene when the application clicked the study button. This scene develops the structure of study scene, with ten option buttons which for the information for quiz of this application. In order to build up this scene, there are some components are required to create introduction scene of game stimulation. Main components in this scene are stated at the table below.

Main Components	Explanation
Main Camera	The first enabled camera tagged "MainCamera" Therefore, you just change the tag of the camera you want to be it, and the tag of the one that had previously been it.
Directional Light	Create light for the scene.
EventSystem	Sending events to objects in the application based on input.
Canvas	Create UI such as background image, logo, play and exit button and texts.
Panel	Panel is an upper-level UI container in which to arrange widgets. Layout object that controls how its widgets are arranged on the screen.
Image	This is the background image
Button 1	This is the information 1 for quiz
Button 2	This is the information 2 for quiz
Button 3	This is the information 3 for quiz
Button 4	This is the information 4 for quiz
Button 5	This is the information 5 for quiz
Button 6	This is the information 6 for quiz
Button 7	This is the information 7 for quiz
Button 8	This is the information 8 for quiz
Button 9	This is the information 9 for quiz
Button 10	This is the information 10 for quiz
Home	This is used to go back the main scene

Table 5.6 Main components in study scene

### 5.7 Development of Video scene

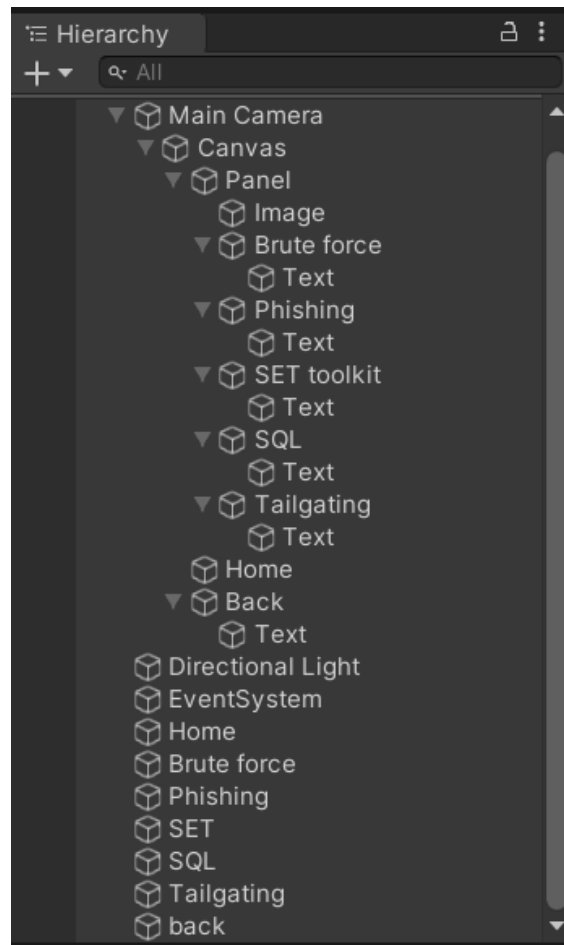


Figure 5.8 Hierarchy of Video scene

Figure 5.7 shows the development of Video scene is the scene when the application clicked the video button. This scene develops the structure of video scene, with four option buttons which for the type of social engineering attack video for this application. In order to build up this scene, there are some components are required to create introduction scene of game stimulation. Main components in this scene are stated at the table below.

Main Components	Explanation
Main Camera	The first enabled camera tagged "MainCamera" Therefore, you just change the tag of the camera you want to be it, and the tag of the one that had previously been it.
Directional Light	Create light for the scene.
EventSystem	Sending events to objects in the application based on input.
Canvas	Create UI such as background image, logo, play and exit button and texts.
Panel	Panel is an upper-level UI container in which to arrange widgets. Layout object that controls how its widgets are arranged on the screen.
Text	Text is the text components every word in this scene
Image	This is the background image
Brute force	This is the video for brute force attack
Phishing	This is the video for phishing
SET toolkit	This is the video for SET toolkit
SQL	This is the video for SQL injection
Tailgating	This is video for Tailgating
Home	This is used to go back the main scene

Table 5.7 Main components in video scene

### 5.8 Design Game Scenario

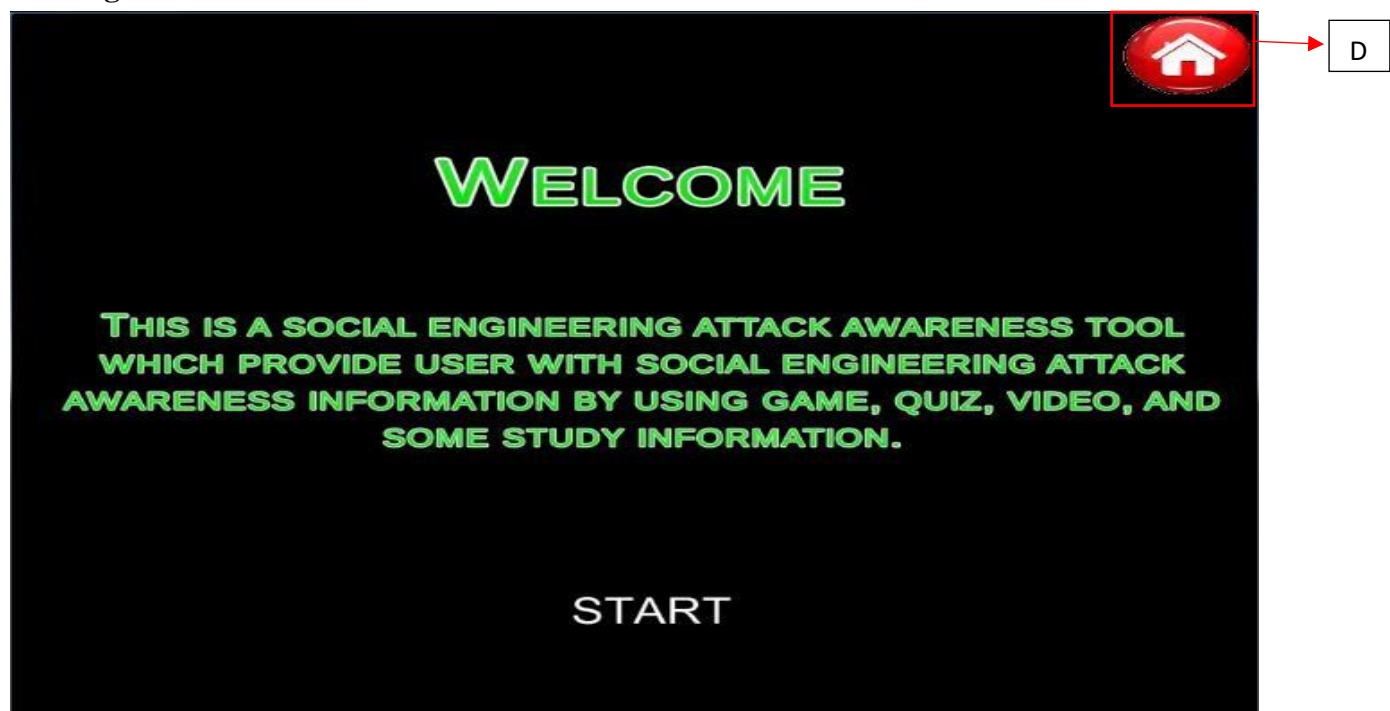


Figure 5.9 Introduction scene of awareness tool

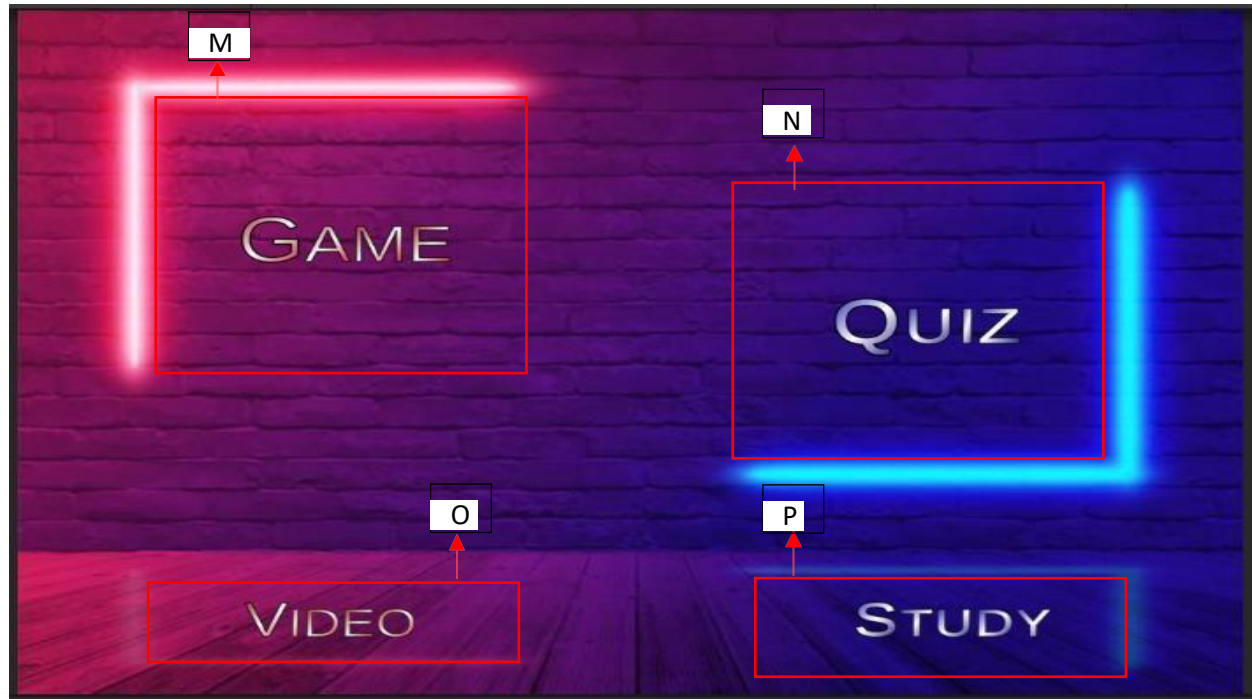


Figure 5.10 This is the menu scene of the awareness tool

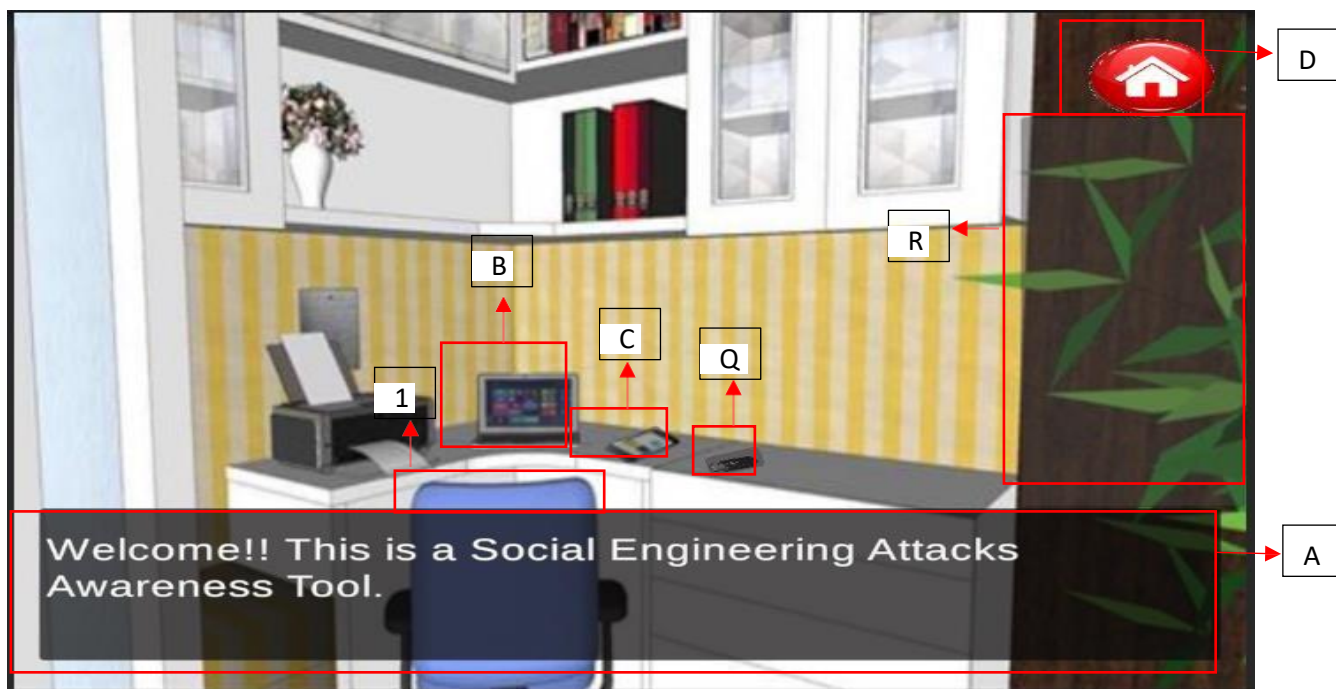


Figure 5.11 This is the game scene of the awareness tool

### 5.8.1 Scene Password Exploitation Attack

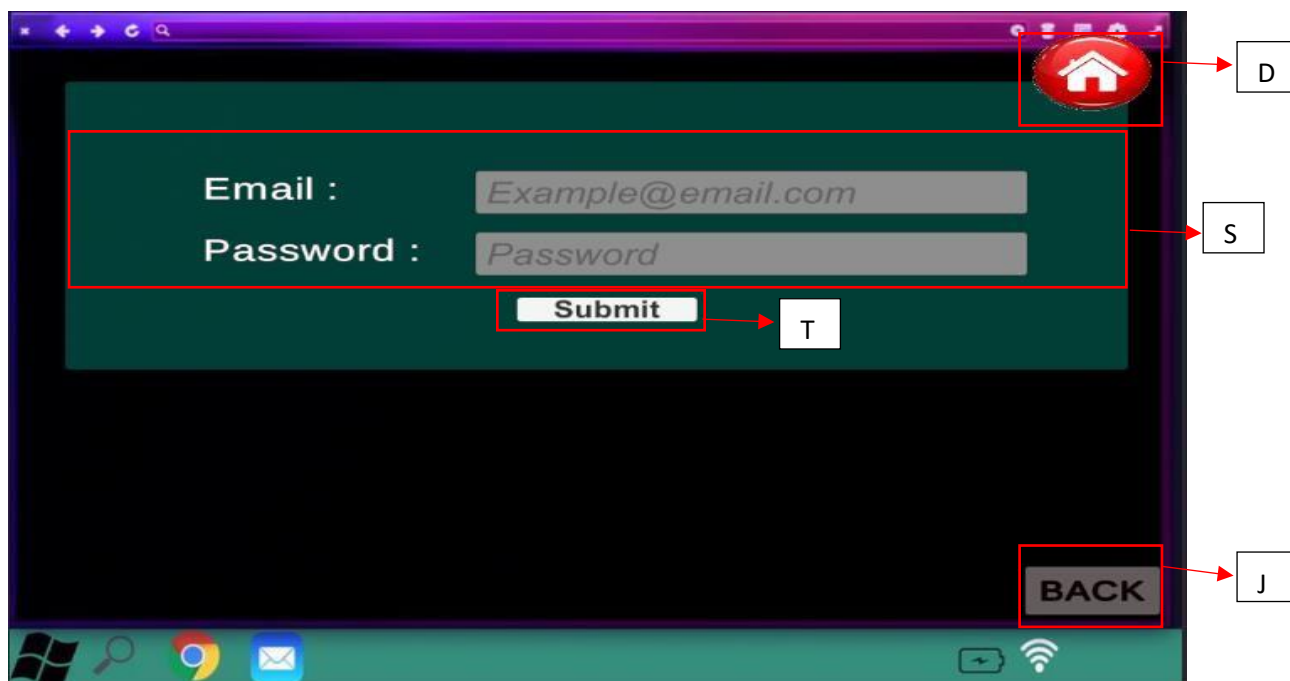


Figure 5.12 Main interface of the Phishing attack and password exploitation attack scenario.

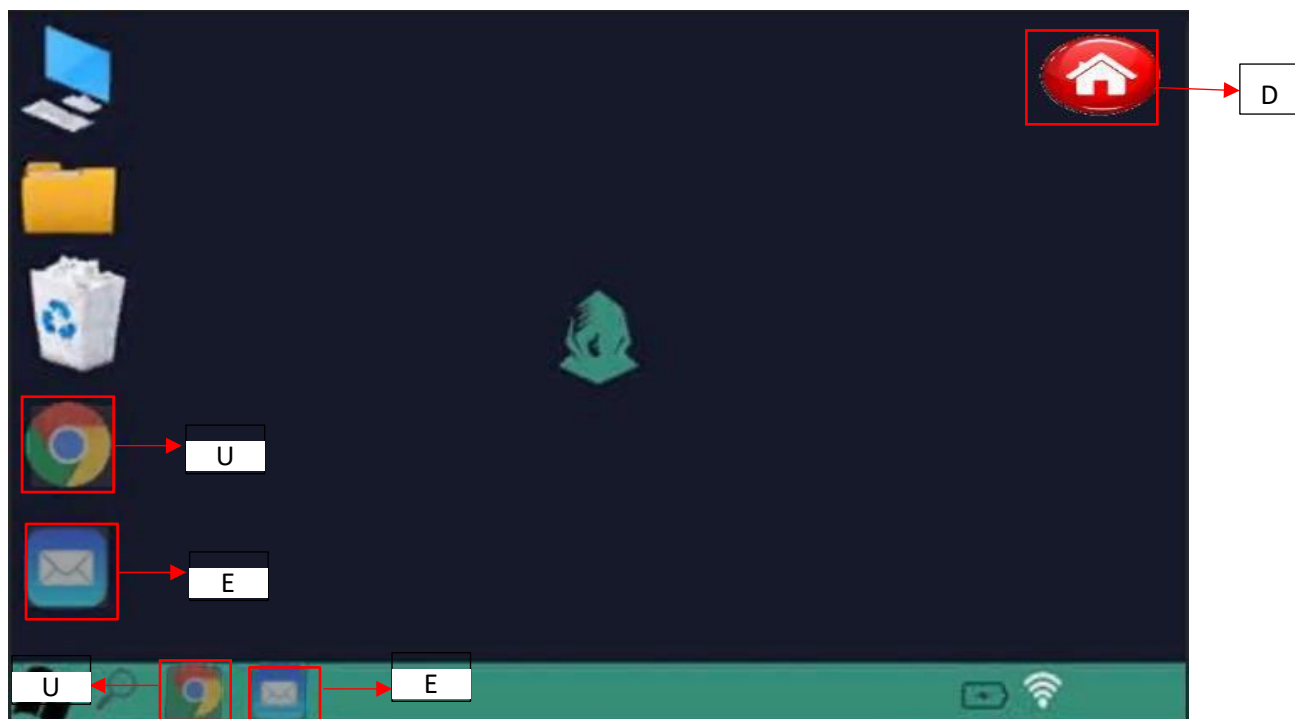


Figure 5.13 Main interface of the password exploitation attack scenario.

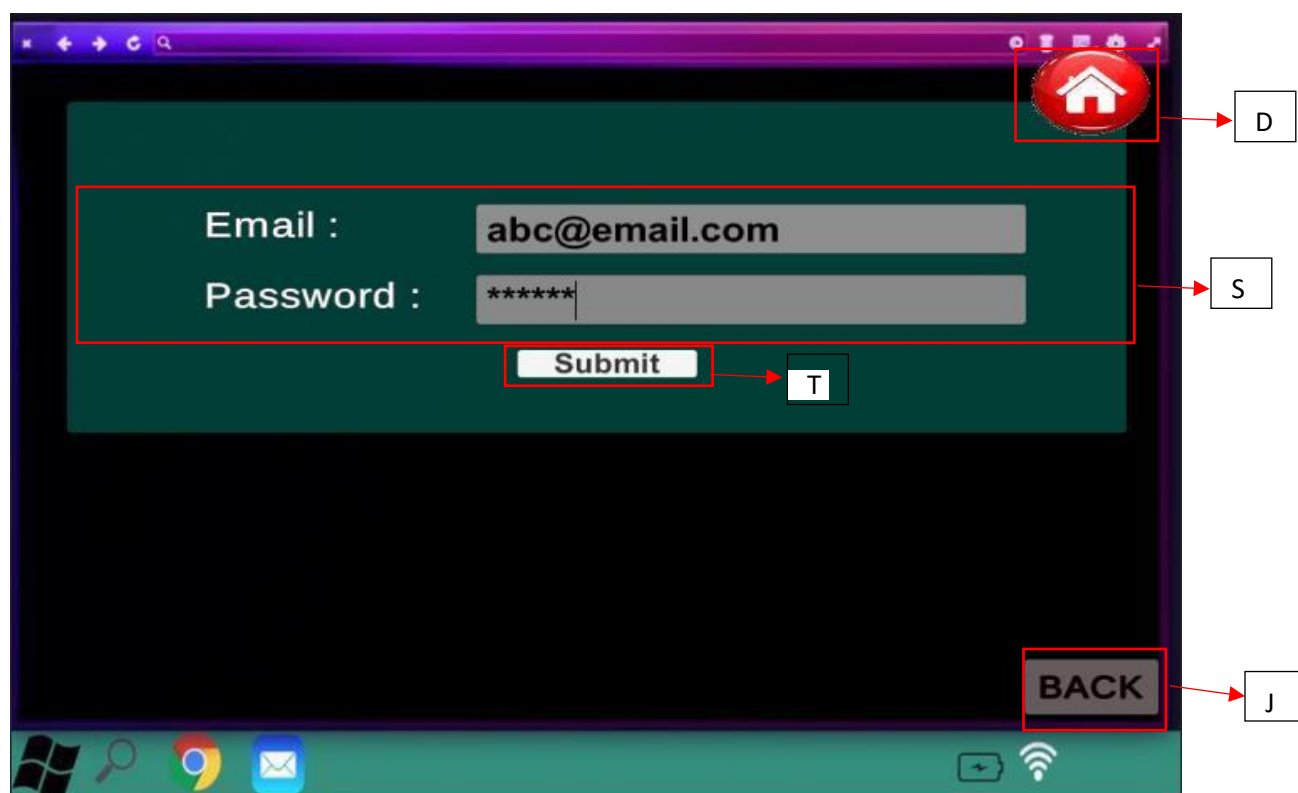


Figure 5.14 This is an example of Password exploitation attack scenario.

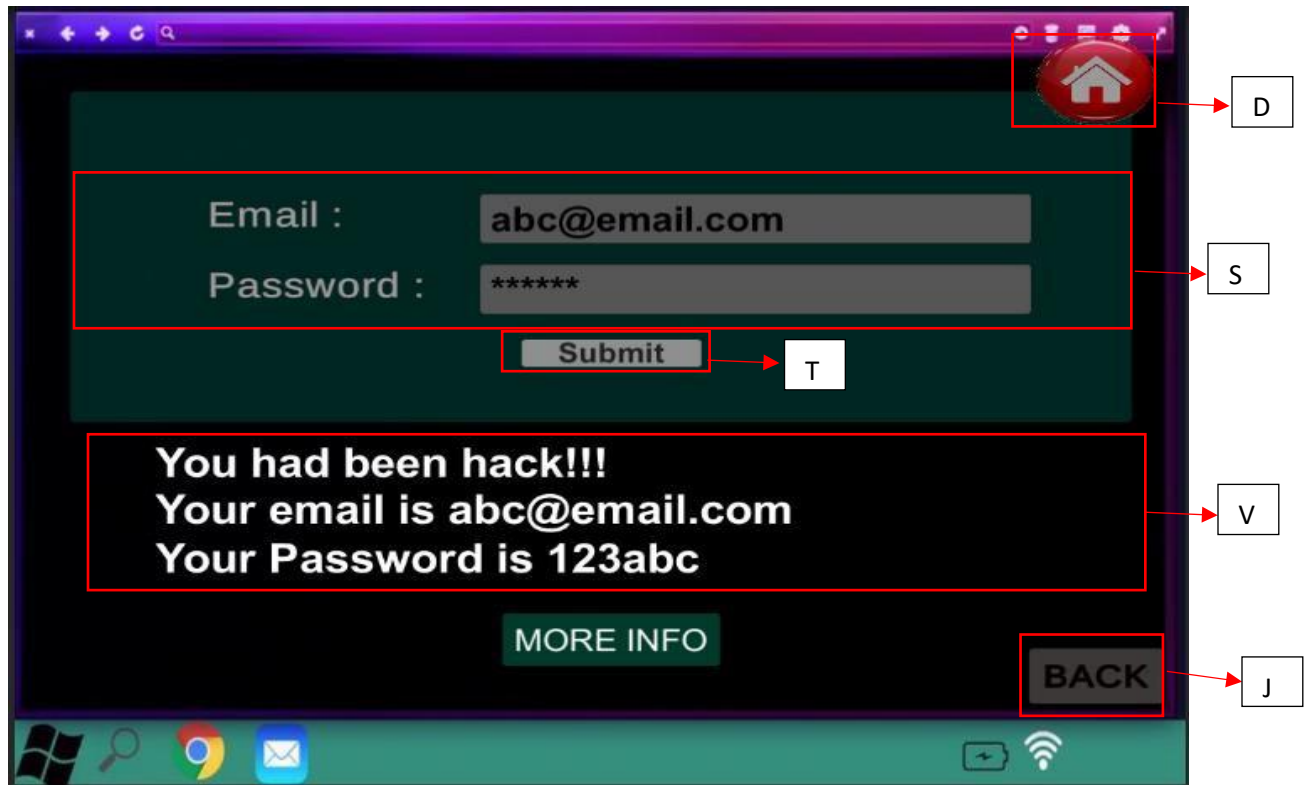


Figure 5.15 This is an example of Password exploitation attack scenario when user click submit, then will pop up a message “You had been hack!! Your email is [abc@email.com](mailto:abc@email.com) Your password is 123abc”





Figure 5.16: When user click on “more info” button, will show this information.

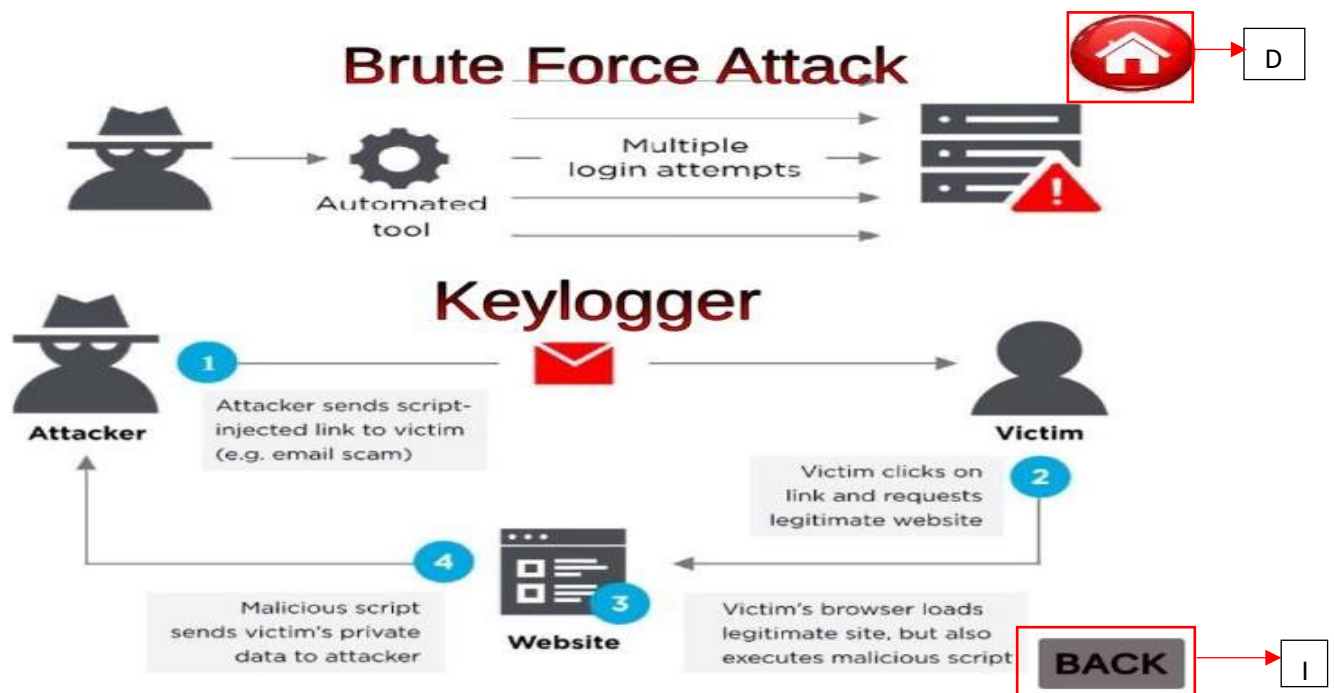


Figure 5.17 Main interface of the Phishing attack and password exploitation attack scenario.

### 5.8.2 Scene 4 Baiting Attack

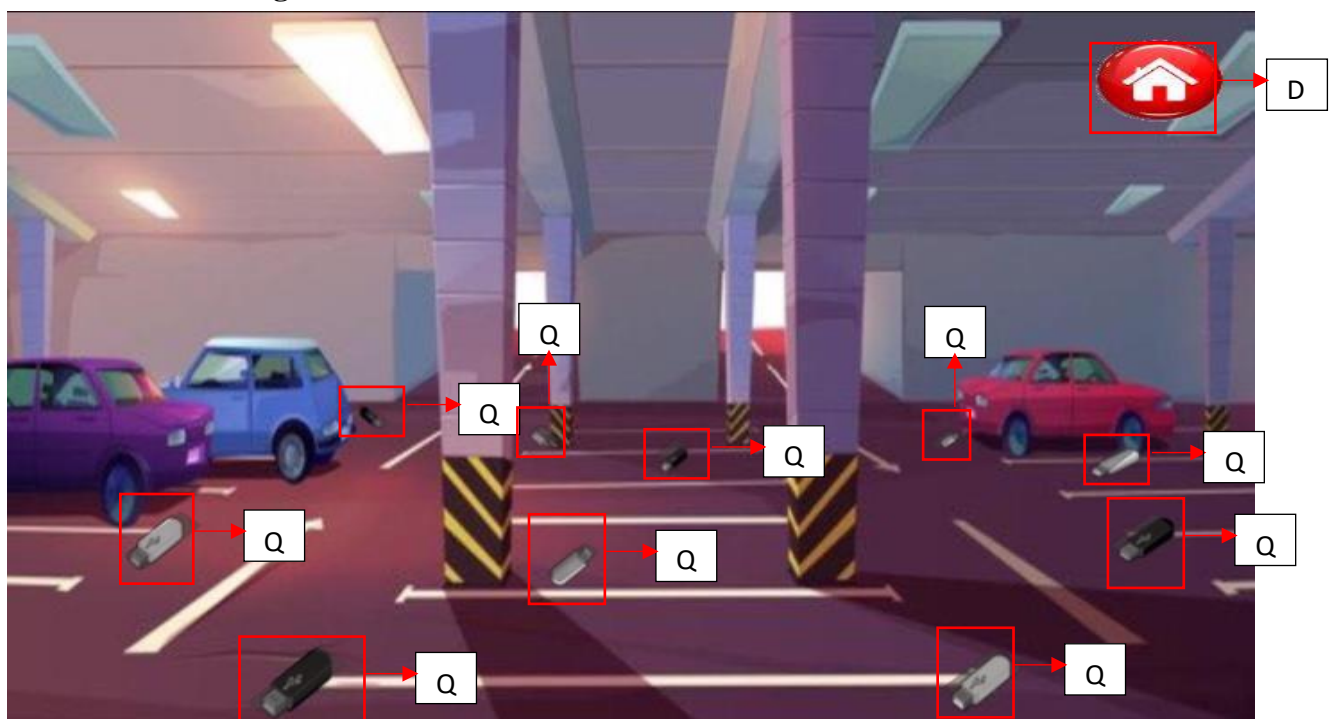


Figure 5.18 Main interface of the Baiting attack scenario.

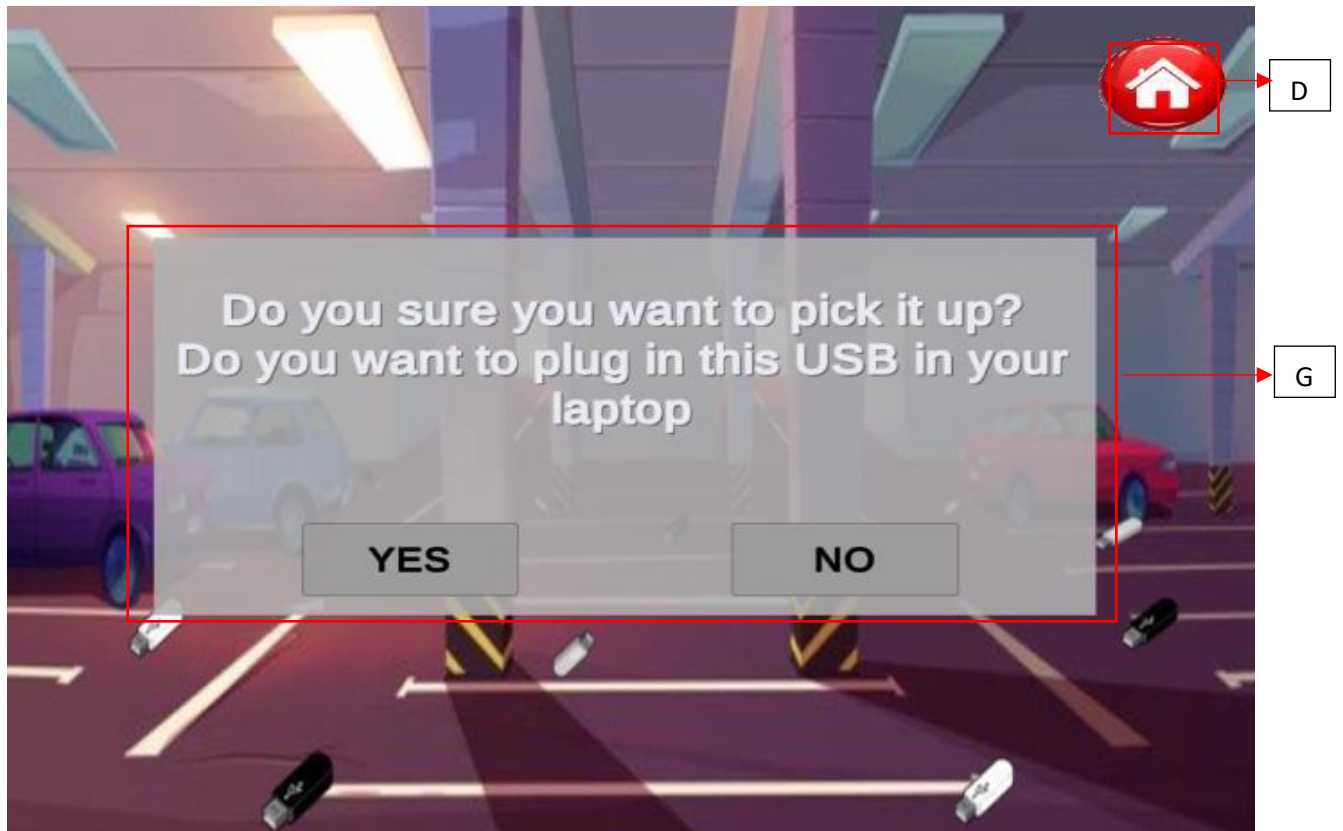


Figure 5.19 When user click at the USB will prompt user a message to select whether pick up and plug into your laptop with two option “Yes” and “No”.

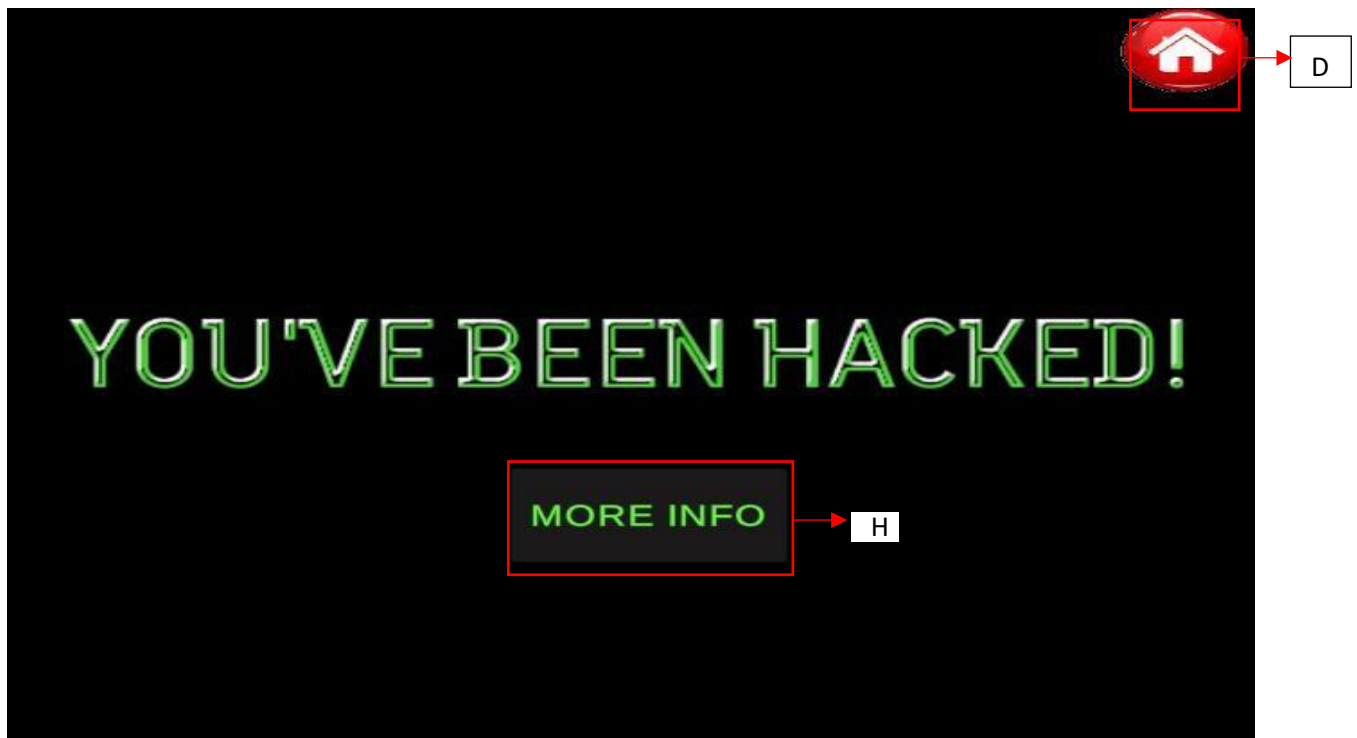


Figure 5.20: If user select “Yes”, will pop this message to user, user can click on the “more info” button to understand which attack and relevant information.

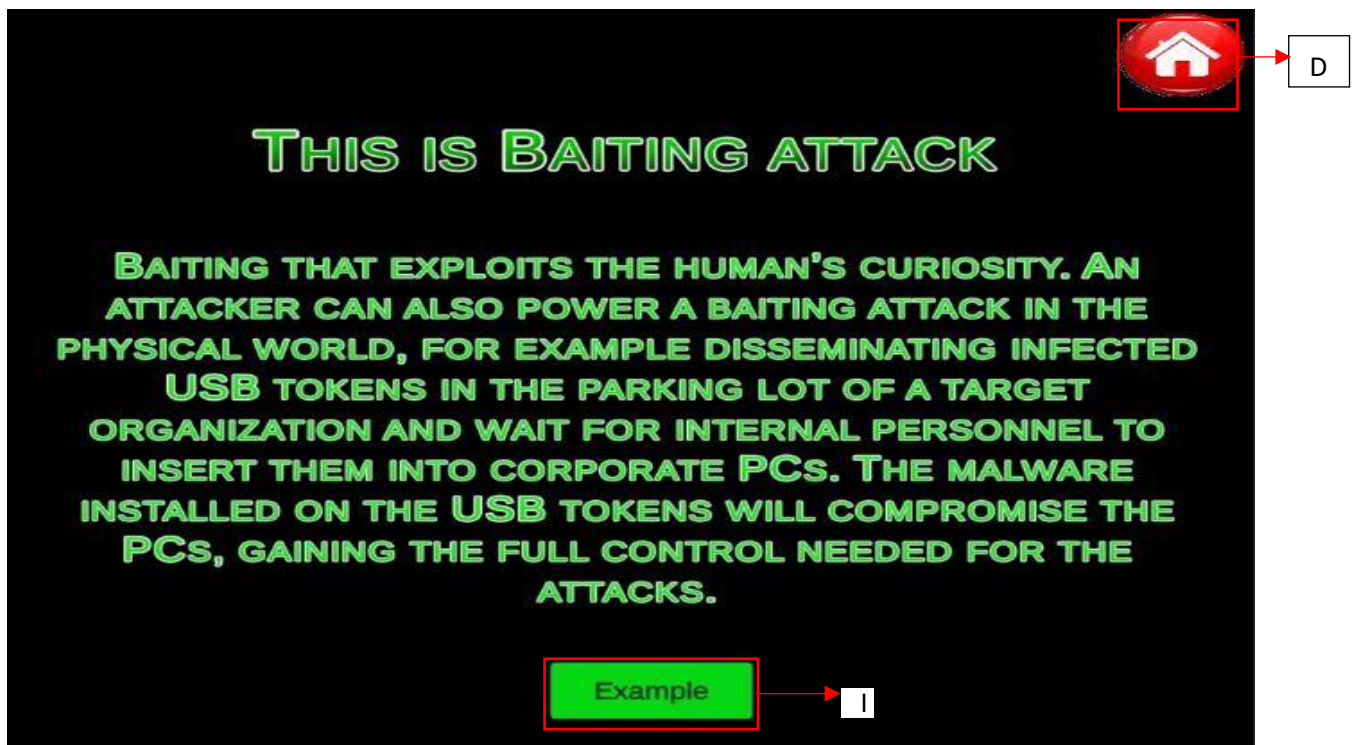


Figure 5.21: When user click on “more info” button, will show this information.



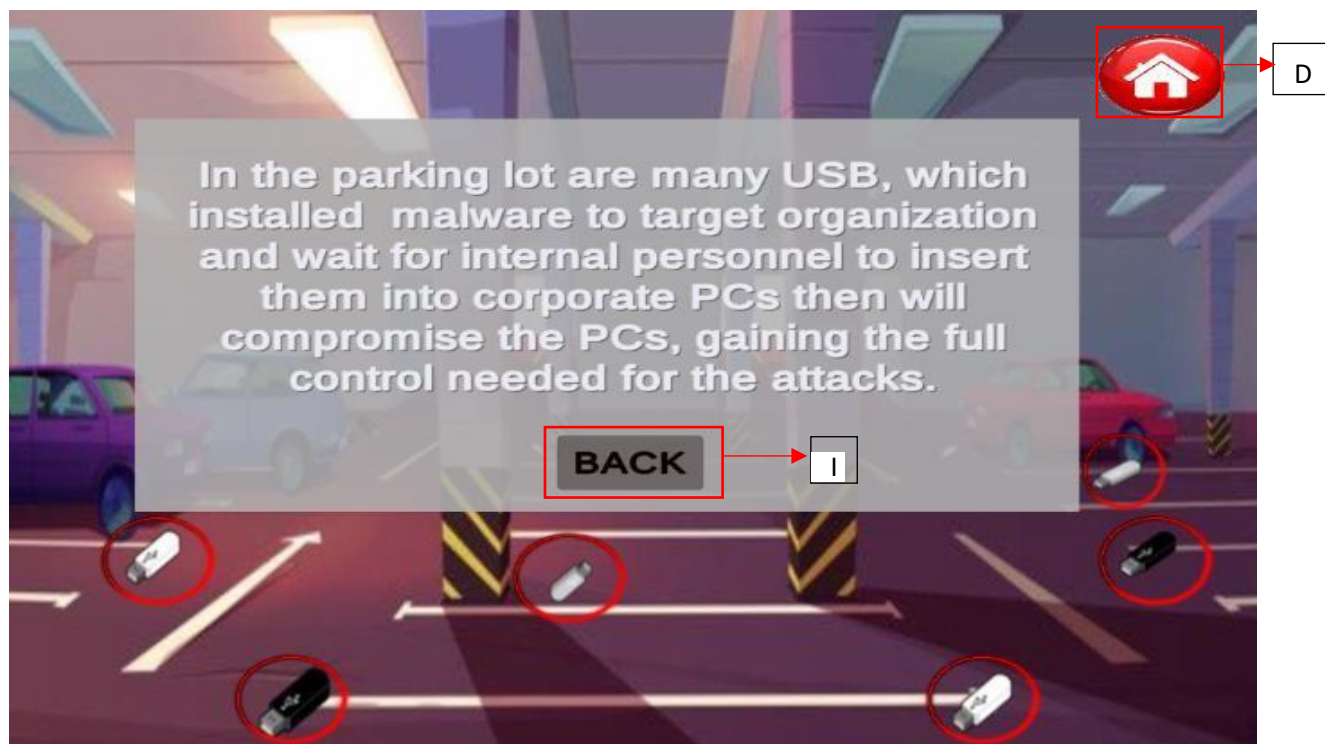


Figure 5.22: When user click on “example” button, will some the previous parking slot and highlighted information for user to aware some details can distinguish the baiting attack.



Figure 5.23: If user select “No”, will pop congrats message to user, user can click on the “more info” button to understand which attack and relevant information or click the back button to continue the game.

### **5.8.3 Scene 5 Tailgating Attack**

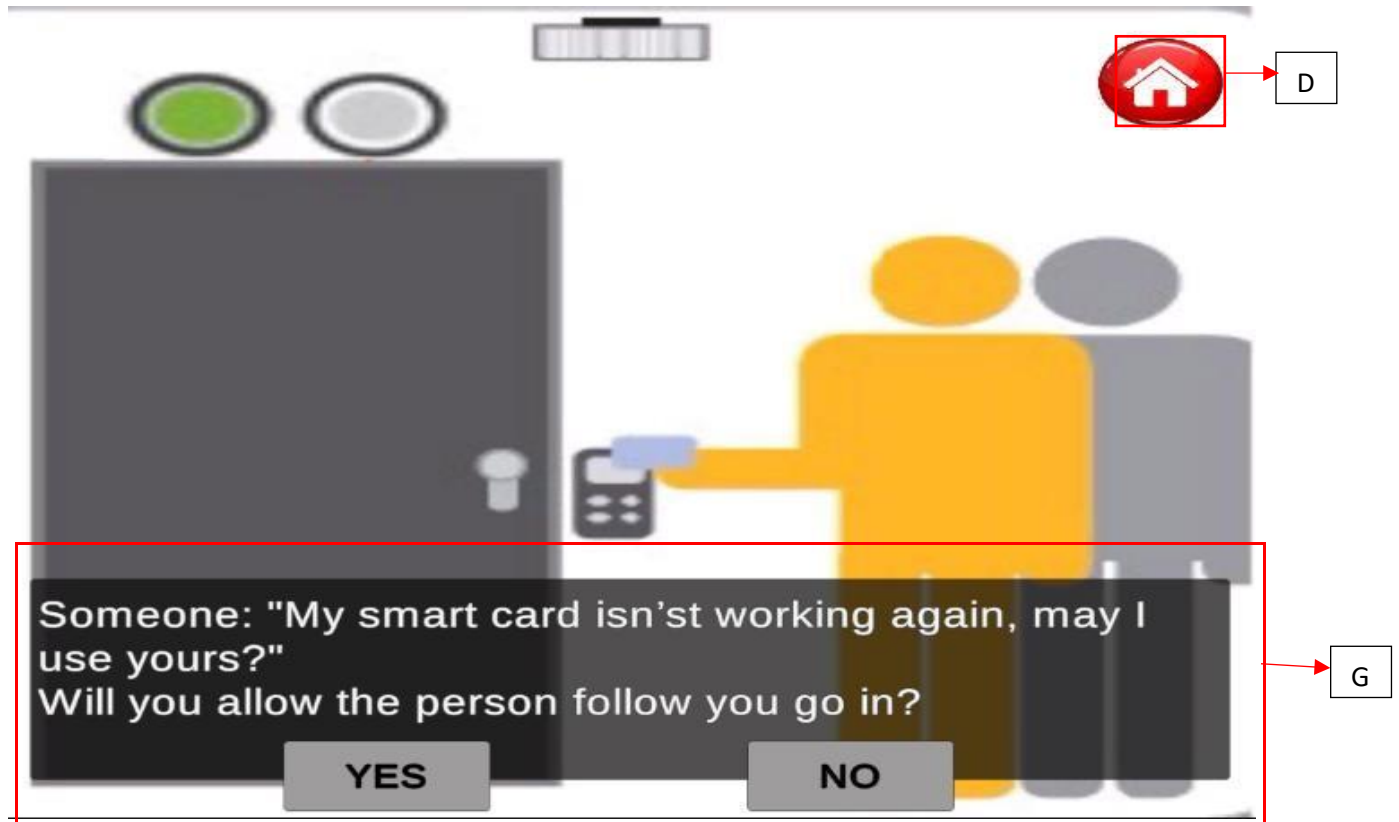


Figure 5.24 Main interface of the Tailgating attack scenario. System will prompt user a message to select whether allow the person follow you go in “Yes” and “No”.



Figure 5.25: If user select “Yes”, will pop this message to user, user can click on the “more info” button to understand which attack and relevant information

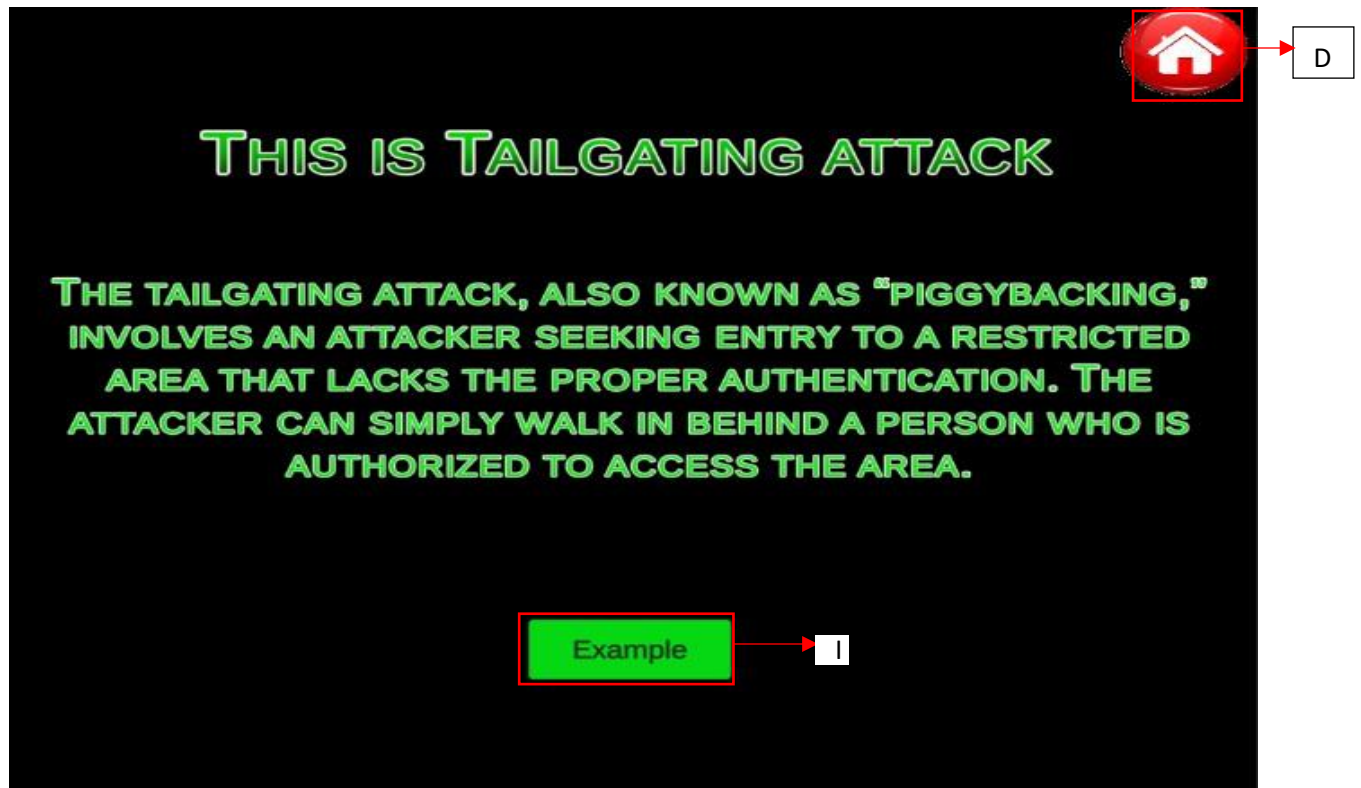


Figure 5.26: When user click on “more” button, will show this information

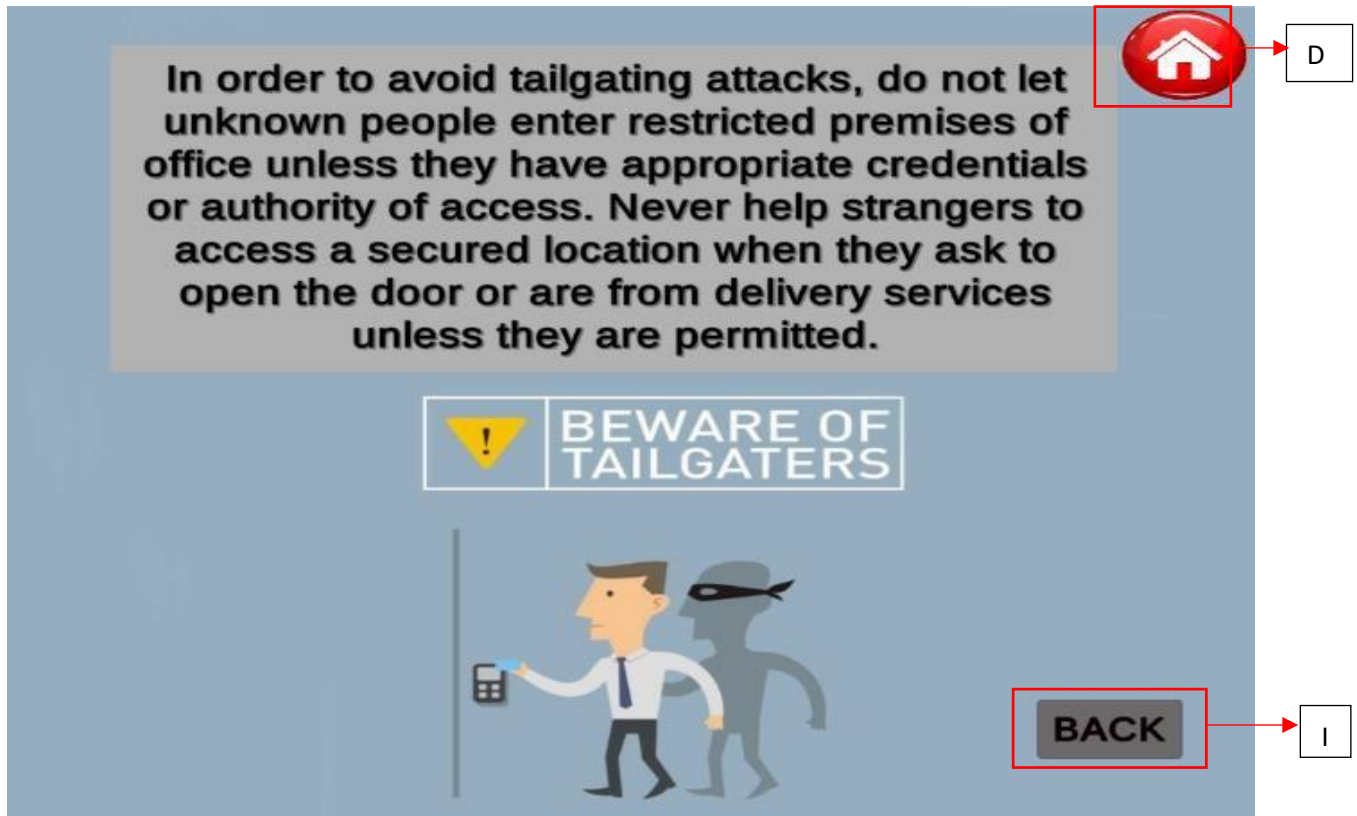


Figure 5.27: When user click on “example” button, will provide some highlighted information for user to aware some details can distinguish the tailgating attack





Figure 5.28: If user select “No”, will pop congrats message to user, user can click on the “more info” button to understand which attack and relevant information or click the back button to continue the game.

#### 5.8.4 Scene 6 Shoulder Surfing Attack



Figure 5.29 Main interface of the Shoulder Surfing attack scenario. System will prompt user a message to select whether enter your password when a person standing behind “Yes” and “No”.

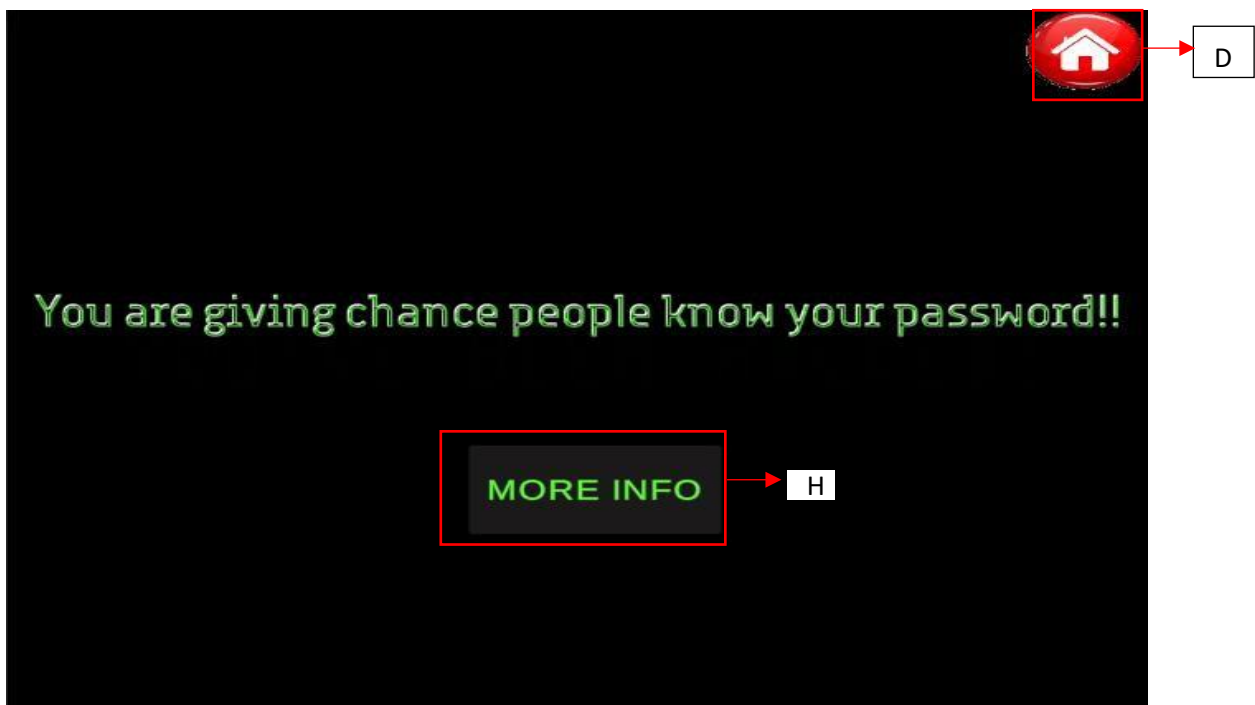


Figure 5.30: If user select “Yes”, will pop this message to user, user can click on the “more info” button to understand which attack and relevant information

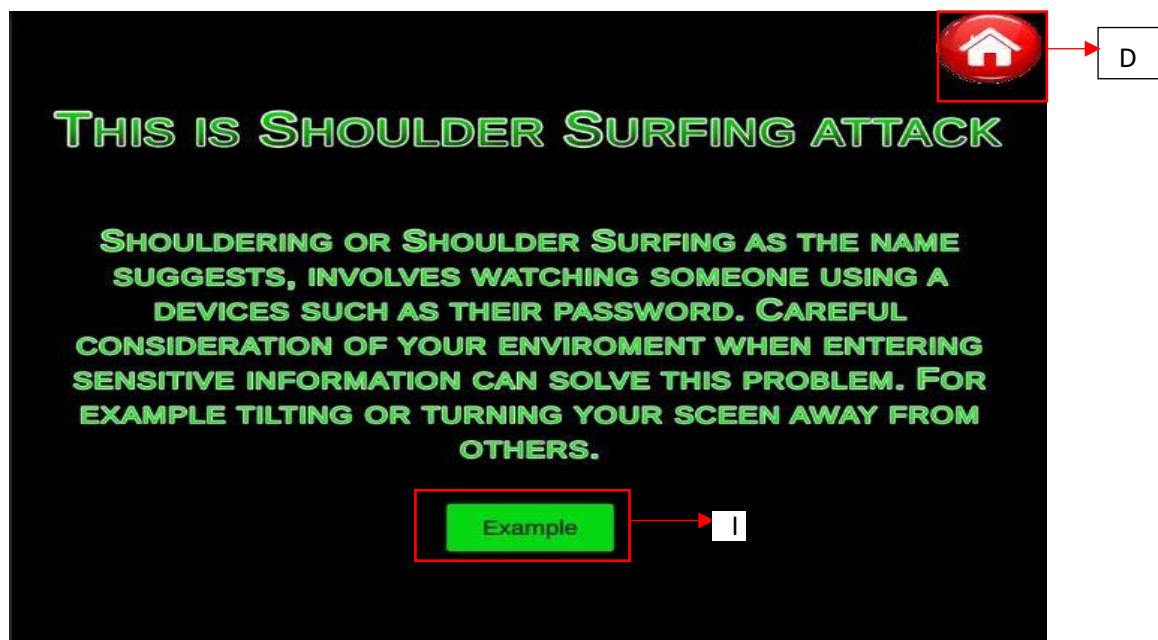


Figure5.31: When user click on “more” button, will show this information



Figure 5.32: When user click on “example” button, will provide some highlighted information for user to aware some details can distinguish the shoulder surfing attack

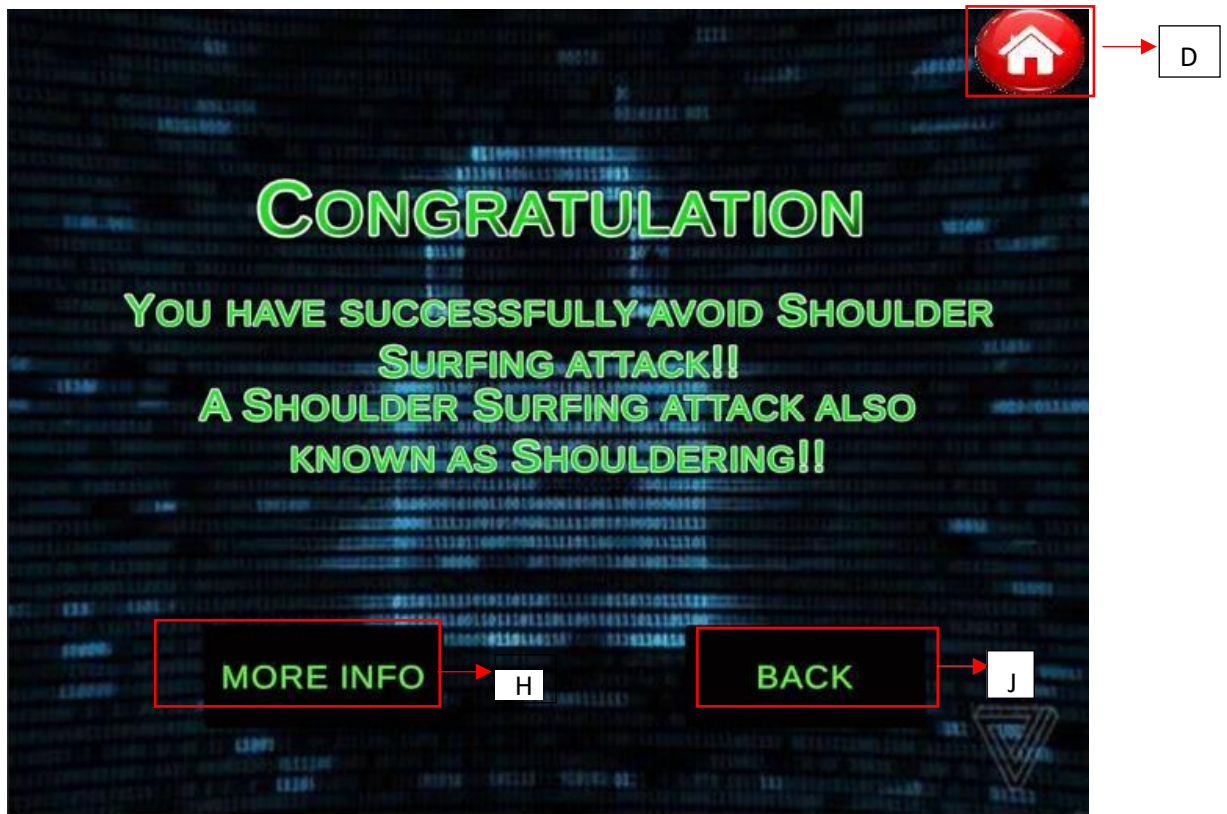


Figure 5.33: If user select “No”, will pop congrats message to user, user can click on the “more info” button to understand which attack and relevant information or click the back button to continue the game.



### 5.8.5 Scene 7 Quiz

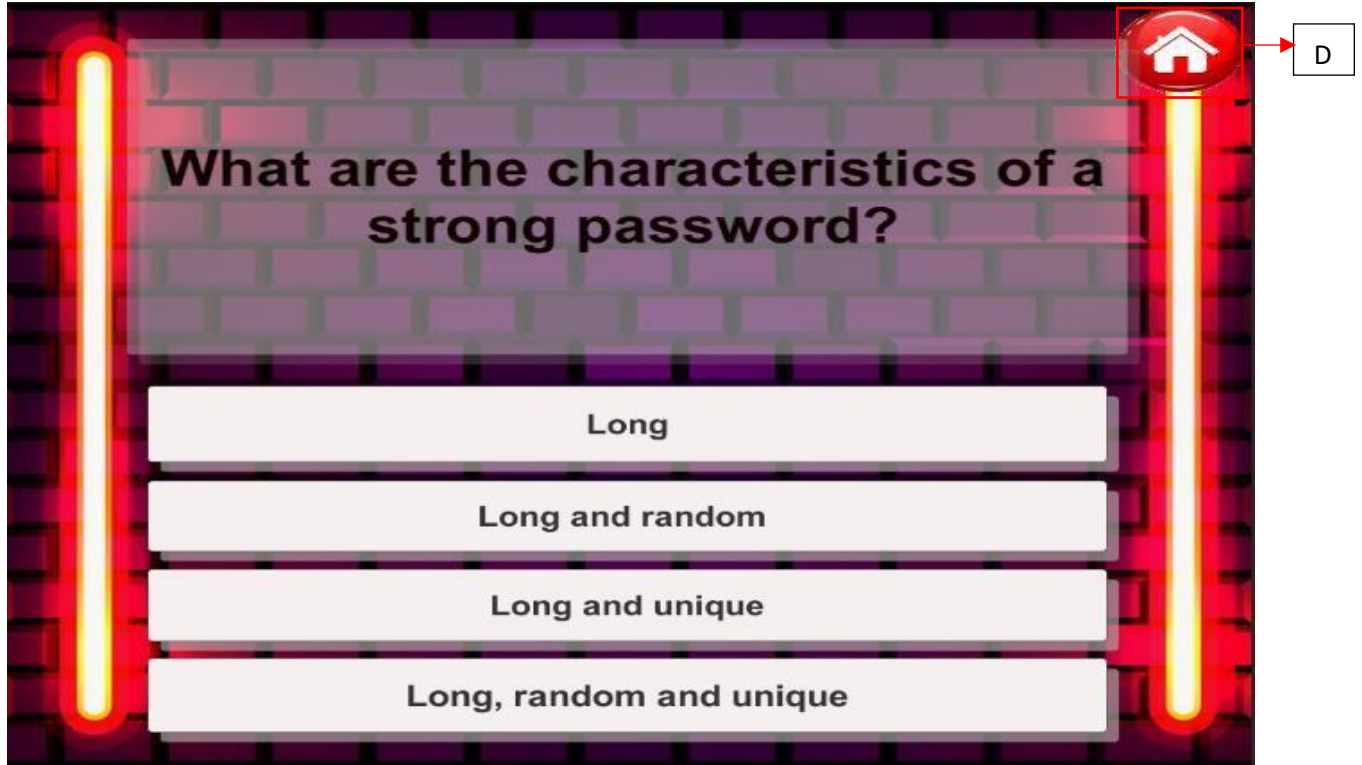


Figure 5.34: This is the first quiz question of the awareness tool.

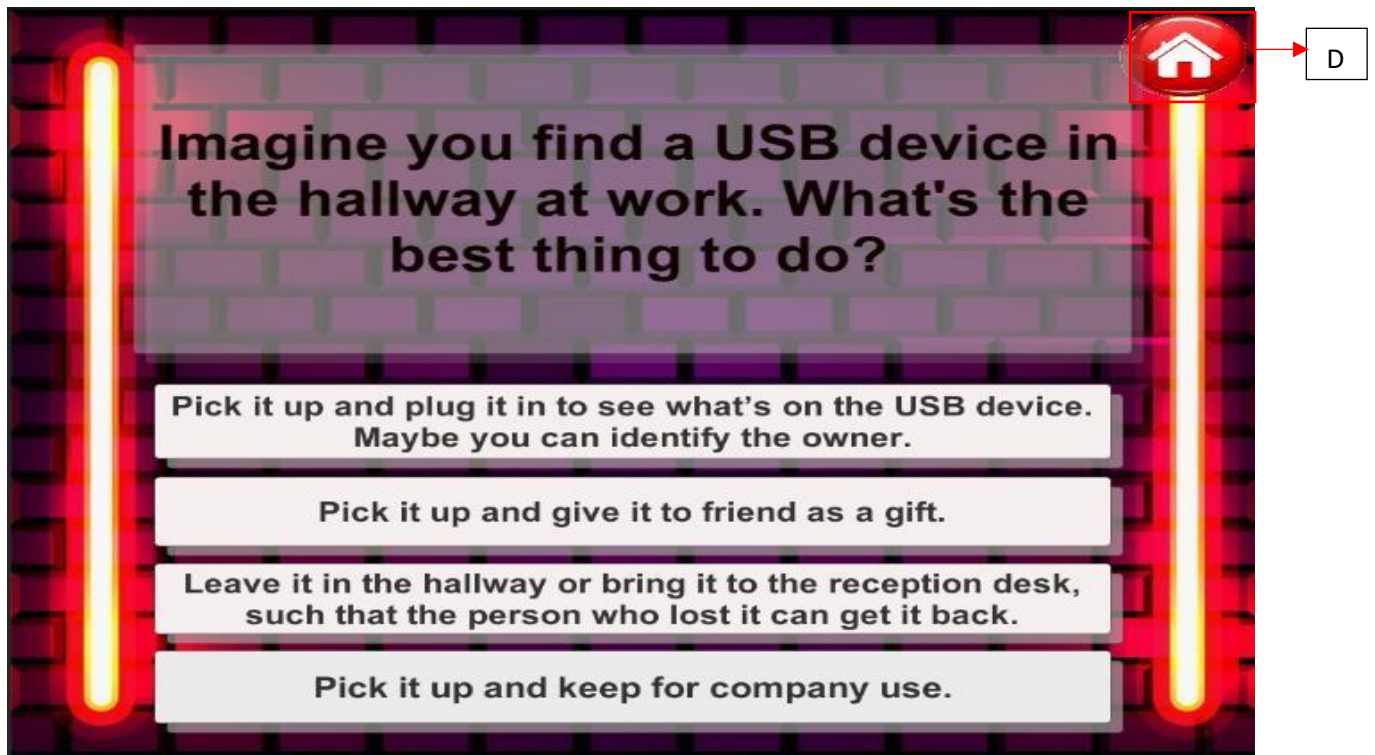


Figure 5.35: When user answer the first question then will pop the second quiz question of the awareness tool.



Figure 5.36: When user answer the second question then will pop the third quiz question of the awareness tool.

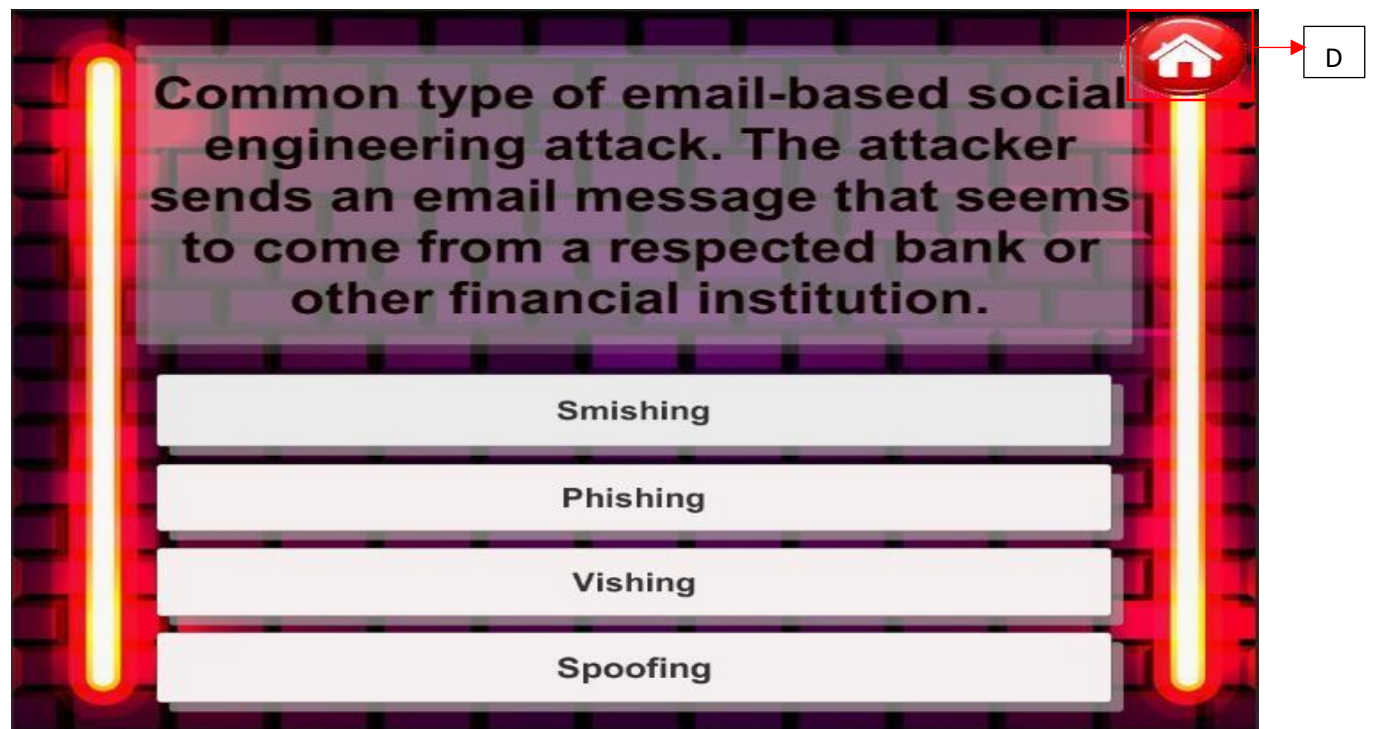




Figure 5.37: When user answer the third question then will pop the fourth quiz question of the awareness tool

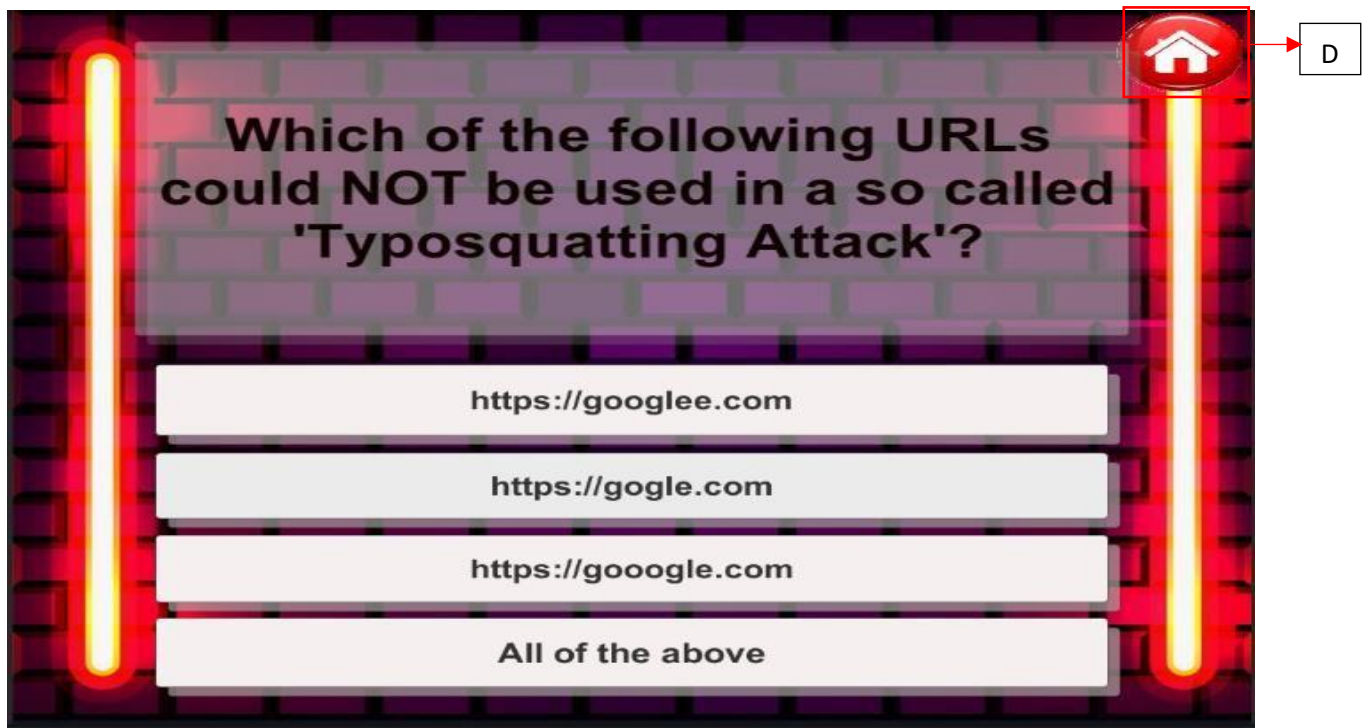


Figure 5.38: When user answer the fourth question then will pop the fifth quiz question of the awareness tool



Figure 5.39: When user answer the fifth question then will pop the sixth quiz question of the awareness tool



Figure 5.40: When user answer the sixth question then will pop the seventh quiz question of the awareness tool

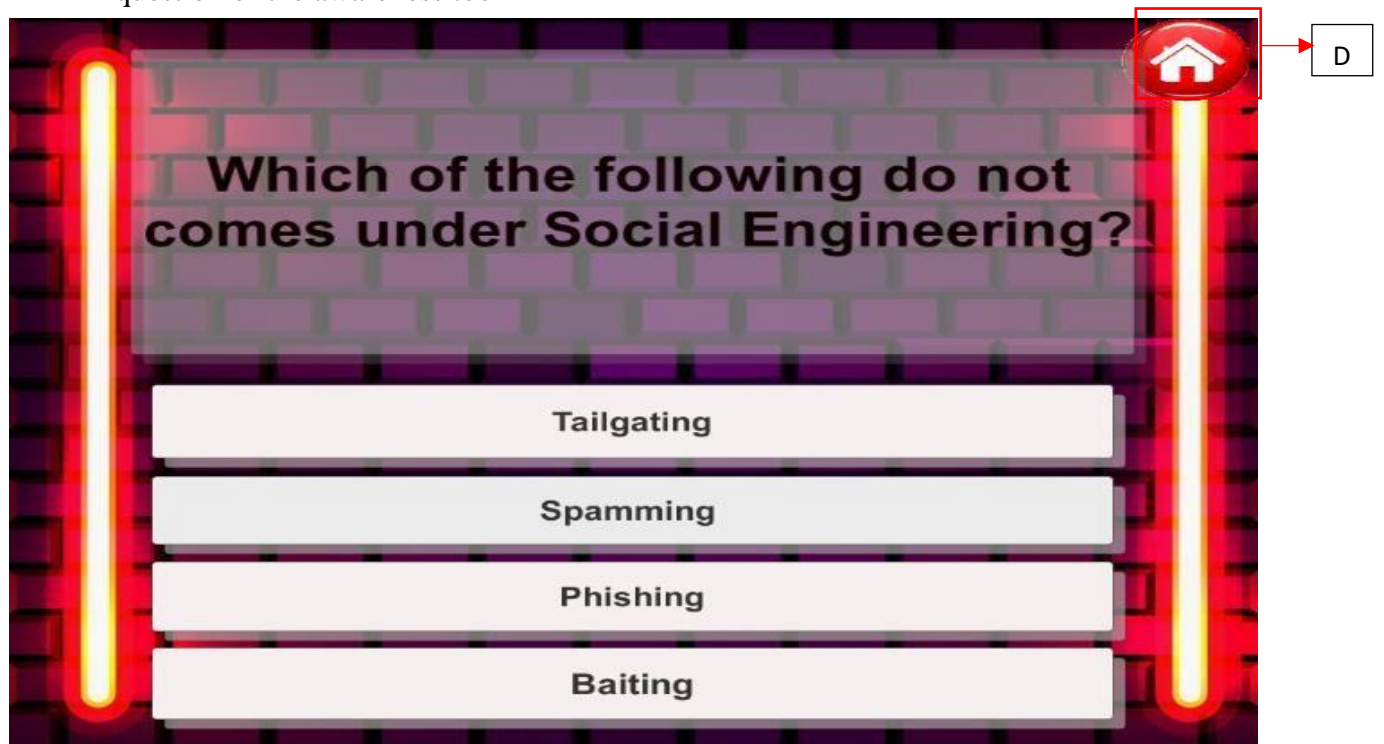




Figure 5.41: When user answer the seventh question then will pop the eighth quiz question of the awareness tool

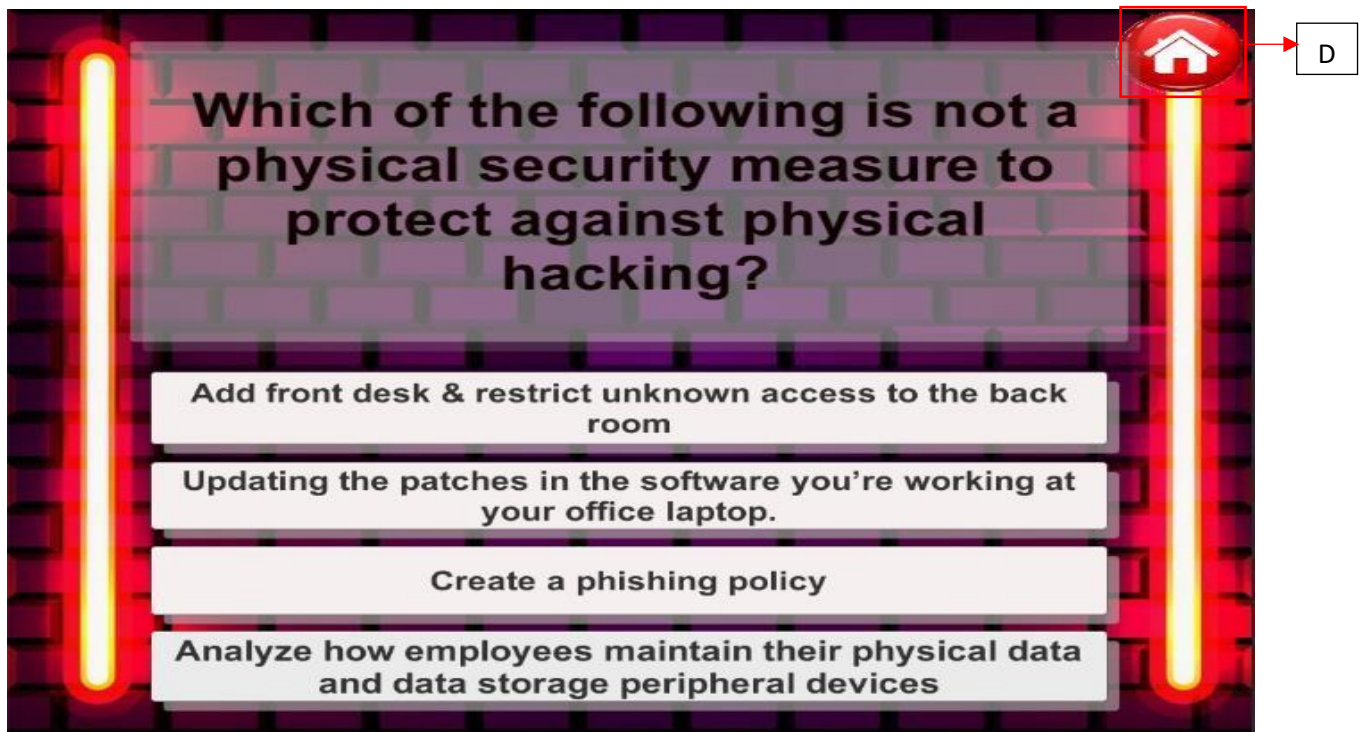


Figure 5.42: When user answer the eighth question then will pop the ninth quiz question of the awareness tool



Figure 5.43: When user answer the ninth question then will pop the last quiz question of the awareness tool

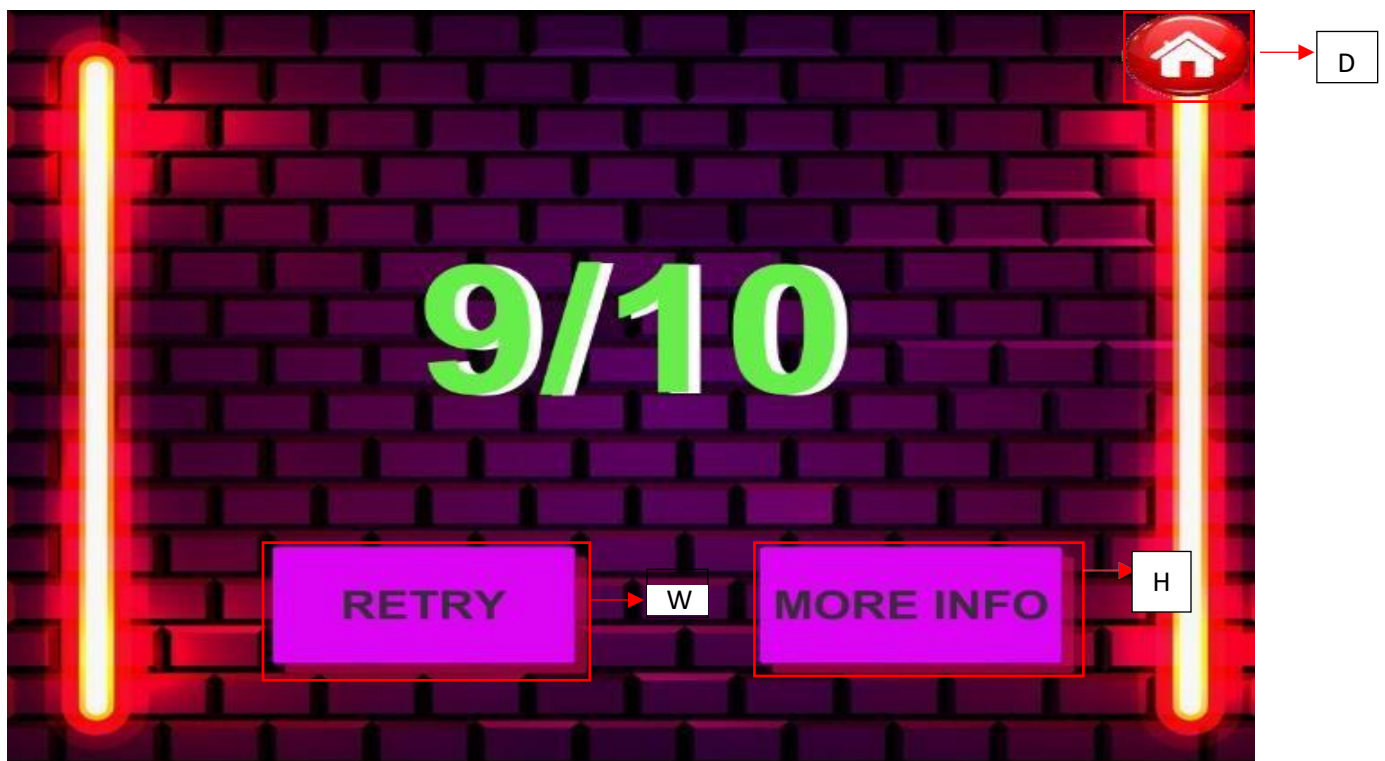


Figure 5.44: After user answer all the social engineering attack quiz will pop the score of the user.

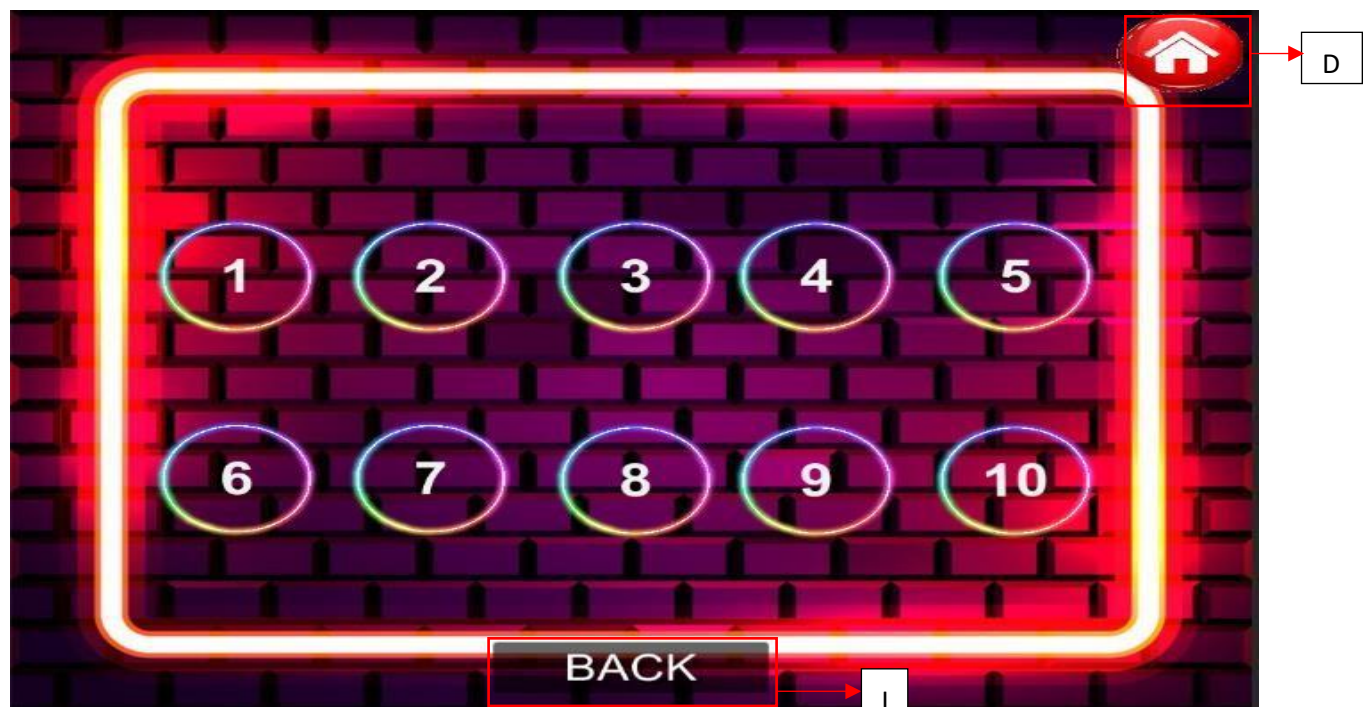


Figure 5.45 When user click “more info” will direct user to the study scene with ten study scene.

### **5.8.6 Scene 8 Video**

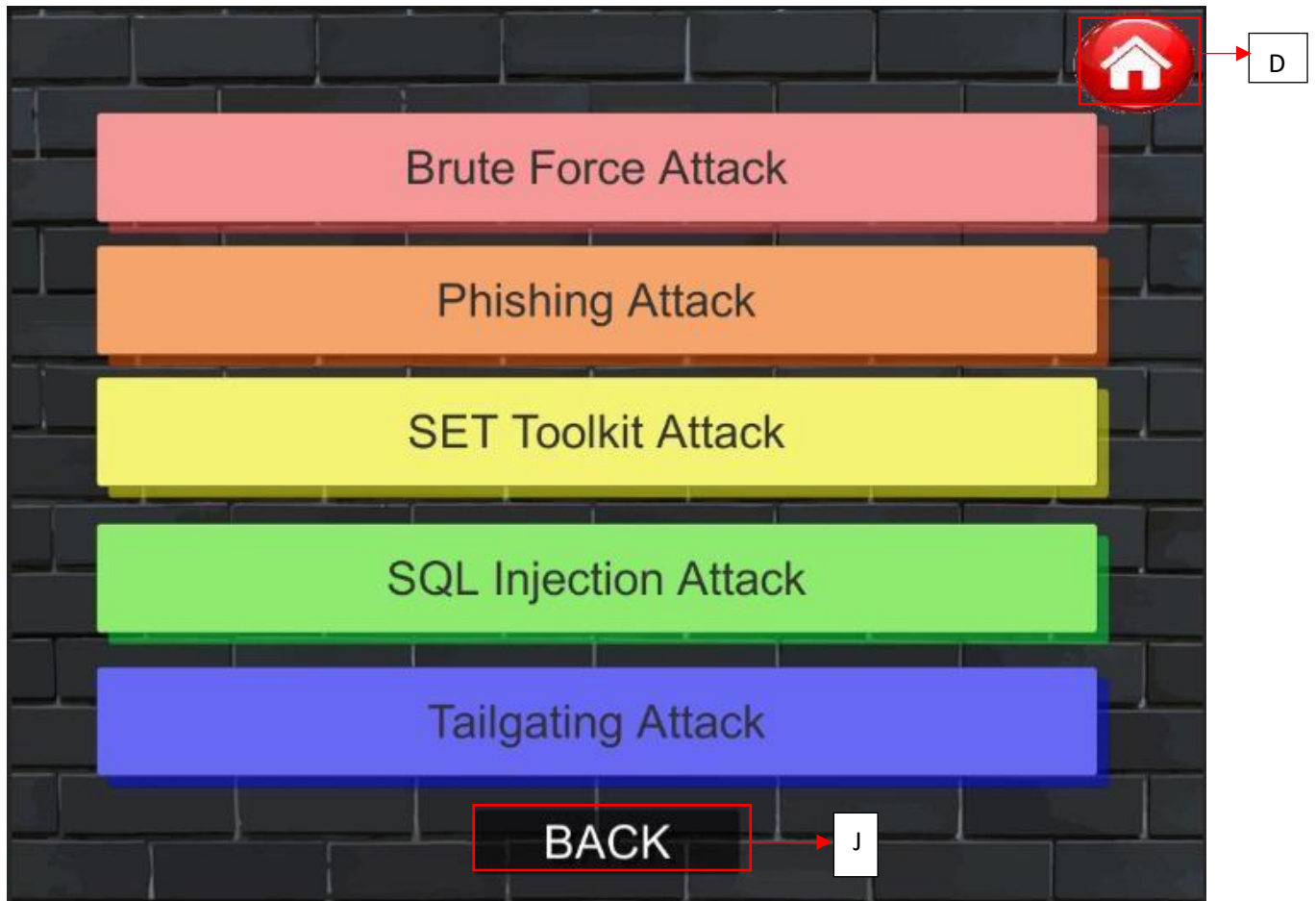


Figure 5.46 This is the video menu scene of the awareness tool





Figure 5.47 This is the brute force attack video scene.



Figure 5.48 This is the phishing attack video scene

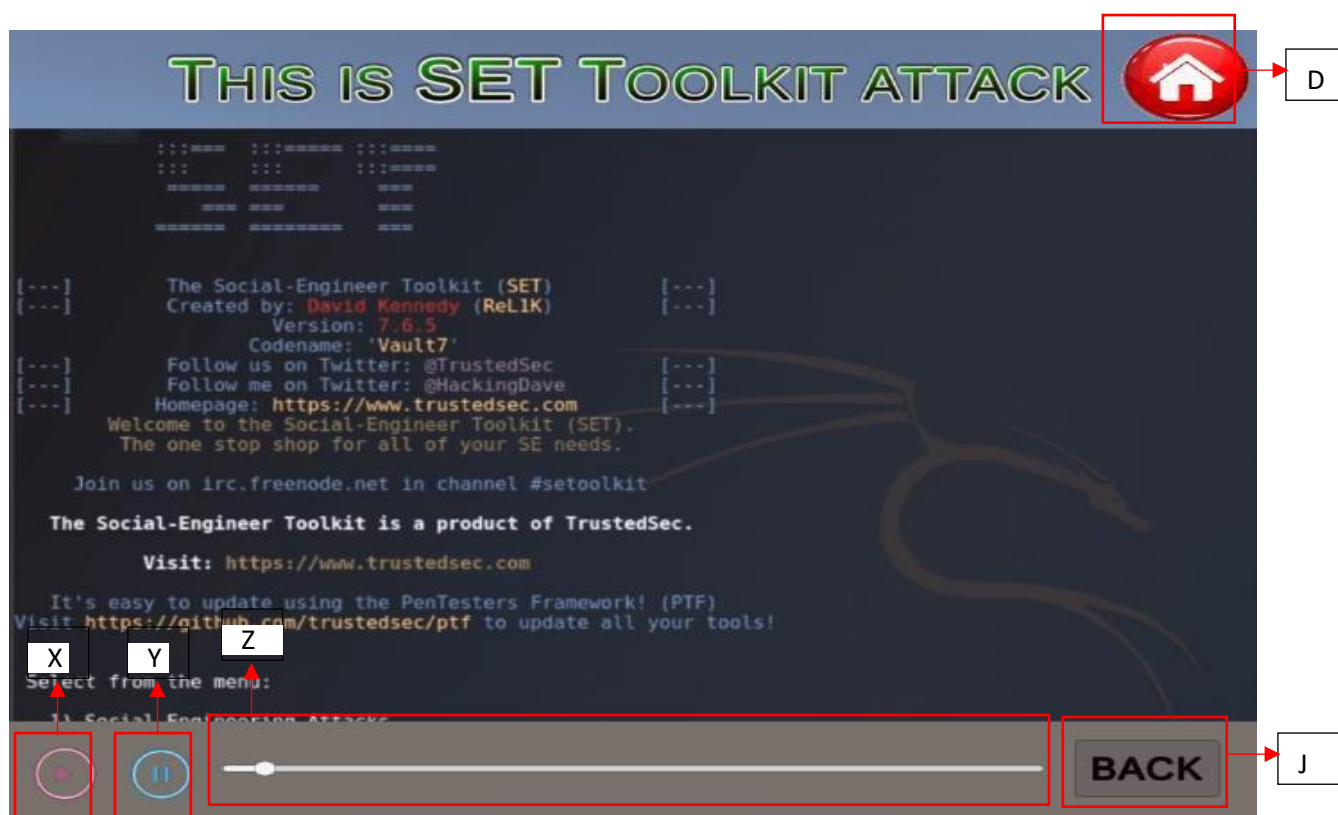


Figure 5.49 This is the SET toolkit attack video scene

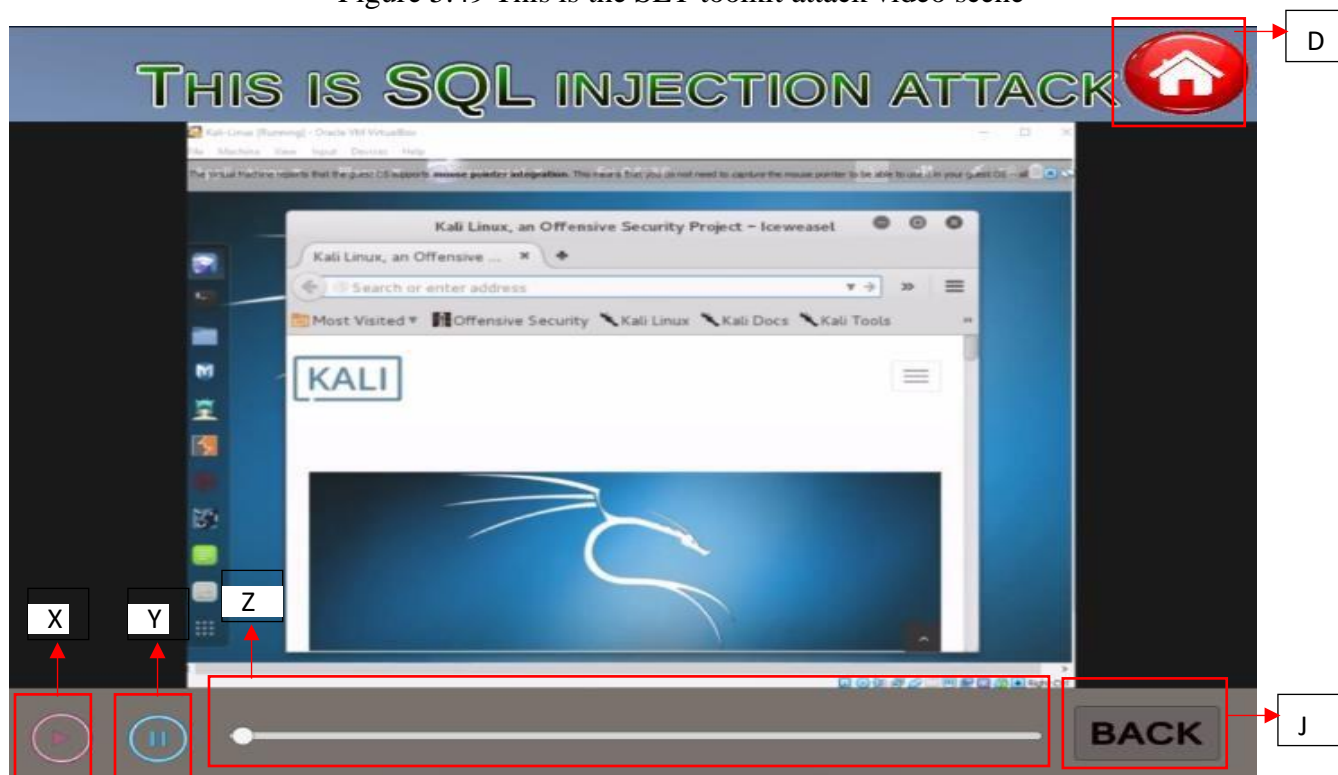


Figure 5.50 This is the SQL Injection attack video scene

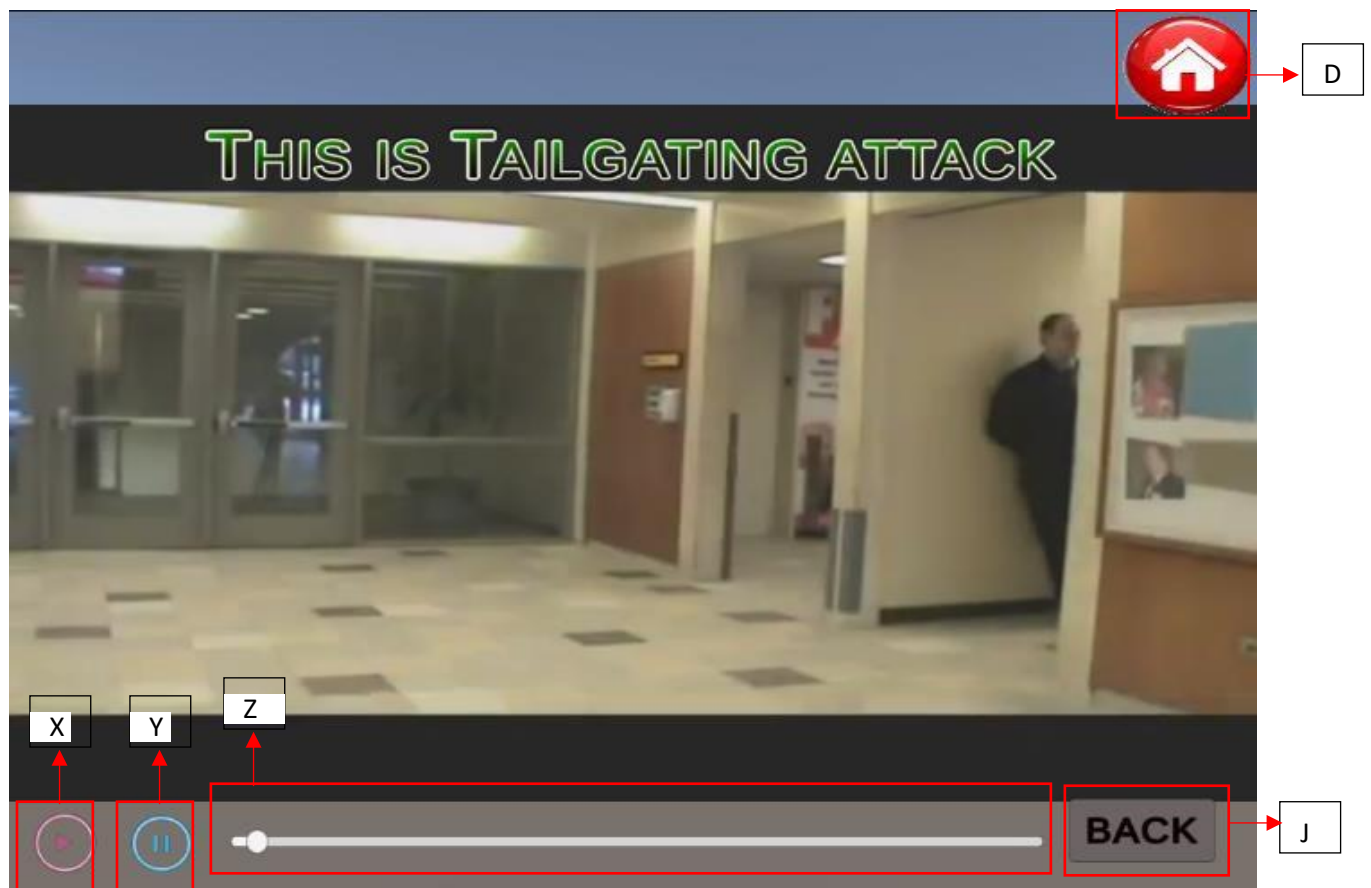


Figure 5.51 This is the Tailgating attack video scene

Label	Name	Function
A	Dialog box	Brief introduction when clicked this dialog box.
B	Laptop	Phishing attack scene when clicked this button.
C	Phone	Smishing attack scene when clicked this button.
D	Home button	Back to Game scene when clicked this button.
E	Mail icon	Phishing email scene when clicked this link.
F	Malicious link	Phishing attack contain in this link when clicked this link.
G	Selection box	Different selection will have different result.
H	More info button	Relevant information and type of attack when clicked this button.
I	Example button	Relevant example with highlighted information when clicked this button.
J	Back button	Back to Game scene when clicked this button.
K	Message icon	Smishing scene when clicked this link.
L	Malicious number	Smishing attack contain in this link when clicked this link.
M	Game button	When click this button will direct user to game scene

## CHAPTER 5 SYSTEM IMPLEMENTATION

N	Quiz button	When click this button will direct user to quiz scene
O	Video button	When click this button will direct user to video scene
P	Study button	When click this button will direct user to study scene
Q	USB	Baiting attack scene when clicked this button.
R	Door	Tailgating attack scene when clicked this button.
S	Login	Require user fill in email and password
T	Submit button	After filling in the email and password submit it
U	Chrome Button	Password Exploitation attack scene when clicked this button.
V	Hacked message	When submit the email and password will pop a “You had been hacked” message
W	Retry Button	When user click this button will allow user to retry the quiz again
X	Play video button	This is the button to play the video
Y	Pause video button	This is the button to pause the video
Z	Slider for video	This is the slider to slide to the desire part of video



1	Chair	Shoulder surfing attack scene when clicked this button.
---	-------	---

Table 5.8 Function of Game Scenario Scene features

### **5.8.7 Discussion**

#### **Scene 1 Phishing Attack Module**

First of all, for the Phishing Attack game when user click on the desktop in the game it will direct user to the desktop screen which have some icon on the monitor screen. Then user click on the mail icon, then will have some email inside the mailbox. It will pop a message ask user whether want to click the link in the email. User can choose either “Yes” or “No”, if “Yes” then will pop a message to tell user that had been attacked and provide some related information about phishing attack to aware user, if choose “No” then will pop a message to congrats user have been successfully avoid a phishing attack and with some related information.

#### **Scene 2 Smishing Attack Module**

Besides, for the Smishing Attack game when user clicks the smart phone then will direct user to the home screen of the smart phone. Then user click the message icon will have few SMS in the inbox, one of the SMS is about user PayPal account has been suspended due to suspicious activity and request user to contact immediately, then will pop a message which request user select “Yes” or “No” whether call the number if user select “Yes” mean the user had been attacked. Therefore, scammers can easily get their login information and login to their account, else they are successfully avoiding a vishing attack and with some related information.

### Scene 3 Password Exploitation Attack Module

Password exploitation attack is just simply trying to steal your password by hackers. Due to there will be some poorly design password by user which is not strong enough to secure your account. In this module, it is responsible of the password exploitation attack happened in when the user fills in their email and password. Then the system will pop a message tell the user “You have been hacked! Your email is XXX (user email). Your password is XXX (the user password). Then user can click for “more info” to get more information about password exploitation attack and have awareness about it.

### Scene 4 Baiting Attack Module

Baiting attack, also known as road apples, it invites users to click on a link to get free stuff. Based human curiosity, attackers can also focus on exploiting via the use of physical media. When user click on any USB on the floor will pop a message to ask user whether pick it up and plug it to the laptop. If user choose “Yes” then will pop a message to tell user that had been attacked and provide some related information about baiting attack to aware user, if choose “No” then will pop a message to congrats user have been successfully avoid a baiting attack and with some related information. Thus, user will know how their password been hacked with different ways.

### Scene 5 Tailgating Attack Module

Tailgating, also called Piggybacking, is when an unauthorised person physically follows an authorised person into a restricted corporate area or system. In this module, it will have a scene which have two people one person will ask the person can help to scan the access card because his access card not working again. Then will ask user whether “Will you allow the person go in with you?”, if user choose “Yes” then will pop a message to tell user that had been attacked and provide some related information about tailgating attack to aware user, if choose “No” then will pop a message to congrats user have been successfully avoid a tailgating attack and with some related information.

### Scene 6 Shoulder Surfing Attack Module

Shoulder surfing is a criminal practice where thieves steal your personal data by spying over your shoulder as you use a laptop, ATM, public kiosk, or other electronic device in public. In this module, system will prompt a message for user whether enter your password when a person standing behind you. If user choose “Yes” then will pop a message to tell user that had been attacked and provide some related information about shoulder surfing attack to aware user, if choose “No” then will pop a message to congrats user have been successfully avoid a shoulder surfing attack and with some related information.

### Scene 7 Quiz Module

A quiz is usually a short test, and often does not have a huge impact on your grades as a test to determine your understanding. In this module, there will be ten questions about social engineering attack different types of pattern such as scenario-based question to give user think if they in that scenario what they will do, each question will have four selection for user to select, only can select one for each question. Then after answering all the questions, system will pop score of the user then can click for more information to study more about the social engineering attack and have more awareness knowledge about it.

### Scene 8 Video Module

In this module, video is a recording content of the social engineering attack to let user more understand social engineering attack based on video because video provide more visualization compare to text. In the video will have sound which more easy ways to let user to know more about social engineering attack then have awareness knowledge about it. There are five different social engineering attack such as brute force attack, phishing attack, SET toolkit attack, SQL Injection attack and Tailgating attack. By using video, visualization may create more memory and rise the awareness about social engineering attack for user.

### CHAPTER 6 CONCLUSION

This research explores the elements that may provide to overcoming the challenges posed from implementing training and awareness programs against social engineering, card game and escape room with SE. Enhancing information security training and awareness programs can help organizations achieve better results against social engineering skills. The main objective of information security SEAP, card game or even escape room is to enable people to enhance techniques in recognising, disabling, and reporting any social engineering malicious attempts. For an organization provide SEAP for all employees which cause a huge amount of expenditure. Then, for the card game, it not effective due to only allow play physically. For the escape room with SE, not convenience for people in different area to participate it. To solve all this obstacle, this paper proposes an awareness tools which provide the same working strategies but in different form to carry out by make use of this advance technology nowadays.

The aim of this Social Engineering attack awareness tool is to let people to have the knowledge of the social engineering attack and have awareness about it. Besides that, everyone can gain more knowledge and have much more awareness without spending a lot of money such as attending SEAP. Furthermore, to enhance the techniques in recognising social engineering attack by playing game will allow user to more clearly and have more attention and interest toward this awareness tool. These tools not just provide basic definitions about social engineering, it will be some fun games to lead users through penetration. Therefore, the user can enjoy the game and understand and have the concept of social engineering. Users are able to get the knowledge about social engineering attack by using this awareness tool while playing the game. This tool is to elicit and prioritize social engineering security requirements. Users are able to identify and understand some common social engineering. The limitation of this project is it is still a quite new tool for the public, it might need time for the public to accept and replace the awareness programs and training.

**BIBLIOGRAPHY**

A. Basden, A. T. Wood-Harper, "A philosophical discussion of the root definition in soft systems thinking: an enrichment of CATWOE", *Systems Research and Behavioral Science*, vol. 23, no. 1, pp. 61-87, 2006. [Accessed on 11 April 2020].

C. Hadnagy, *Unmasking the social engineer: The human element of security*, John Wiley & Sons, 2014. Available at <https://www.wiley.com/en-us/Unmasking+the+Social+Engineer%3A+The+Human+Element+of+Security-p-9781118608579> [Accessed on 11 April 2020].

C. Klimmt, U. Ritterfeld, M. Cody, P. Vorderer, "Serious games and social change: Why they (should) work" in *Serious games: Mechanisms and effects*, Routledge, 2009. [Accessed on 1 April 2020].

E.D.Oroszi, 2019, Security awareness escape room - a possible new method in improving security awareness of users Available at <https://ieeexplore-ieee-org.libezp2.utar.edu.my/document/8899715> [Accessed on 12 April 2020].

E. Elstad, "Educational Technology in Schools", *Digital Expectations and Experiences in Education*, pp. 47-57, 2016. [Accessed on 11 April 2020].

F. L. Greitzer, O. A. Kuchar, K. Huston, "Cognitive science implications for enhancing training effectiveness in a serious gaming context", *J. Educ. Resour. Comput.*, vol. 7, no. 3, 2007 [Accessed on 31 March 2020].

Ghafir, V. Prenosil, A. Alhejailan, M. Hammoudeh, "Social engineering attack strategies and defence approaches", *Future Internet of Things and Cloud (FiCloud) 2016 IEEE 4th International Conference*, pp. 145-149, 2016 [Accessed on 13 April 2020].

G. Watson, A. Mason, R. Ackroyd, *Social Engineering Penetration Testing: Executing Social Engineering Pen Tests Assessments and Defense*, 2011 [Accessed on 31 March 2020].

K.Beckers, S.Pape, 2016, A Serious Game for Eliciting Social Engineering Security Requirements. Available at <https://ieeexplore-ieee-org.libezp2.utar.edu.my/document/7765507/authors#authors> . [Accessed on 4 April 2020].

BIT (HONS) Communications and Networking  
Faculty of Information and Communication Technology (Kampar Campus), UTAR.

## BIBLIOGRAPHY

K. D. Mitnick, W. L. Simon, *The Art of Deception - Controlling the Human Element of Security*, Wiley, 2003 [Accessed on 6 April 2020].

M. Wilson, J. Hash, "Building an information technology security awareness and training program", NIST Special publication, vol. 800, no. 50, 2003 [Accessed on 11 April 2020].

P. Van den Boer, Introduction to Gamification Whitepaper, [online] Available: <https://cdu.edu.au/olt/ltrsources/downloads/whitepaper-introductiontogamification-130726103056-phpapp02.pdf>. [Accessed on 11 April 2020].

S. H. Houmb, S. Islam, E. Knauss, J. Jürjens, K. Schneider, "Eliciting security requirements and tracing them to design: An integration of common criteria heuristics and umlsec", *Requir. Eng.*, vol. 15, no. 1, pp. 63-93, 2010. [Accessed on 31 March 2020].

S. M. Poremba, "Open to Attack?", *Campus Technology*, vol. 25, no. 9, pp. 14-10, 2012. [Accessed on 11 April 2020].

S.Mohammed, E. Apeh, 2016, A model for social engineering awareness program for schools, Available at <https://ieeexplore-ieee-org.libezp2.utar.edu.my/document/7916253/authors#full-text-header> [Accessed on 12 April 2020].

T. Denning, A. Lerner, A. Shostack, T. Kohno, "Control-alt-hack: The design and evaluation of a card game for computer security awareness and education", *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security ser. CCS '13*. ACM, pp. 915-928, 2013. [Accessed on 31 March 2020].

T. Dimkov, A. van Cleeff, W. Pieters, P. Hartel, "Two methodologies for physical penetration testing using social engineering", *Proceedings of the 26th Annual Computer Security Applications Conference ser. ACSAC '10*. ACM, pp. 399-408, 2010. [Accessed on 31 March 2020].

Yuen (2020) In need of cybersecurity experts, *The Star*, Available at <https://www.thestar.com.my/news/focus/2020/03/22/in-need-of-cybersecurity-experts> [Accessed on 31 March 2020].

## BIBLIOGRAPHY

Yuen. MK, “Don’t fall prey to identity thieves”, The Star, p.12, Nov 2, 2017. [Online]. Available at [https://www.thestar.com.my/news/nation/2017/11/02/dont-fall-prey-to-identity-thieves-rising - cases-ofcriminals-stealing-personal-details-and-exploitin/](https://www.thestar.com.my/news/nation/2017/11/02/dont-fall-prey-to-identity-thieves-rising-cases-ofcriminals-stealing-personal-details-and-exploitin/) [Accessed on 31 March 2020]

# A PRELIMINARY PROPAGATION TOOL IN SOCIAL ENGINEERING ATTACKS



## INTRODUCTION

Levels of sophistication of social engineering threats and the exploits from such attacks are evolving. In particular, the lack of social engineering awareness is a concern in the context of human cyber security risks. There are some of the challenges that encounter in the process of developing the human knowledge to fight against social engineering attacks. This awareness tool let user to able understand the social engineering attacks which provide real case scenario for them know how social engineering attacks happen.



## METHODOLOGY

CREATE A PLATFORM USING UNITY HUB



DESIGN THE FEATURE REQUIRE



PROVIDE FEEDBACK AND GUIDE USER



LET USER KNOW THE PROBLEM THEN CAN BE  
TACKLED



## OBJECTIVES

- ➡ To design an awareness tools that ease user to explore the social engineering attacks rather than attend awareness program.
- ➡ To provide real case scenario how the social engineering attacks happen to lend them to understand how social engineering attacks are composed.



## DISCUSSION

AWARENESS TOOLS WHICH PROVIDE THE SAME WORKING STRATEGIES AS SOCIAL ENGINEERING AWARENESS PROGRAM BUT IN DIFFERENT FORM TO CARRY OUT WHICH IS BY AWARENESS TOOL TO LET USER ABLE TO UNDERSTAND THE SOCIAL ENGINEERING WITH SOME FUN GAMES, QUIZ, VIDEO, AND STUDY INFORMATION. BY USING GAME TO CREATE INTEREST AND LET THEM HAVE MORE STRONG AWARENESS THEN NEXT TIME WILL BE MORE VIGILANT.



## RESULTS



GAME



QUIZ



VIDEO



STUDY INFOMATION





Turnitin Originality Report Screenshot

Document Viewer

Turnitin Originality Report

Processed on: 05-Apr-2021 12:28 +08

ID: 1547242101

Word Count: 16726

Submitted: 3

A Preliminary Propagation Tool in Social Engi... By Peggy Hoong

Similarity Index

11%

Similarity by Source

Internet Sources: 8%

Publications: 6%

Student Papers: N/A

include quoted

include bibliography

exclude small matches

mode: quickview (classic) report

Change mode

print

download

1% match (publications)

[Eszter Diana Oroszl. "Security awareness escape room - a possible new method in improving security awareness of users", 2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment \(Cyber SA\), 2019](#)

1% match (publications)

[Kristian Beckers, Sebastian Pape. "A Serious Game for Eliciting Social Engineering Security Requirements", 2016 IEEE 24th International Requirements Engineering Conference \(RE\), 2016](#)

1% match (Internet from 07-Oct-2020)

<https://www.thestar.com.my/news/focus/2020/03/22/more-should-be-done-to-tackle-cyberthreats-in-the-community>

1% match (publications)

[Saba Mohammed, Edward Apeh. "A model for social engineering awareness program for schools", 2016 10th International Conference on Software, Knowledge, Information Management & Applications \(SKIMA\), 2016](#)

1% match (Internet from 22-Nov-2020)

<https://www.mdpi.com/1999-5903/11/13/73/htm>

1% match (Internet from 01-Apr-2019)

<http://eprints.utar.edu.my>

1% match (Internet from 09-Feb-2021)

<https://www.thestar.com.my/news/focus/2020/03/22/in-need-of-cybersecurity-experts>

<1% match (Internet from 17-Jul-2020)

<https://resources.infosecinstitute.com/whats-the-right-age-to-introduce-security-awareness/>

<1% match (Internet from 13-Sep-2020)



<b>Universiti Tunku Abdul Rahman</b>			
<b>Form Title : Supervisor's Comments on Originality Report Generated by Turnitin for Submission of Final Year Project Report (for Undergraduate Programmes)</b>			
Form Number: FM-IAD-005	Rev No.: 0	Effective Date: 01/10/2013	Page No.: 1 of 1



**FACULTY OF INFORMATION TECHNOLOGY**

<b>Full Name(s) of Candidate(s)</b>	PEGGY HOONG
<b>ID Number(s)</b>	17ACB02596
<b>Programme / Course</b>	CN
<b>Title of Final Year Project</b>	A Preliminary Propagation Tool in Social Engineering Attacks

<b>Similarity</b>	<b>Supervisor's Comments (Compulsory if parameters of originality exceeds the limits approved by UTAR)</b>
<b>Overall similarity index: <u>11</u> %</b>  <b>Similarity by source</b> Internet Sources: <u>8</u> % Publications: <u>6</u> % Student Papers: <u>N/A</u> %	Checked and Verified
<b>Number of individual sources listed of more than 3% similarity: <u>0</u></b>	Checked and Verified
<b>Parameters of originality required and limits approved by UTAR are as follows:</b> (i) Overall similarity index is 20% and below, and (ii) Matching of individual sources listed must be less than 3% each, and (iii) Matching texts in continuous block must not exceed 8 words <i>Note: Parameters (i) – (ii) shall exclude quotes, bibliography and text matches which are less than 8 words.</i>	

Note Supervisor/Candidate(s) is/are required to provide softcopy of full set of the originality report to Faculty/Institute

***Based on the above results, I hereby declare that I am satisfied with the originality of the Final Year Project Report submitted by my student(s) as named above.***

Signature of Supervisor  
Name: Dr Vasaki a/p Ponnusamy

Signature of Co-Supervisor  
Name: \_\_\_\_\_

Date: 5<sup>th</sup> April 2021

Date: \_\_\_\_\_



## UNIVERSITI TUNKU ABDUL RAHMAN



### FACULTY OF INFORMATION & COMMUNICATION TECHNOLOGY (KAMPAR CAMPUS)

#### CHECKLIST FOR FYP2 THESIS SUBMISSION

Student Id	17ACB02596
Student Name	PEGGY HOONG
Supervisor Name	Dr Vasaki a/p Ponnusamy

TICK (✓)	DOCUMENT ITEMS
	Your report must include all the items below. Put a tick on the left column after you have checked your report with respect to the corresponding item.
✓	Front Cover
✓	Signed Report Status Declaration Form
✓	Title Page
✓	Signed form of the Declaration of Originality
✓	Acknowledgement
✓	Abstract
✓	Table of Contents
✓	List of Figures (if applicable)
✓	List of Tables (if applicable)
✓	List of Symbols (if applicable)
✓	List of Abbreviations (if applicable)
✓	Chapters / Content
✓	Bibliography (or References)
✓	All references in bibliography are cited in the thesis, especially in the chapter of literature review
✓	Appendices (if applicable)
✓	Poster
✓	Signed Turnitin Report (Plagiarism Check Result - Form Number: FM-IAD-005)

\*Include this form (checklist) in the thesis (Bind together as the last page)

<p>I, the author, have checked and confirmed all the items listed in the table are included in my report.</p>  <hr/> <p>(Signature of Student) Date: 5th April 2021</p>	<p>Supervisor verification. Report with incorrect format can get 5 mark (1 grade) reduction.</p>  <hr/> <p>(Signature of Supervisor) Date: 5th April 2021</p>
---	---

# FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

<b>Trimester, Year:</b> Trimester 3, Year 3	<b>Study week no.:</b> 2
<b>Student Name &amp; ID:</b> Peggy Hoong 17ACB02596	
<b>Supervisor:</b> Dr Vasaki a/p Ponnusamy	
<b>Project Title:</b> A Preliminary Propagation Tool in Social Engineering Attacks	

## 1. WORK DONE

- Research

## 2. WORK TO BE DONE

- Revise back FYP1 report.

## 3. PROBLEMS ENCOUNTERED

## 4. SELF EVALUATION OF THE PROGRESS

- Self-assigned tasks are completed within expected timeframe.



Supervisor's Signature



Student's Signature

# FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

<b>Trimester, Year:</b> Trimester 3, Year 3	<b>Study week no.:</b> 4
<b>Student Name &amp; ID:</b> Peggy Hoong 17ACB02596	
<b>Supervisor:</b> Dr Vasaki a/p Ponnusamy	
<b>Project Title:</b> A Preliminary Propagation Tool in Social Engineering Attacks	

## 1. WORK DONE

- Structure the game
- Plan for the game flow

## 2. WORK TO BE DONE

- Design the image needed in the game

## 3. PROBLEMS ENCOUNTERED

## 4. SELF EVALUATION OF THE PROGRESS

- Good start of the project, keep it up



Supervisor's Signature



Student's Signature

# FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

<b>Trimester, Year:</b> Trimester 3, Year 3	<b>Study week no.:</b> 6
<b>Student Name &amp; ID:</b> Peggy Hoong 17ACB02596	
<b>Supervisor:</b> Dr Vasaki a/p Ponnusamy	
<b>Project Title:</b> A Preliminary Propagation Tool in Social Engineering Attacks	

## 1. WORK DONE

- Design the image needed in the game

## 2. WORK TO BE DONE

- Create and design the different scene in game (quiz scene)
- Writing FYP II report

## 3. PROBLEMS ENCOUNTERED

- Clicked the button in game scene no response

## 4. SELF EVALUATION OF THE PROGRESS

- Self-assigned tasks are completed within expected timeframe.



Supervisor's Signature



Student's Signature

# FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

<b>Trimester, Year:</b> Trimester 3, Year 3	<b>Study week no.:</b> 8
<b>Student Name &amp; ID:</b> Peggy Hoong 17ACB02596	
<b>Supervisor:</b> Dr Vasaki a/p Ponnusamy	
<b>Project Title:</b> A Preliminary Propagation Tool in Social Engineering Attacks	

## 1. WORK DONE

- Create and design the different scene in game (quiz scene)

## - WORK TO BE DONE

- Create and design the text box in the game (game scene)
- Writing FYP II report
- Meeting with supervisor

## 2. PROBLEMS ENCOUNTERED

- The scene in game cannot join and display smoothly

## 3. SELF EVALUATION OF THE PROGRESS

- Self-assigned tasks are completed within expected timeframe.



Supervisor's Signature



Student's Signature



# FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

<b>Trimester, Year:</b> Trimester 3, Year 3	<b>Study week no.:</b> 10
<b>Student Name &amp; ID:</b> Peggy Hoong 17ACB02596	
<b>Supervisor:</b> Dr Vasaki a/p Ponnusamy	
<b>Project Title:</b> A Preliminary Propagation Tool in Social Engineering Attacks	

## 1. WORK DONE

- Create and design the text box in the game (game scene)
- Meeting with supervisor

## - WORK TO BE DONE

- Combine all the scene and edit the smoothness of flow
- Create and design the text box in the game (video scene)
- Add shoulder surfing scene in the awareness tool
- Edit FYP report

## 2. PROBLEMS ENCOUNTERED

- The scene in unity has some problems
- Video editing problem

## 3. SELF EVALUATION OF THE PROGRESS

- Self-assigned tasks are completed within expected timeframe



Supervisor's Signature



Student's Signature

# FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

<b>Trimester, Year:</b> Trimester 3, Year 3	<b>Study week no.:</b> 11
<b>Student Name &amp; ID:</b> Peggy Hoong 17ACB02596	
<b>Supervisor:</b> Dr Vasaki a/p Ponnusamy	
<b>Project Title:</b> A Preliminary Propagation Tool in Social Engineering Attacks	

## 1. WORK DONE

- Combine all the scene and edit the smoothness of flow
- Add shoulder surfing scene in the awareness tool
- Finished writing FYP II report

## 2. WORK TO BE DONE

- Need to send the report to Turnitin for plagiarism checking.
- 

## 3. PROBLEMS ENCOUNTERED

-

## 4. SELF EVALUATION OF THE PROGRESS

- Self-assigned tasks are completed within expected timeframe.



Supervisor's Signature



Student's Signature

# FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

<b>Trimester, Year:</b> Trimester 3, Year 3	<b>Study week no.:</b> 12
<b>Student Name &amp; ID:</b> Peggy Hoong 17ACB02596	
<b>Supervisor:</b> Dr Vasaki a/p Ponnusamy	
<b>Project Title:</b> A Preliminary Propagation Tool in Social Engineering Attacks	

## 5. WORK DONE

- Turnitin for plagiarism checking.
- Finished writing FYP II report

## 6. WORK TO BE DONE

- Generate a final version of report and let supervisor to sign

## 7. PROBLEMS ENCOUNTERED

-

## 8. SELF EVALUATION OF THE PROGRESS

- Self-assigned tasks are completed within expected timeframe.



Supervisor's Signature



Student's Signature