Ain Shams University
Faculty of Computer and Information Sciences
CYBER SECURITY PROGRAM

Cyber Learning Adventure (Junior)

July 2022

Ain Shams University
Faculty of Computer and Information Sciences
CYBER SECURITY PROGRAM

Cyber Learning Adventure (Junior)

By:

Omar Ahmed Wafaa Eldeen
Abdelrahman Mohamed Kamal
Ahmed Essam El-Deen Mohamed Ahmed
David Moheb Anwar
Omar Magdy Abdelhamed Nassar

Under Supervision of:

Dr. Hanan Hindy
Lecturer,
Computer Science Department,
Faculty of Computer and Information Sciences,
Ain Shams University.

Acknowledgement

First, we would like to thank God for giving us the strength to achieve this project.

We owe our deepest gratitude to our supervisor Dr. Hanan Hindy for all her efforts guiding us through the whole project duration, encouragement and continuous optimism concerning this work. Moreover, her leadership and how she managed to inspire and guide us through the past year, her experience and enthusiasm that she passed on to every one of the team.

We are deeply grateful for our college support that came from all the staff there, all the professors who lectured us and teaching assistants who gave us lots of guidance.

Finally, it is a pleasure to thank those who made this project possible who are represented in our colleagues and most important our families for their support through the whole project duration.

Abstract

The Covid-19 pandemic caused kids nowadays to depend on e-learning and as a result spend a lot of time in front of their screens on daily basis. This means that children can be exposed to a new set of threats due to their use of web-based tools, downloading new applications, or reliance on email grows and there is no way for parents who are preoccupied with their daily tasks to monitor what their children are doing on the internet.

Added to that, most of the websites and resources available to raise awareness towards dealing with the dangers of internet are aimed at adults which means that they are far too advanced and not easy to understand by kids. As a result, it is nearly impossible for the younger generation to benefit from this information in any way. This makes them in danger while using the internet and easy target for internet predators.

This is where Cyber Learning Adventure (Junior) kicks in, it is a game that aims to strengthening children's defences against security threats as well as teaching them how to deal with them in an enjoyable yet efficient way. It guarantees the child to have enough practical hands-on experience and learn about famous attacks such as phishing, social engineering and brute force to get him ready before using the internet.

Table of Contents

List of Figures

1- Introduction

1.1 Motivation

This project aims to help children in gaining the necessary awareness to protect themselves against the threats they can face while using the internet. This is because the only available awareness-providing tools are aimed at adults and are far too advanced for children.

1.2 Problem Definition

Since the Covid-19 pandemic, kids nowadays spend a lot of time in front of screens and using the internet on daily basis. With the lack of awareness, children are exposed to a new set of threats as their use of web-based tools, downloading new applications, and reliance on email grows.

1.3 Objectives

- Offering a gamified and enjoyable way for kids to learn about cyber security threats and attacks.
- Providing a simple, yet efficient ways to report security attacks.
- Implementing practical hands-on experience.

1.4 Time Plan

Figure 1 shows the time plan of the project which covers the different phases. Firstly, the project background contains a common description of the field of the project, all the scientific background related to the project, a survey of the related work done in the field, and searching for existing similar systems and description of any technology used. The implementation phase includes the actual implementation of all the functions in the system,. The areas to improve contains the parts of the project where some enhancements need to be done. Finally, the project documentation is the process of recording the key project details and producing the documents that are required to implement it successfully.

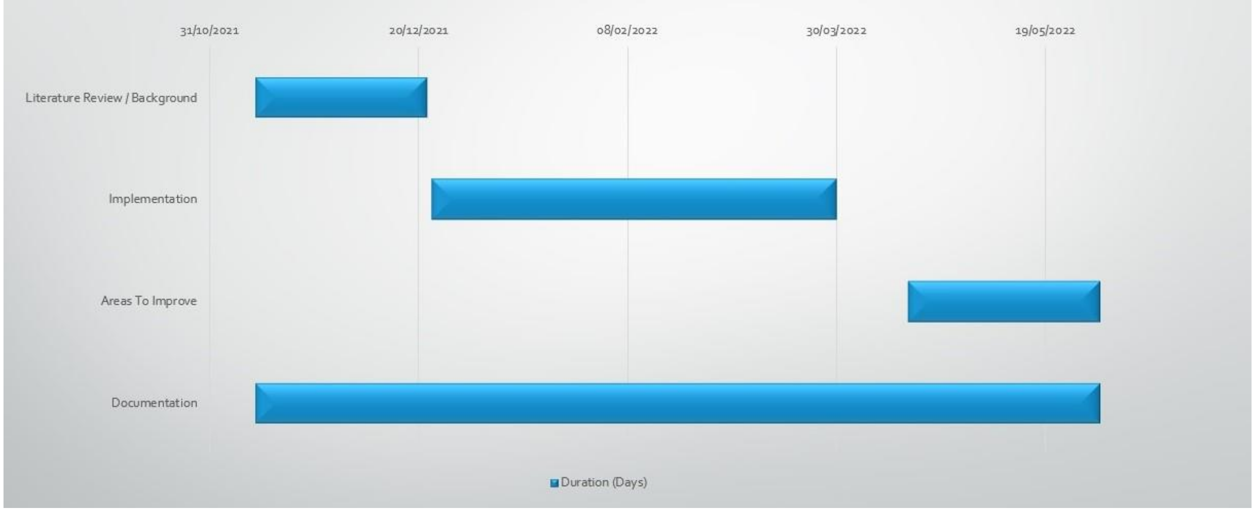


Figure 1- Time Plan

1.5 Document Organization

Chapter 2 explains the different topics regarding the background of the project such as the field of the project, a survey of the work done in this field. It also discusses, the scientific background related to the project, similar systems to the game and technologies used. Chapter 3 outlines the implementation and testing, it describes all the functions used in the system, all the techniques and algorithms used, and a description of any new technologies used in implementation & testing procedures and levels used. Chapter 4 includes the user manual. In Chapter 5, the project is summarized with the results obtained and the future work is stated.

2- Background

This chapter includes citation of theoretical background, related work be included. This chapter is going to discuss and go deeper in how we plan the project and explain the steps and theinstructions that we’ve followed to analysis and plan the project phases.

2.1 Statistics

Figure 1 shows the statistics of the most famous threats that children face online. These threats include; malware, identity theft and others.

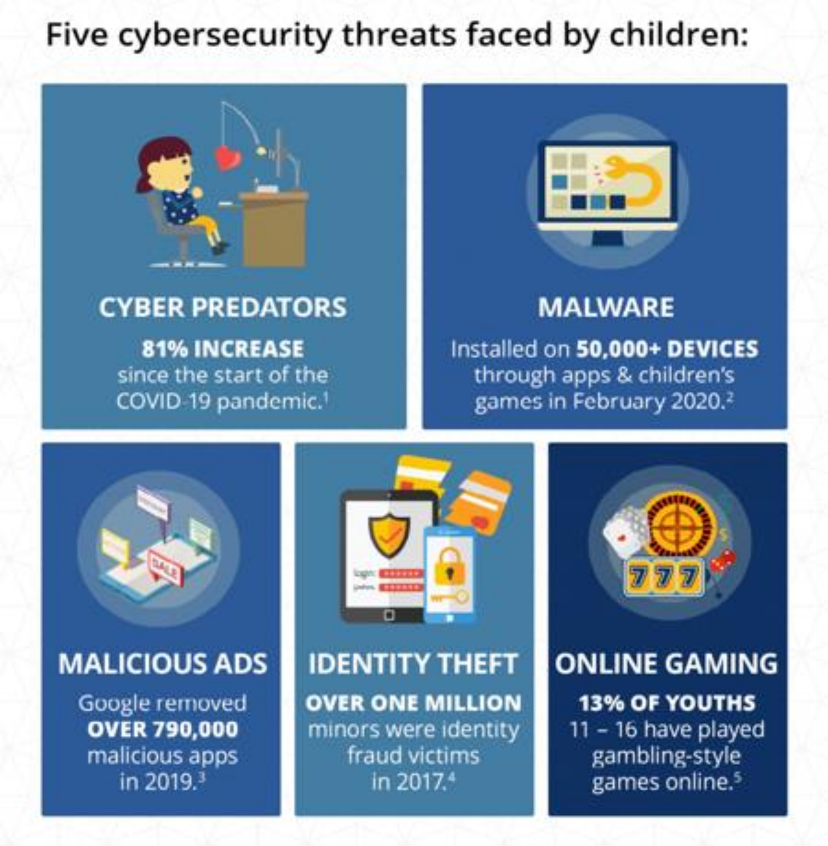

Five cybersecurity threats faced by children:
CYBER PREDATORS
81% INCREASE since the start of the COVID-19 pandemic.[1]
MALWARE
Installed on 50,000+ DEVICES through apps & children's games in February 2020.[2]
MALICIOUS ADS
Google removed OVER 790,000 malicious apps in 2019.[3]
IDENTITY THEFT
OVER ONE MILLION minors were identity fraud victims in 2017.[4]
ONLINE GAMING
13% OF YOUTHS 11 – 16 have played gambling-style games online.[5]

Figure 2 – Cybersecurity threats and Children [1]

As shown in Figure 2, internet consumption by children based on their age. Furthermore, the figure shows that from 2007 to 2017 the internet consumption increased in terms of weekly hours and as the child grows, he uses the internet more.

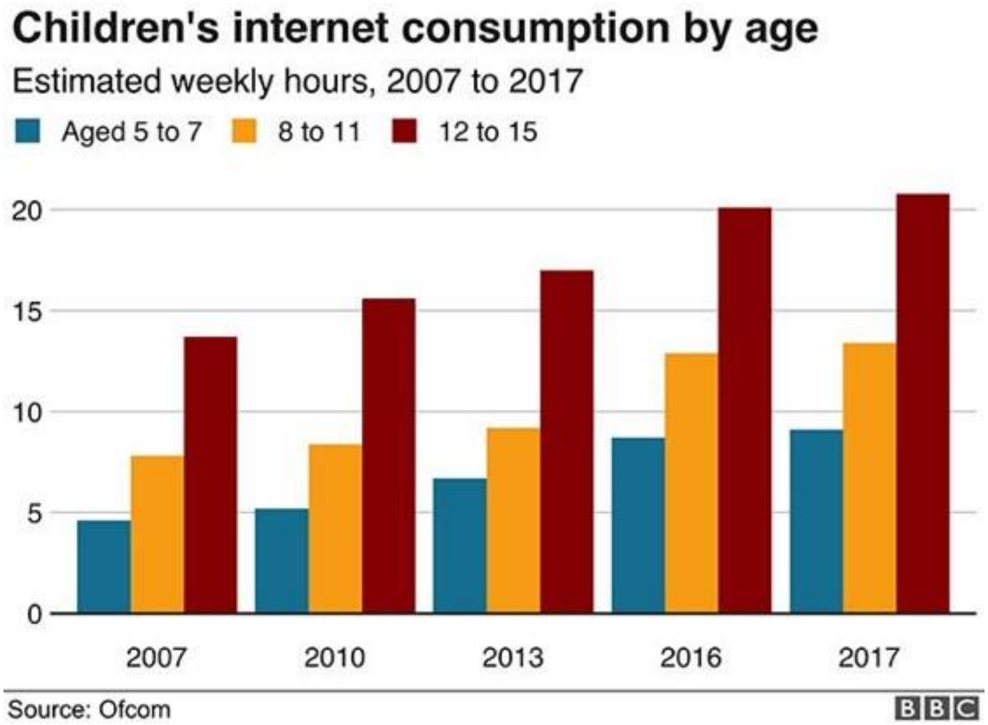


Figure 3 – Internet consumption by Children [2]

2.2 Cyber Threat Modelling

Almost all software systems today deal with a range of threats, and new ones are continually being added as technology evolves. These threats can emerge from both inside and outside of organizations, and their impact can be severe. Systems could be rendered inoperable, or sensitive information could be disclosed, eroding user trust in the system provider [1]. Therefore, any organization shall be ready for any consequences and know how to act upon that.

As the world has gotten more digital, cyber assaults have become more regular and frequent; as a result, threat modelling is no longer an optional activity. Threat modelling can assist you in making your product safer and trustworthy. As there are many threat models out there, some of which are typically used alone, some are usually used in conjunction with others, and some are examples of how different methods can be combined, No one threat modelling method is recommended over another; the decision of which method(s) to use should be based on the needs of the project and its specific concerns like are there any specific areas you want to target (risk, security, privacy), or how long you have to perform threat modelling.

Cyberbullying is one of the most famous threats that faces kids online every day, it is bullying that takes place over digital devices like cell phones, computers, and tablets. This is arguably one of the most challenging threats to deal with as it happens easily and does not need face to face communication to happen. It can happen to any kid while using social media platform, communication platform etc. This activity is very famous as statistics[1] showed that almost 34% of kids aged 12–17 have been cyberbullied at some point in their life, and 11.5% have bullied someone else online.

Anonymous sharing is another common online threat which is about using the apps that allows posting content without revealing who you are, this content can be showed up temporarily and then removed like snapchat. But the fact that it is temporary does not make it safe because screenshots can be taken. Anonymous sharing also gives kids the satisfaction to share information with people online without being afraid that he can be known but this can lead to oversharing which means they can give away important information or being mocked into opening links or attachments containing malware. This can be explained as social engineering which is a method used by cyberthieves to get private information.

Speaking about theft of private information, phishing must be mentioned because it is the most common tactic to steal personal and financial information. Children can be targeted by scammers pretending to be other players in video games and friends on messaging apps. They can also be targeted on social media apps and fooled by messages containing prizes, corrupted links.

Kids using internet can be exposed to inappropriate content at any time if they are not careful or not using child-friendly browser. The Internet is chock-full of inappropriate content from vulgar language and hate speech to graphically violent or sexual images can have a harmful effect on an impressionable child.

Inappropriate content takes us to another huge threat which is malware is a type of program that infects your computer or phone with the intention of causing harm. Malware is used to damage or destroy your device, allow cyber criminals to spy on you, steal your personal information or hold your files for ransom. Kids who love gaming and downloads games regularly can download malicious files without noticing.

Cyber stalking is a widely prevalent cybercrime that poses a risk to children online. Anyone can conceal his/their identity or use fake names to start a conversation with a child online or use the available information about the child such as their email address to send them harassing or intimidating content online [2].

2.3 Cyber Threats on Kids

The internet can be a dangerous neighborhood for everyone, but children and teens are especially vulnerable. From cyber predators to social media posts that can come back to haunt them later in life, online hazards can have severe, costly, even tragic, consequences. Children may unwittingly expose their families to internet threats, for example, by accidentally downloading malware that could give cyber criminals access to their parents' bank account or other sensitive information. Protecting children on the internet is a matter of awareness—knowing what dangers lurk and how to safeguard against them [3].

2.4 Kids Internet Usage

According to best estimates one in three children around the world now uses the internet. First things first, why are the internet rapidly used by children? Internet is fast becoming trusted by both children and adults as reliable and accurate sources of information. Through the internet children now can have access to an almost endless supply of information and opportunity for interaction. However, there can be real risks and dangers for an unsupervised child.

Since the start of the pandemic, governments worldwide have implemented measures to contain the spread of covid-19, one of which is school closures all over the world. As a result, e-learning has become a viable solution. Internet usage can be a medium of learning online, the information related to the task as well as the latest information can impact the cognitive development [4].

In Indonesia, until the 1990s, after school, children used to go out with their friends to play together and interact among each other. But during these times, this condition has become very rare. This is due to the child “net generation” tends to use the internet as fun activity for them. With using the internet, their needs are met such as obtaining entertainment.

Social media is another aspect that makes children use internet. The internet facilitates communication with geographically distant family and friends as well as making it easier to communicate frequently with those nearby. There is another of advantage of social media which is making new friends through games and groups made on social media.[5]

2.5 Gamification

The idea behind gamification is enriching products, services, and information systems with game-design elements in order to positively influence motivation, productivity. Gamification is a persuasive technology that attempts to influence user behavior by activating individual motives via game-design elements. The idea of gamification is spawning an intense public debate as well as numerous applications ranging across productivity, finance, health, education, sustainability, as well as news and entertainment media. Several vendors now offer “gamification” as a software service layer of reward and reputation systems with points, badges, levels and leader boards. More specific notion is that since video games are designed with the primary purpose of entertainment, and since they can demonstrably motivate users to engage with them with unparalleled intensity and duration, game elements should be able to make other, non-game products and services more enjoyable and engaging as well .

Games with a purpose reflect an approach in which problems that cannot satisfactorily be solved with information systems are transformed, so that human individuals can solve them in a game-like fashion. The potential of gamification is based on comprehensive motivational support and on invoking flow experiences [6].

IT-based gamified enhancing services able to arouse the intrinsic motivation of users regarding a core offer:

- Increase in user satisfaction.
- Conveyance of optimism.
- Facilitation of social interaction.
- Provision of meaning.

2.6 Capture the Flag Challenges

Capture the Flag (CTF) challenges are a popular form of cybersecurity education, where students/participants solve hands-on tasks in an informal, game-like setting. The term "Capture the Flag" originally refers to an outdoor game for two teams. Each team must simultaneously defend a (physical) flag in their base and steal the other team's flag. CTF tasks, called challenges, feature diverse assignments from exploiting websites, through cracking passwords, to breaching unsecured networks. A successful solution of a challenge yields a text string called a flag that is submitted online to prove reaching the solution. Three types of CTF games are generally distinguished: quiz based, in which participants score points by answering questions; scavenger-hunt, or flag-based, in which participants locate and exploit vulnerabilities in systems security in order to gain access to files which contain "flags" in the form of random strings, and king-of-the-hill, or castle-based, in which participants score points by defending a server against attackers.

CTF competitions are very popular for testing skills and presenting challenges for practice on various security topics such as cryptography, steganography, web or binary exploitation and reverse engineering among others. CTF challenges should also include non-technical aspects to address the current advanced cyber threats and attract audience to cybersecurity. CTF tasks showed the prominence of technical knowledge about cryptography and network security, but human aspects, such as social engineering and cybersecurity awareness are neglected, which we will focus on. By introducing gamification components, a shared scoring system to encourage some friendly competition, and the ability to buy hints using points that were scored by solving previous challenges, we anticipate that students will enjoy participation in the CTF. By active participation, students will spend more time learning and develop stronger outcomes. Overwhelmingly, participants were able to define and explain the consequences of password re-use, phishing and weak configurations. Significant increases in outcomes will be observed in participants' ability to describe the risks of using weak passwords. Self-confidence of students will improve by participating in (CTFs). Participating in the CTF reinforces theoretical concepts.[6]

2.7 Related Work and Similar Systems

CyberTalents Kids is a gamified cybersecurity training platform focused on kids from 11 to 16 years old across the globe where they can learn, practice, compete, and get ranked [7]. However, CyberTalents Kids is complex and not simple enough to be understood by the kids.

Cybersmart challenge is a Teacher-led activities using animated videos to introduce primary school students to key online safety issues including cyberbullying, protecting personal information and sharing images. The outcome is that the Students will be better equipped to understand and manage key online safety issues, including inappropriate or unwanted contact, cyberbullying and the risks of sharing images online.[8]

Added to that, Hack The Box is another existing platform which is an online platform allowing you to test one's penetration testing skills and exchange ideas and methodologies with other members of similar interests. It contains several challenges that are constantly updated. Some of them simulating real world scenarios and some of them leaning more towards a CTF style of challenge. As an individual, a simple challenge can be completed to prove skills level and then create an account, allowing the participant to connect to our private network (HTB Net) where several machines can be hacked. By hacking machines, points are gained that help in increasing the rankings [9].

Furthermore, The Open Web Application Security Project® (OWASP) is a nonprofit foundation that works to improve the security of software. Through community-led open-source software projects, hundreds of local chapters worldwide, tens of thousands of members, and leading educational and training conferences, the OWASP Foundation is the source for developers and technologists to secure the web [10].

The research conducted by Quayyum *et al.* about "Cybersecurity awareness for children" summarize the current findings on cybersecurity awareness research for children and help guide future studies. The authors performed a systematic literature review on cybersecurity awareness for children, analyzing 56 peer-reviewed studies that report in depth on various cybersecurity risks and awareness-raising approaches.

The results of this review include a list of cybersecurity risks for children, a list of commonly used approaches and theories for raising cybersecurity awareness among children, and a list of factors that researchers have considered when evaluating cybersecurity awareness approaches and solutions [11].

The work done in [12] introduces a new mobile app in the Arabic language to educate Arab-speaking people in the Middle East and North Africa (MENA) about cybersecurity and to increase their awareness of information assurance and cybercrimes. The app was developed for Android and iOS devices, and it includes multiple-choice information assurance questions, terms, and articles. Examples of the term definitions are Two-Factor Authentication, Ethical Hacking, and Honeypot.[12]

2.8 Technologies used

- Game Engine
  -Unity
- Programming Language
  -C#
- Code IDE
  -Visual Studio
- Graphics Tool
  -Gimp
  -Photoshop

3- Implementation and Testing

3.1 Password Complexity

Password complexity is a measure of how difficult a password is to guess in relation to any number of guessing or cracking methods. In our context, the player is asked initially to enter a password haphazardly. During the adventure, the player passes by different scenarios that strengthen his or her knowledge regarding how to have a secure password.

Based on NIST password requirements, a minimum of eight characters and a maximum length of at least 64 characters is required for a complex password[13], therefore, the player's first challenge is to choose a password that suits the required length. If the password entered by the player passes the condition, the player proceeds to the next scenario which also strengthen his or her knowledge. The next scenario focuses on what type and structure of characters the player uses; as per NIST, a complex password shall have different structures of characters: upper case, lower case, special characters, numbers, and symbols. The player is asked to enter a password that contains the mentioned structure of characters; the password shall contain upper and lower characters, in addition to symbols and numbers. If the entered password satisfies the implemented condition, the player proceeds to the final scenario.

The final scenario focuses on the password's unfamiliarity as NIST requires to never use common passwords and dictionary words. The player is asked to enter a password, and that password is checked if it's in the most common 1000 passwords that got leaked online. If the password bypasses the condition and got to be unfamiliar, the player proceeds to final scene where the boss is awaiting. In the boss fight scene, the player shall already got the knowledge needed in how to have a secure complex password. To kill the boss, the player should use the knowledge from previous scenarios in that final scene; the player is asked to enter a secure complex password as per NIST requirements. The password entered should have the required length, the required structure of characters and should be unfamiliar, the three conditions are dependent and should be fulfilled in order to pass the boss and finalize the first level of the game.

3.2 Phishing

Phishing happens when a person sends a bogus SMS, email, or pop-up message in order to get personal information, passwords, or financial information from others[14]. Once they obtain this information, the hackers will use it to commit identity theft or to steal money. In our context, we got templates of malicious pop-up messages and advertisements that we encounter in our daily life; clicking on such pop-ups may lead to malicious activities done by hackers who host such pop-ups.

During the game journey, the player encounters random attractive malicious pop-ups, clicking on the pop-ups' malicious buttons will cost the player his or her health and closing the pop-up window is the only way to bypass that scenario; the goal is to never trust such pop-ups and always ignore their existence.

The next scenario focuses on fake links that are sent with phishing emails. Fake links are malicious links hosted by hackers and the aim of phishing attacks is to redirect victims to these malicious links. The player comes across random well known and common domain links, but some are not legitimate, a letter could be added or transposed to another letter and the goal is to always stay focused and distinguish between fake and legitimate ones. The player is asked to tell if a certain domain link is fake or not, if the player is not focused enough, his or her health will decrease. The goal of that scenario is to know what a fake domain looks like in order to know if the sent email is a phishing email or not in terms of links included in such emails.

3.3 Information Disclosure

Information disclosure happens when sensitive and confidential information are exposed to users who are not normally supposed to have access to that data. While such flaws are not usually exploitable, they allow malicious hackers to gather valuable information that can be used later in the attack lifecycle. Armed with such data, attackers can achieve much more than they could without it.

To simulate an attack that targets information disclosure, we implemented a chat bot since such attack needs some sort of person-to-person communication. A chat bot is a software or computer program that simulates human conversation or "chatter" through text or voice interactions.[15]

Chat bots can be stateless or stateful, with differing degrees of complexity. Stateless chat bots approach each discussion as though it were their first encounter with a new user. Stateful chat bots, on the other hand, can evaluate previous encounters and frame new responses in context.

In our context, we implemented a stateless chat bot based on Oscova which is a part of Syn.Bot framework in unity. We started by setting up the chat interface which consists of a display box and buttons. We then started to setup the chat bot and linked the chat interface with the chat bot: Anonymous message and color, User message and color and what messages will be displayed. The bot’s knowledge base was focused on scenarios that target a user to expose personal information. The player chats with a hacker who claims to be innocent in order to deceive the player to expose sensitive information. The player has 3 buttons to click on: Accept, Reject and Skeptical. Each button sends different response to the hacker, and each response from the player gets a different response from the hacker as well as per the knowledge base we implemented in the chat bot. The Accept button if clicked sends an acceptance response to the hacker but that will cost the player his or her health.

The Reject button for instance will ignore the chat and that is only way to bypass that scenario. The goal is to never chat with anonymous persons and always ignore such chats that may lead to such attack since the attack is carried by expert social engineers who know how to deceive victims.

4- User Manual

In this chapter you would find a guide that teaches the users how to play the game through guidelines that will explains every aspect of the game.

4.1 Main Menu

This is the screen you will see when you open the game, it contains three buttons, the first button the play now which starts the game when you click it, the second button is the exit which closes the game when you click it, and the third button is the settings.

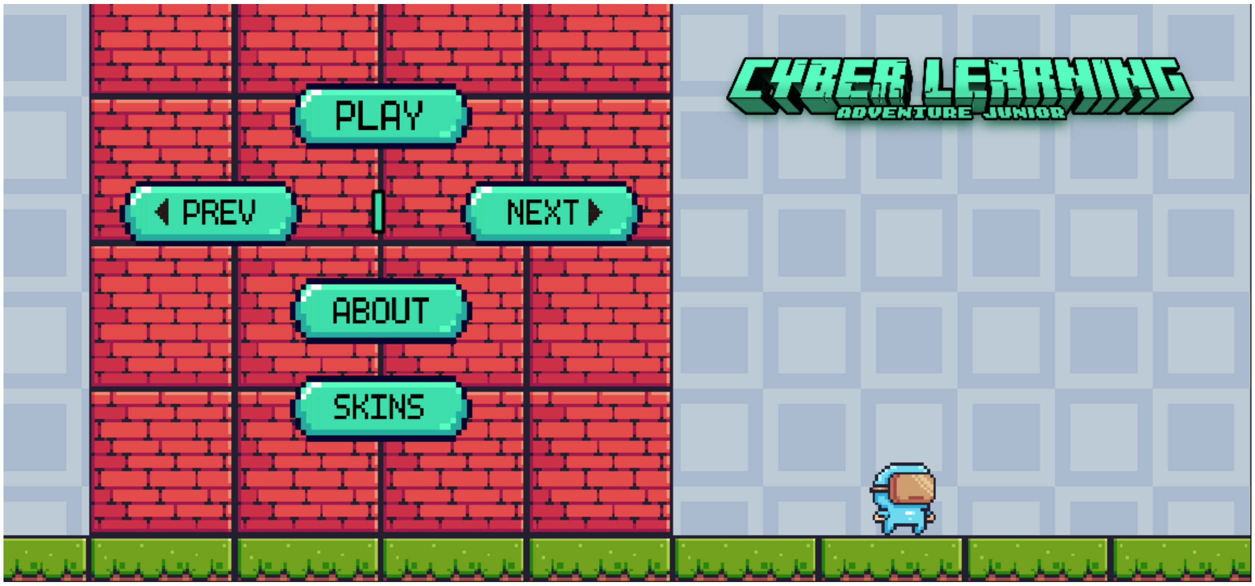


Figure 4- Main Menu, Prototype

4.2- Settings

This is the screen that opens after clicking the settings button in the start page. It contains three buttons, the first button is About which shows a description about the game, the second button is a button that resets your progress in the game and the third button moves you back to the start page.

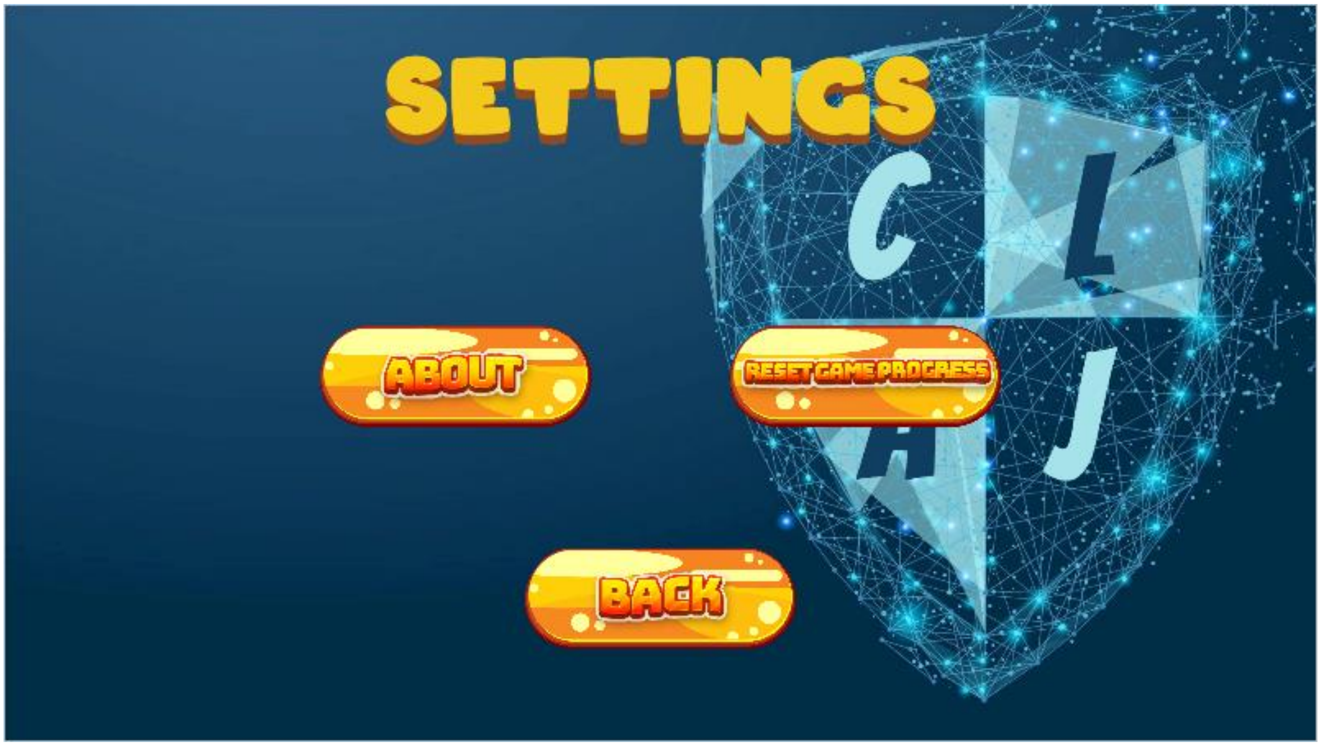
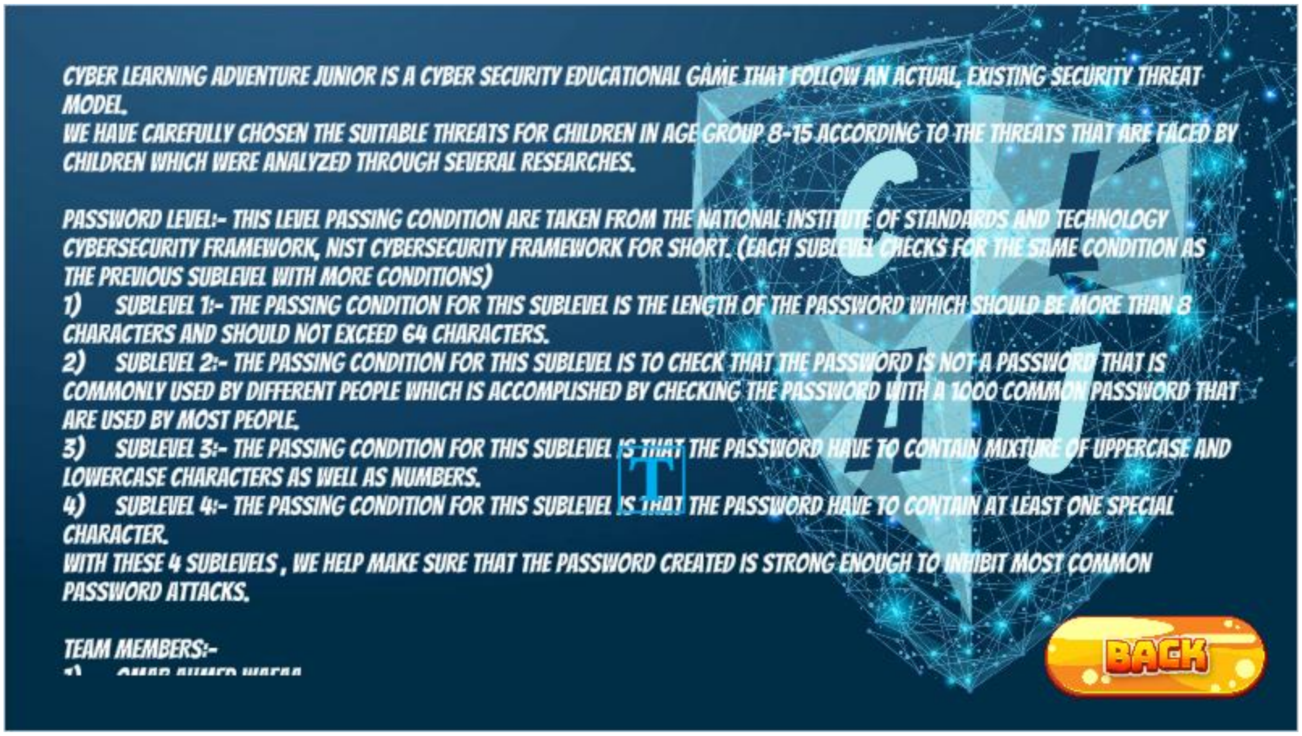


Figure 5- Settings Screen, Prototype

4.3- About

This is the about screen that contains a full description of the game and names of the team members.



CYBER LEARNING ADVENTURE JUNIOR IS A CYBER SECURITY EDUCATIONAL GAME THAT FOLLOW AN ACTUAL, EXISTING SECURITY THREAT MODEL.
WE HAVE CAREFULLY CHOSEN THE SUITABLE THREATS FOR CHILDREN IN AGE GROUP 8-15 ACCORDING TO THE THREATS THAT ARE FACED BY CHILDREN WHICH WERE ANALYZED THROUGH SEVERAL RESEARCHES.

PASSWORD LEVEL:- THIS LEVEL PASSING CONDITION ARE TAKEN FROM THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY CYBERSECURITY FRAMEWORK, NIST CYBERSECURITY FRAMEWORK FOR SHORT. (EACH SUBLEVEL CHECKS FOR THE SAME CONDITION AS THE PREVIOUS SUBLEVEL WITH MORE CONDITIONS)

1) SUBLEVEL 1:- THE PASSING CONDITION FOR THIS SUBLEVEL IS THE LENGTH OF THE PASSWORD WHICH SHOULD BE MORE THAN 8 CHARACTERS AND SHOULD NOT EXCEED 64 CHARACTERS.
2) SUBLEVEL 2:- THE PASSING CONDITION FOR THIS SUBLEVEL IS TO CHECK THAT THE PASSWORD IS NOT A PASSWORD THAT IS COMMONLY USED BY DIFFERENT PEOPLE WHICH IS ACCOMPLISHED BY CHECKING THE PASSWORD WITH A 1000 COMMON PASSWORD THAT ARE USED BY MOST PEOPLE.
3) SUBLEVEL 3:- THE PASSING CONDITION FOR THIS SUBLEVEL IS THAT THE PASSWORD HAVE TO CONTAIN MIXTURE OF UPPERCASE AND LOWERCASE CHARACTERS AS WELL AS NUMBERS.
4) SUBLEVEL 4:- THE PASSING CONDITION FOR THIS SUBLEVEL IS THAT THE PASSWORD HAVE TO CONTAIN AT LEAST ONE SPECIAL CHARACTER.

WITH THESE 4 SUBLEVELS , WE HELP MAKE SURE THAT THE PASSWORD CREATED IS STRONG ENOUGH TO INHIBIT MOST COMMON PASSWORD ATTACKS.

TEAM MEMBERS:-
1) OMAR AHMED WAFAA

Figure 6- About Screen, Prototype

4.4- Levels

Here you can find the different levels in the game where you can start or continue playing in the level you like.

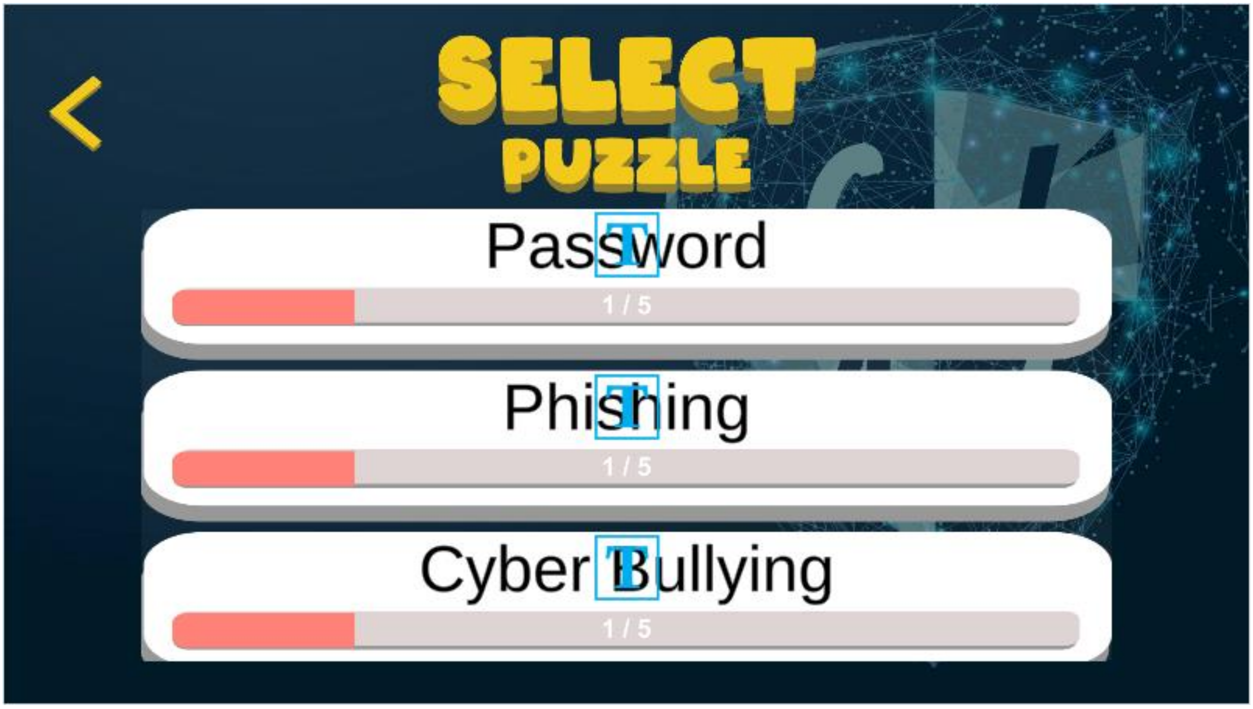


Figure 7- Screen displays different levels, Prototype

4.5- Well Done

After you win this is the screen that opens, it contains two buttons, next button that you click in case you want to continue playing and exit button that closes the game.

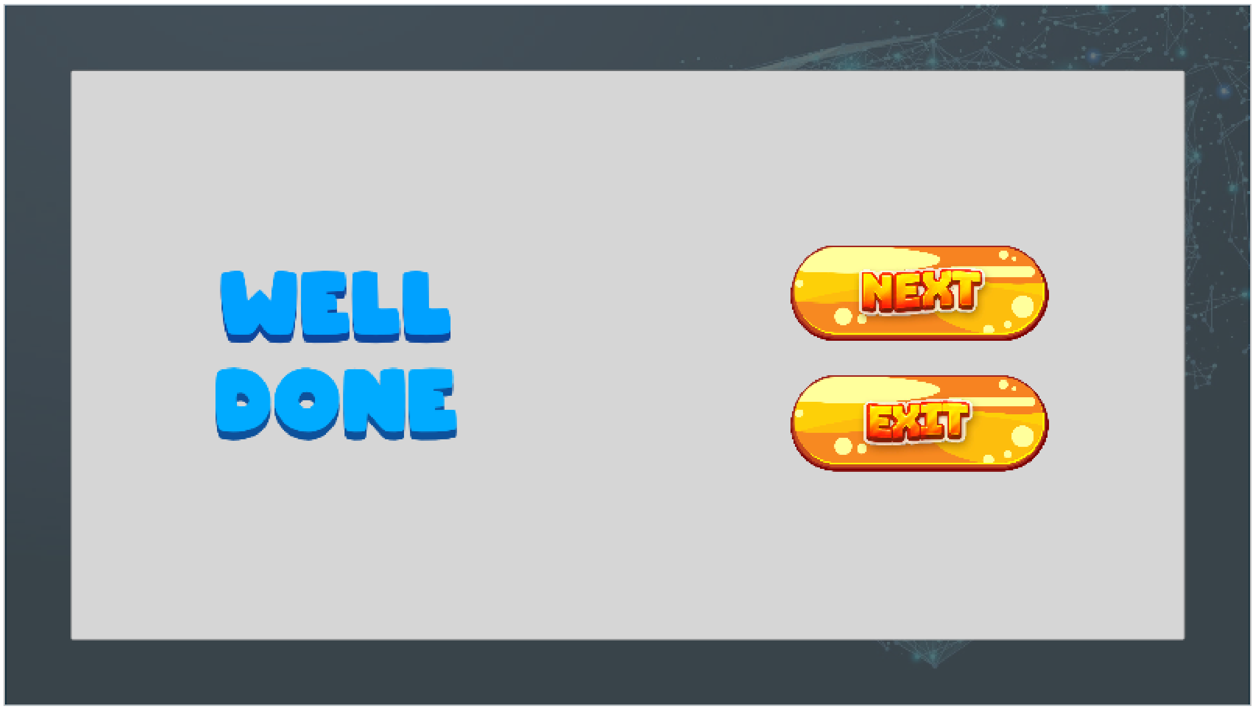


Figure 8- Screen in case you win, Prototype

4.6- Game Over

In case you lost, you get two buttons, one to start playing again and one to close the game.

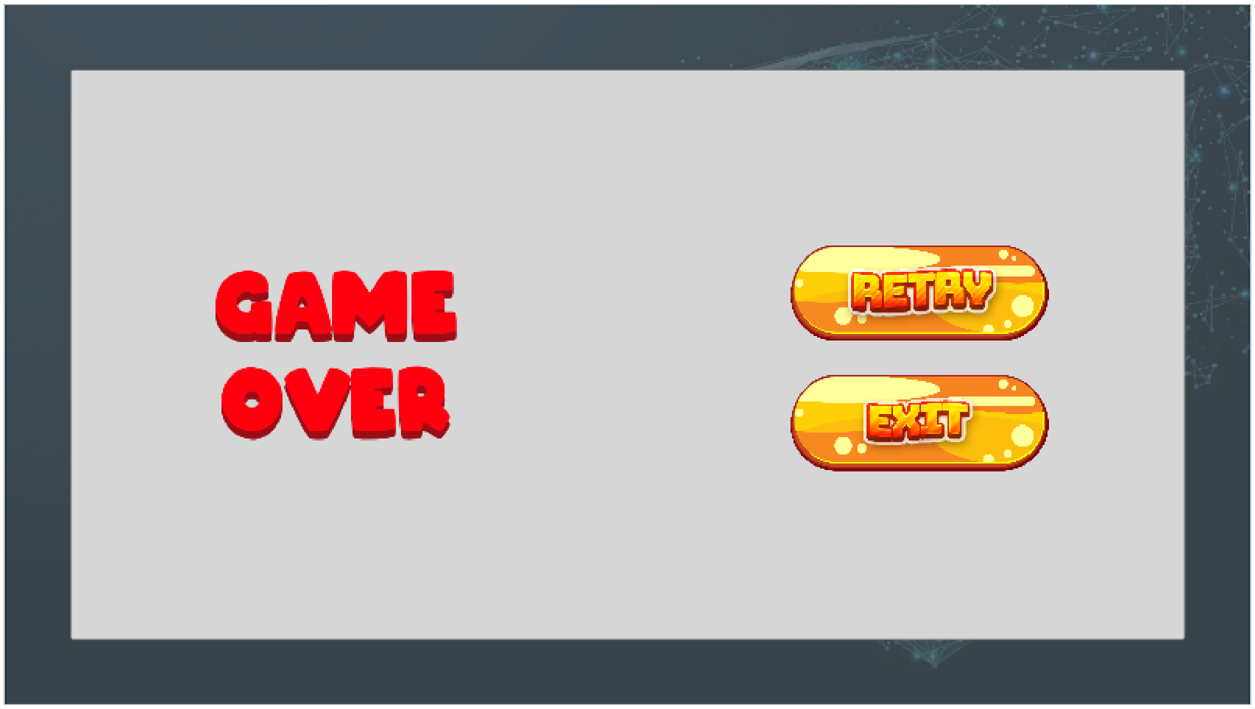
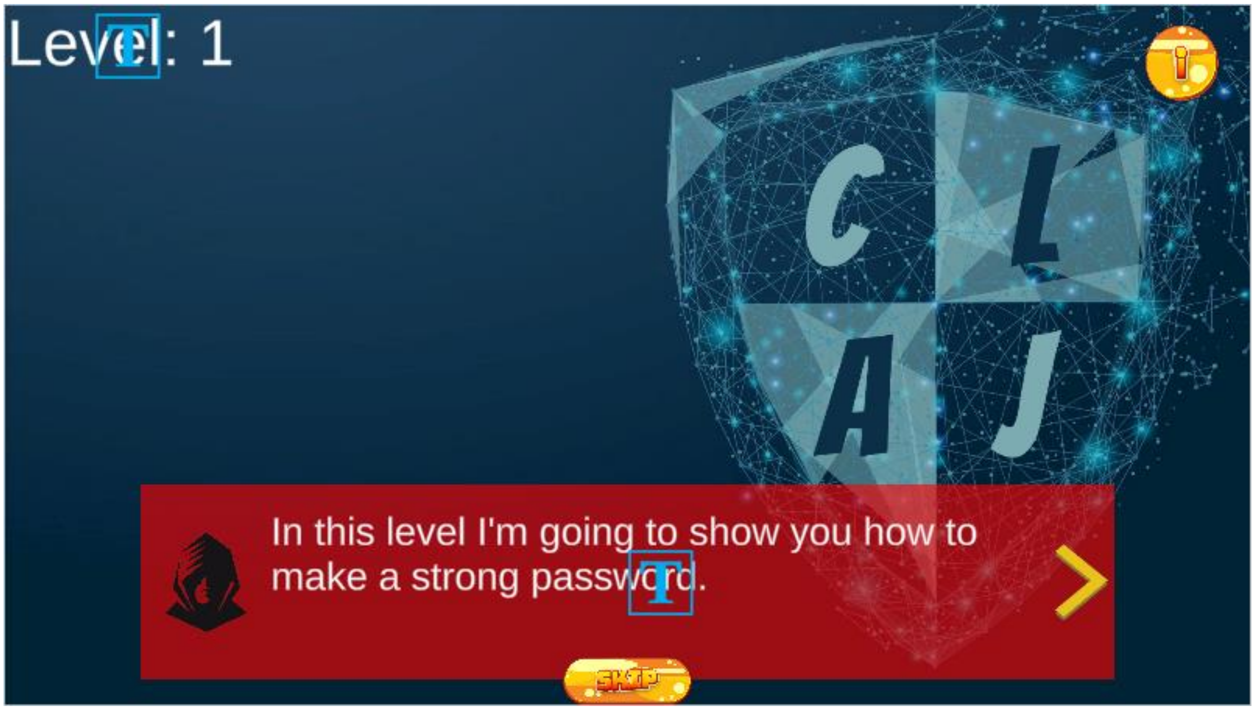


Figure 9- Screen in case you lose, Prototype

4.7- Instructions

This screen will display instructions consecutively to the kid, so he knows the conditions of the password he is going to enter.



In this level I'm going to show you how to make a strong password.

Figure 10 – Instructions screen, Prototype

4.8- Password Level

This screen displays the password game where the kid will enter the passwords based on the instructions displayed in the previous screen.

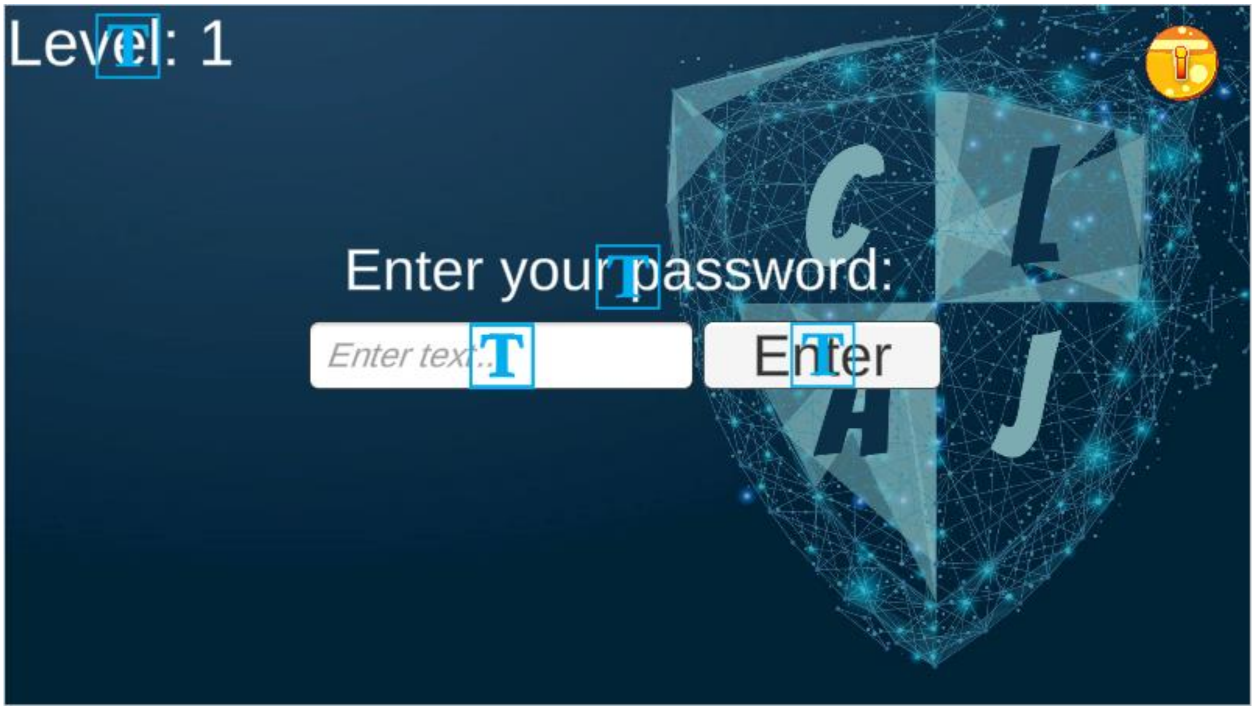
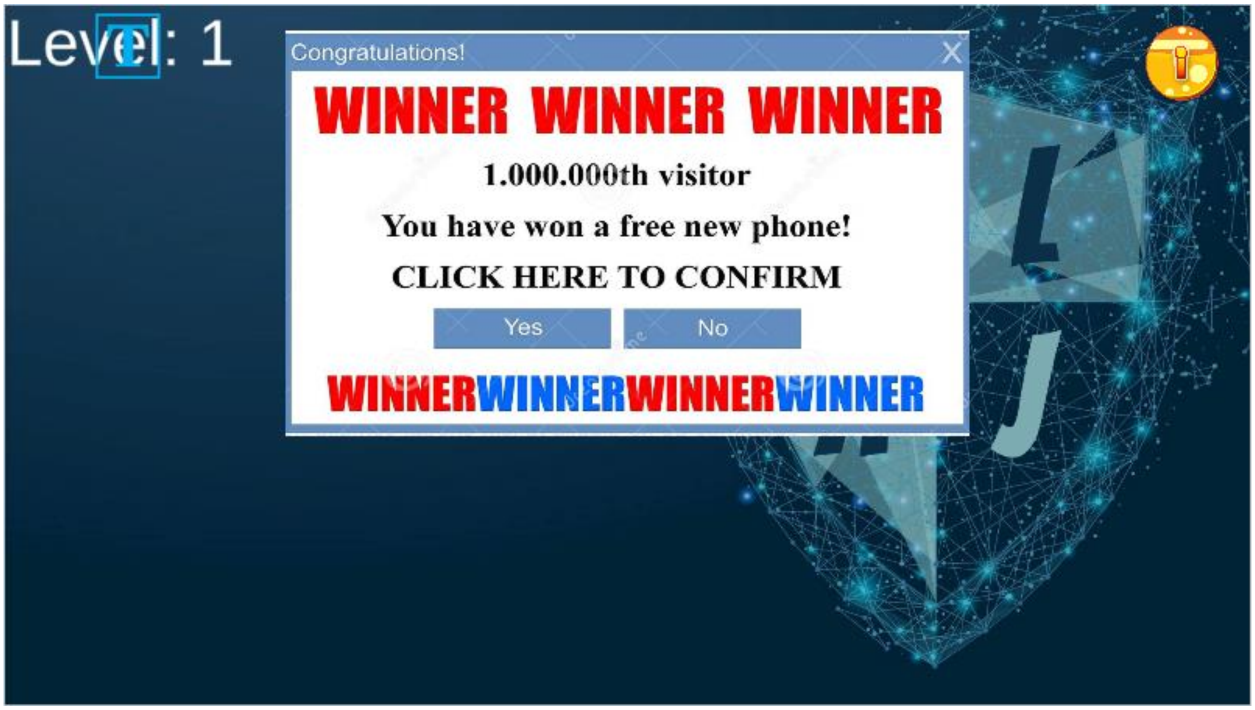


Figure 11- Screen after knowing the instructions to start playing, Prototype

4.9 - Scam v1.0

This screen shows fake advertisements to test the kid whether he will be deceived or will know that it is a scam.



WINNER WINNER WINNER

1.000.000th visitor

You have won a free new phone!

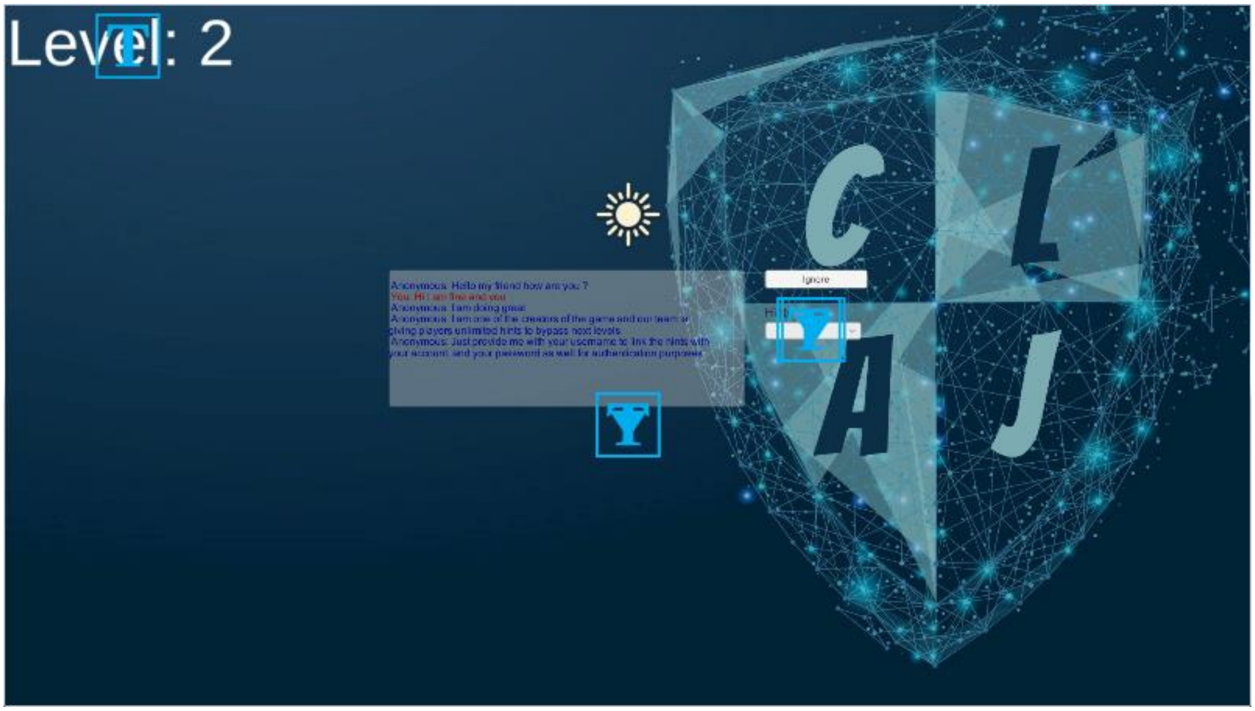
CLICK HERE TO CONFIRM

WINNERWINNERWINNERWINNER

Figure 12- Scam screen, Prototype Level: 1

5.0 - Scam v2.0

This is also a screen that shows scam but in game 2.



Anonymous: Hello my friend how are you ?
You: Hi I am fine and you
Anonymous: I am doing great
Anonymous: I am one of the creators of the game and our team is giving players unlimited hints to bypass next levels
Anonymous: Just provide me with your username to link the hints with your account and your password as well for authentication purposes

Figure 13- Scam screen, Prototype Level:2

5.1- Final Game Level 1

This is the start screen of level 1 in final game, it shows the health bar not full because no password entered yet. The character in pink is a friend who will help through the whole game and will teach you how to enter strong password to have full health bar.

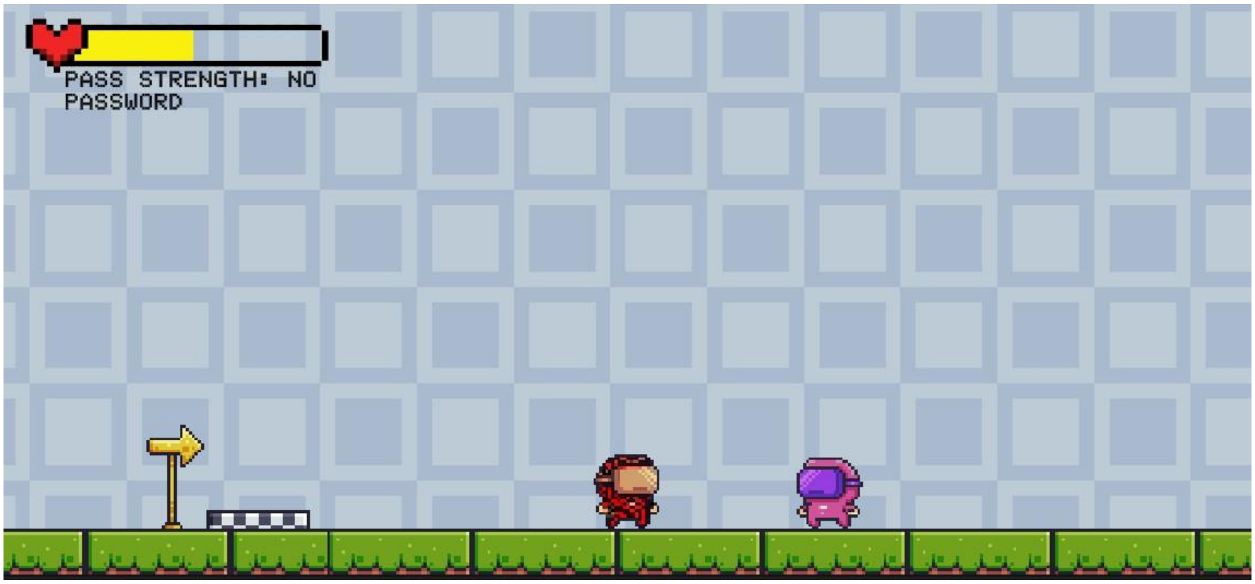


Figure 14 – Start Screen Final Game Level 1

5.2 – Password screen

This is the screen where you enter your first password in level 1 of final game.

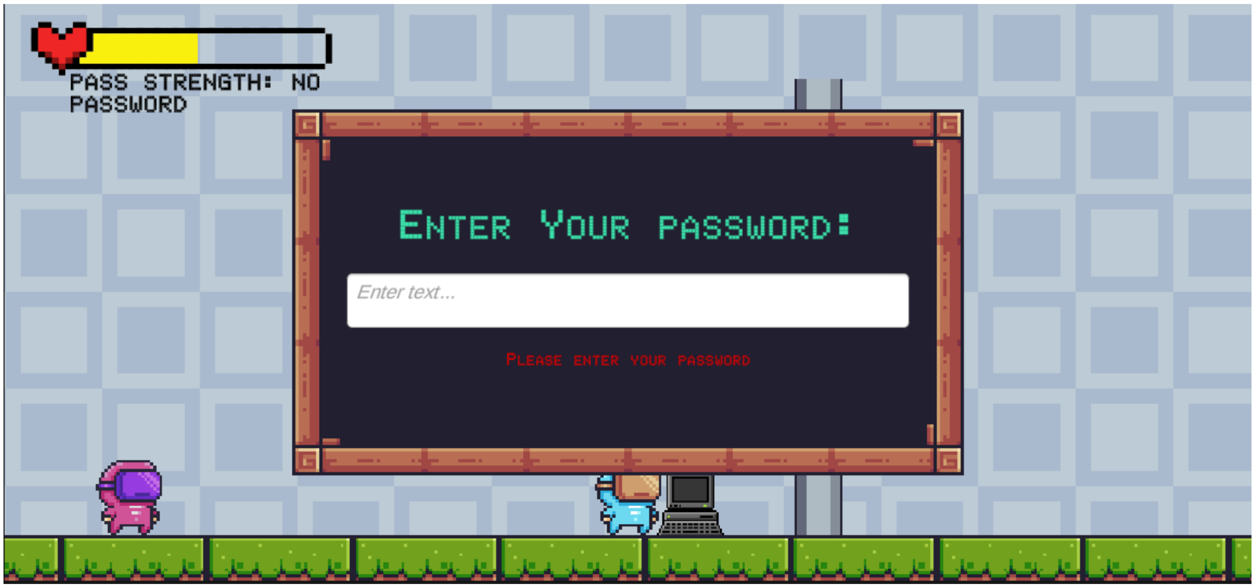


Figure 15 – Initial password screen

5.3 – Elevator levels

This screen contains an elevator which the character rides to pass through three levels where he learns new things about passwords, the last level is the boss level, and it will not open until you finish the first three levels.

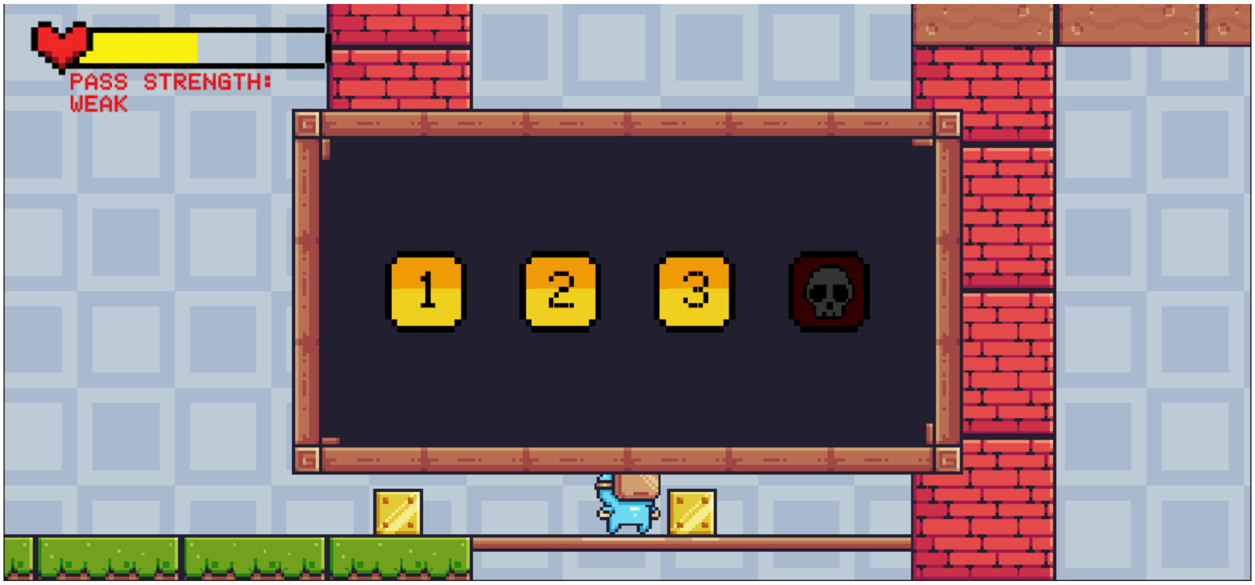
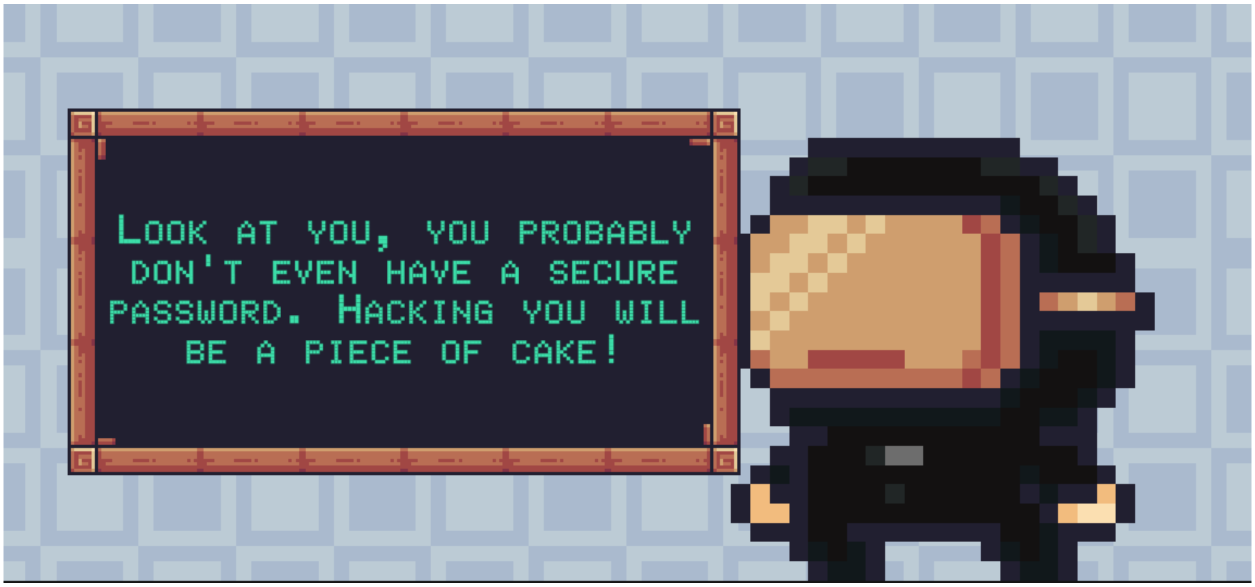


Figure 16 – Elevator screen Final Game Level 1

5.4 – Hacker

After you pass the three levels you will be able to face the hacker who will challenge you and try to get your password.

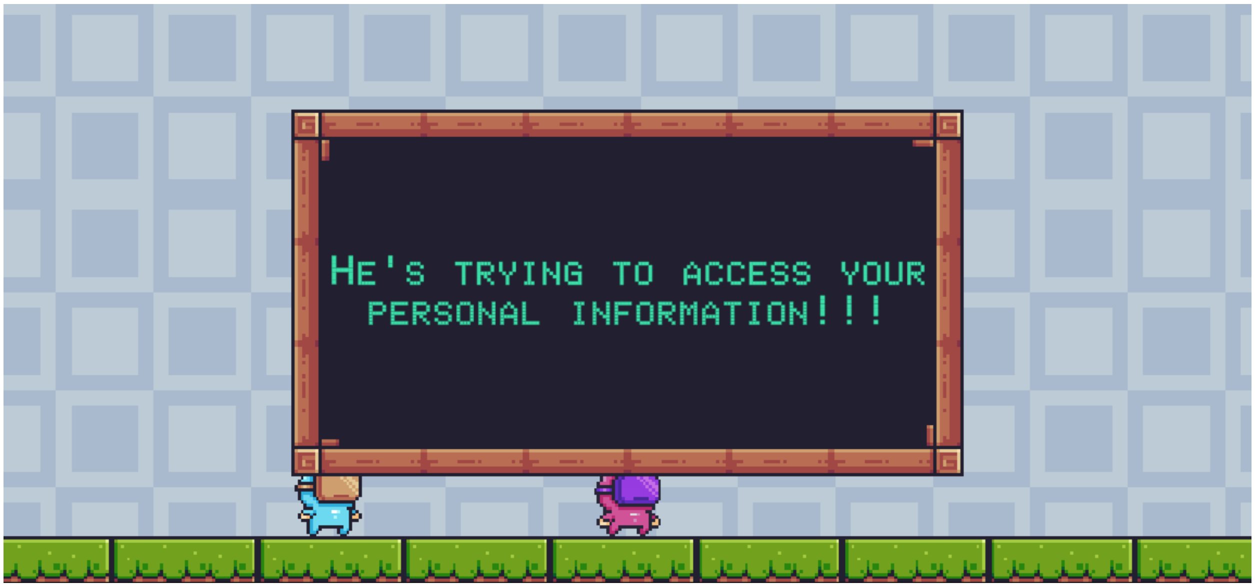


Look at you, you probably don't even have a secure password. Hacking you will be a piece of cake!

Figure 17 – Facing the hacker Final Game Level 1

5.5 – Instructions

In this screen your friend will warn you that the hacker is trying to get your personal information and password so you can be ready.

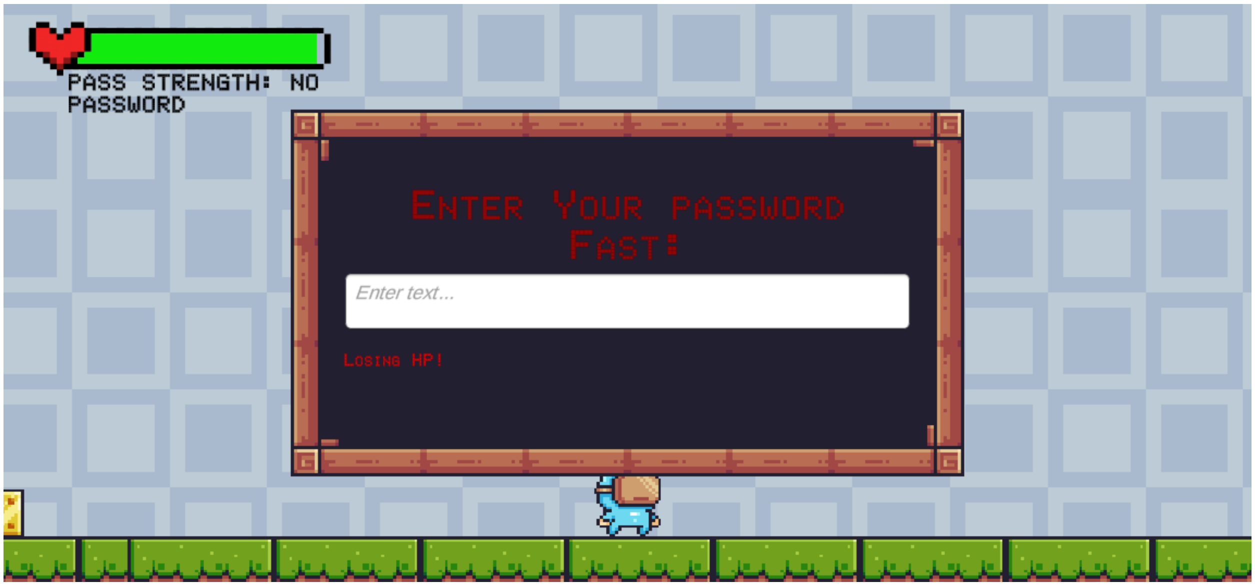


HE'S TRYING TO ACCESS YOUR PERSONAL INFORMATION!!!

Figure 18 – Instructions by friend Final Game Level 1

5.6 – Challenging the hacker

In this screen, you should enter your password as fast as you could before your health finished and by time the health decreases.



PASS STRENGTH: NO PASSWORD

ENTER YOUR PASSWORD FAST:

Enter text...

LOSING HP!

Figure 19 – Facing the hacker Final Game Level 1

5.7 – Final Game Level 2

This is the start screen of level 2 in final game where the hacker acts as your friend and try to get your password.

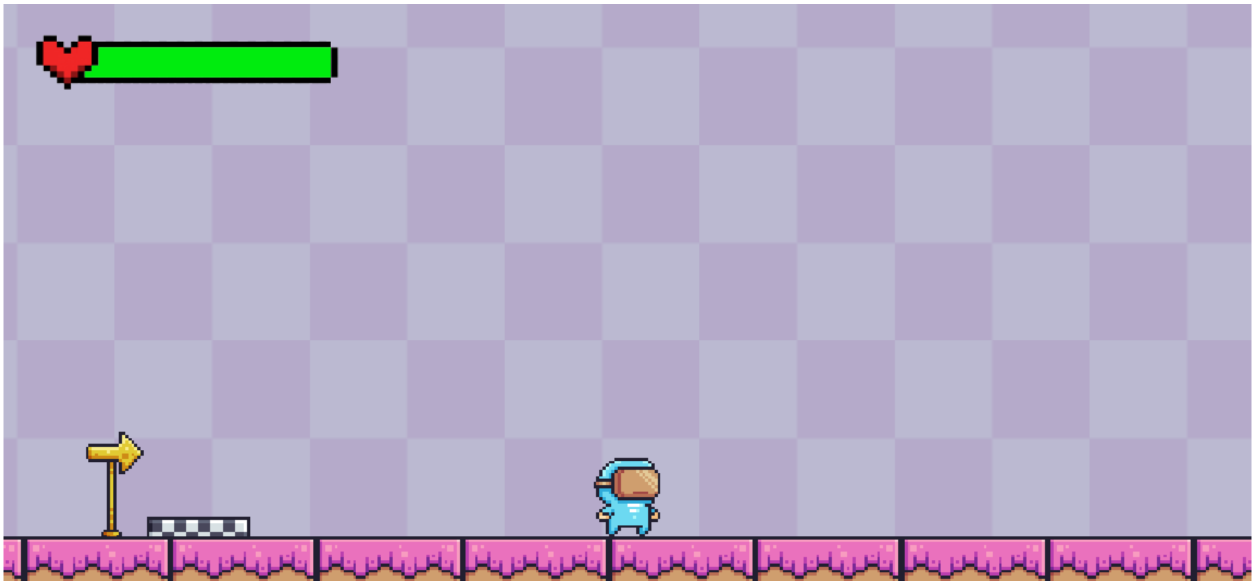
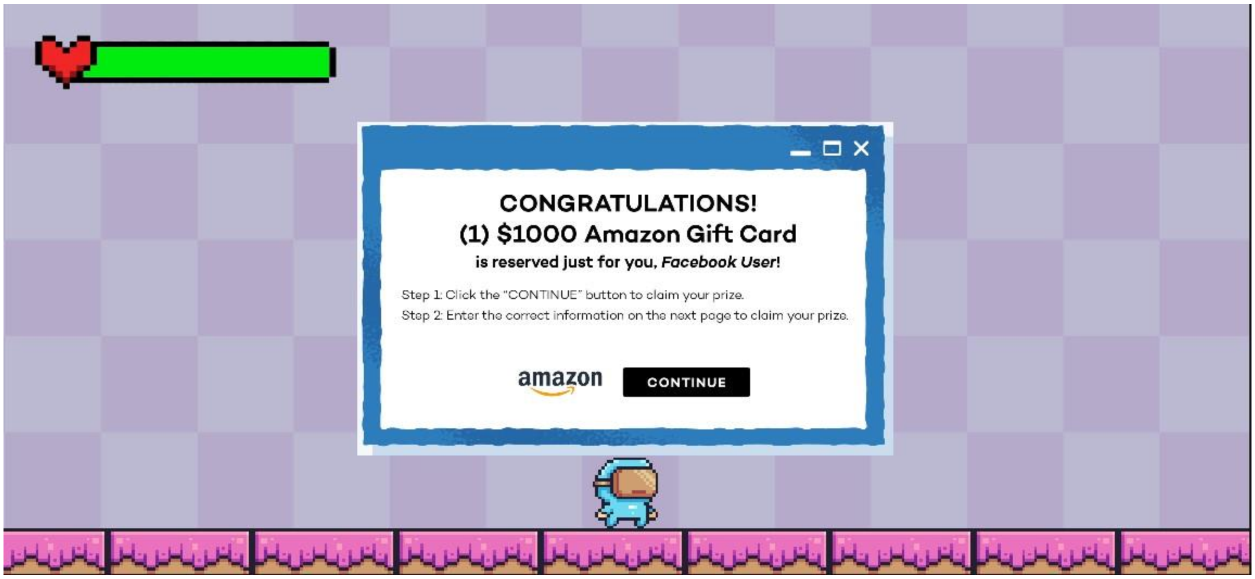


Figure 20 – Start screen final game level 2

5.8 – Scam

This is fake advertisement if the player clicked on continue his health will decrease, if he clicked on X he will pass.



CONGRATULATIONS!

(1) $1000 Amazon Gift Card

is reserved just for you, *Facebook User*!

Step 1: Click the "CONTINUE" button to claim your prize.

Step 2: Enter the correct information on the next page to claim your prize.

Figure 21 – Scam Screen Final game level 2

5.9 – Password

In this screen you will enter your password and the hacker will get it.

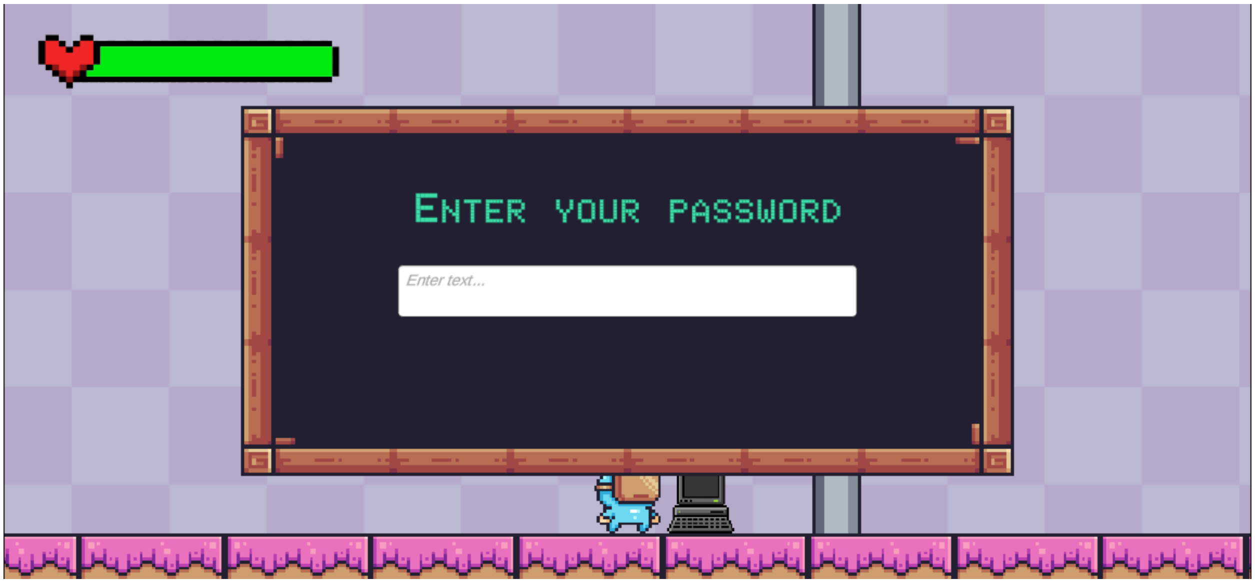

ENTER YOUR PASSWORD

Figure 22 – Enter your password Final game level 2

6.0 – You got hacked

You realize you got hacked and the hacker currently knows your password.

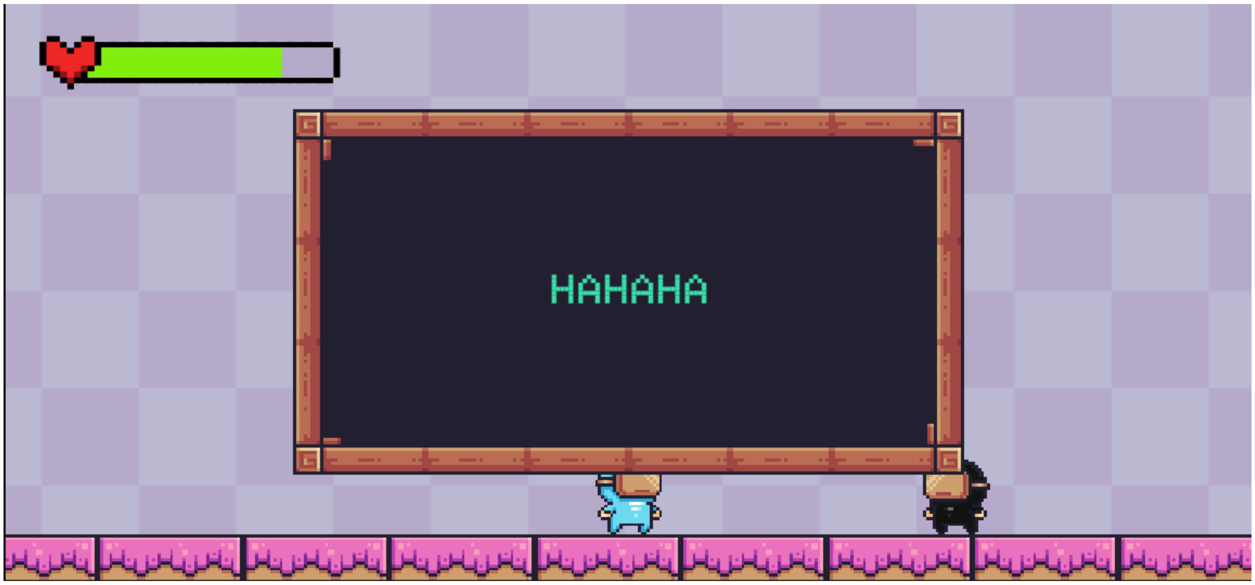

HAHAHA

Figure 23 – Hacker reaction to getting your password Final game level 2

6.1 – New Password v1.0

In this screen, your friend is advising you to creae new password after the hacker knew the old password.

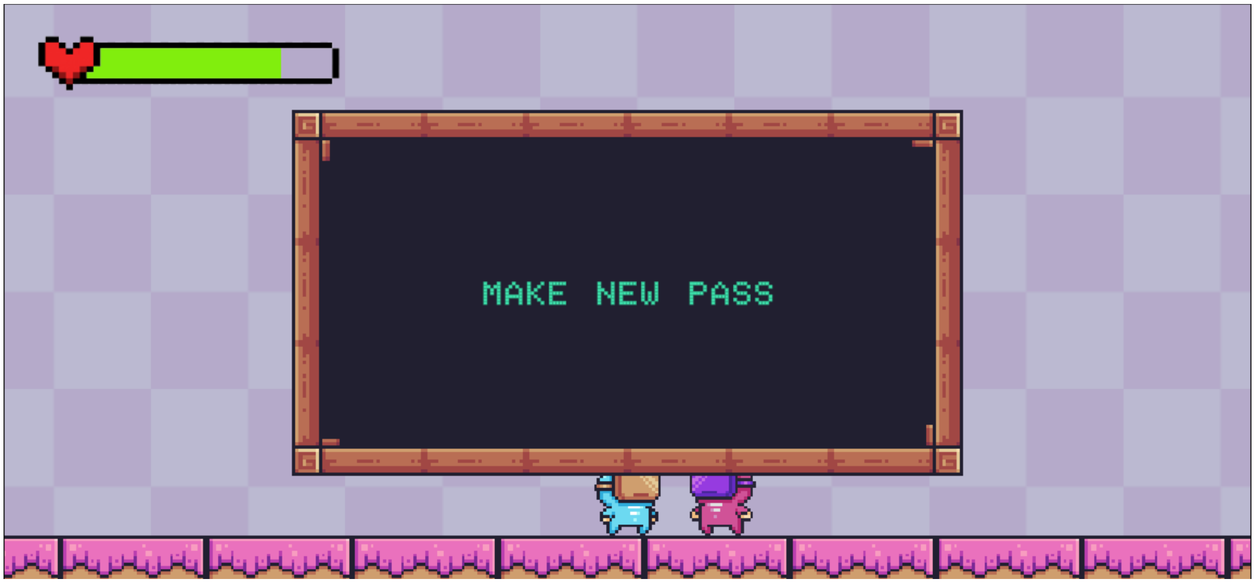
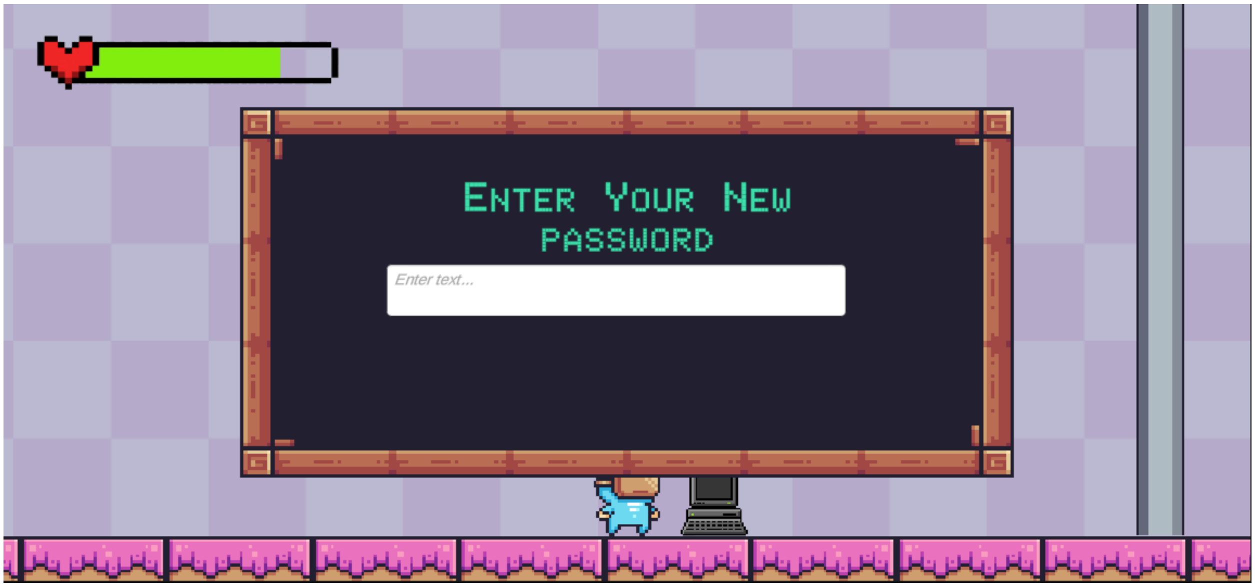


Figure 24 – Creating new password Final game level 2

6.2 – New Password v2.0

This is the screen where you enter your new password.



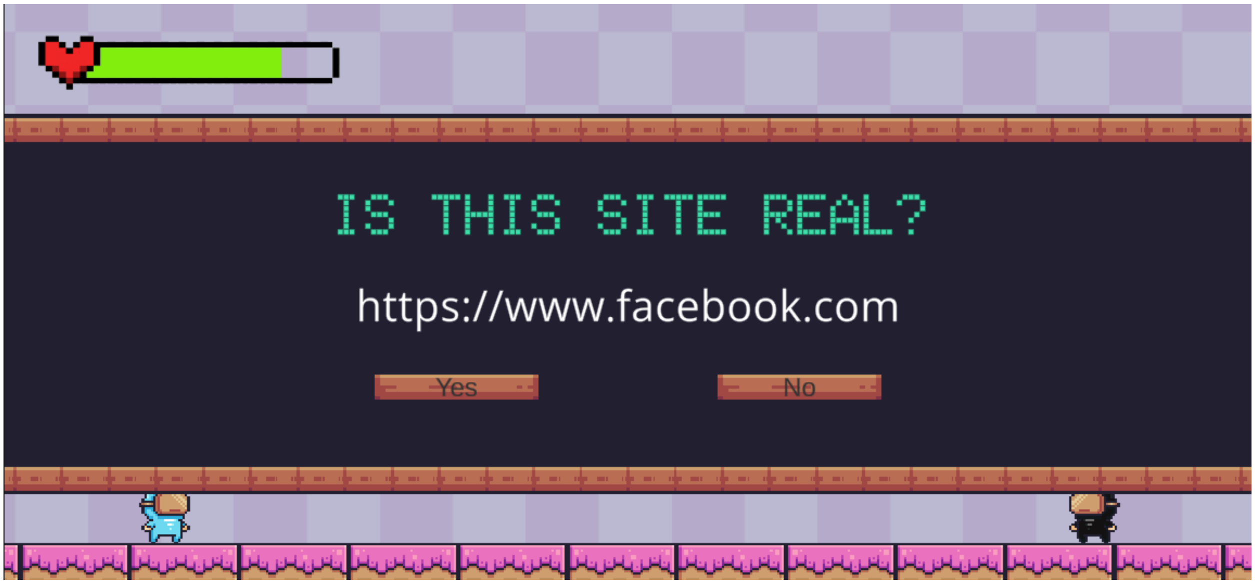
ENTER YOUR NEW PASSWORD

Enter text...

Figure 25 – Entering new password Final game level 2

6.3 Final boss fight

In this screen, you will be shown links and decide which one is correct and which is malicious, based on this your health will decrease or not.



IS THIS SITE REAL?

https://www.facebook.com

Figure 26 – Links test Final game level 2

6.4 – Final Game level 3

Level 3 starts by meeting anonymous person who will try to act as a friend to get your personal information.

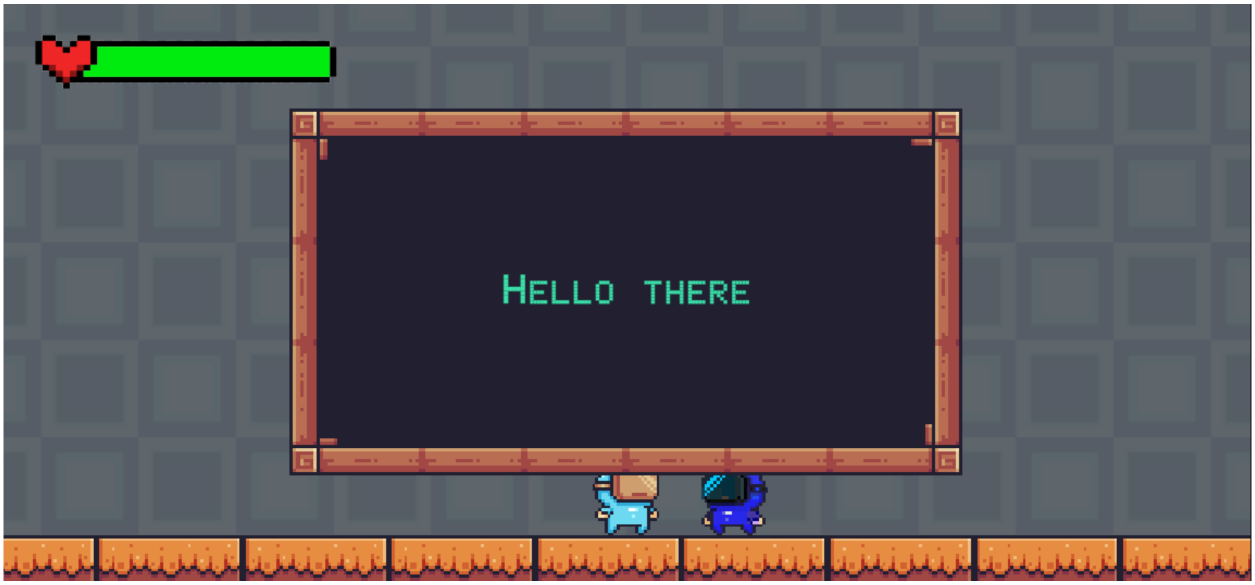

HELLO THERE

Figure 27 – Meeting anonymous person Final game level 3

6.5 – Pin Code v1.0

You need to enter the pin code to pass through the gate.

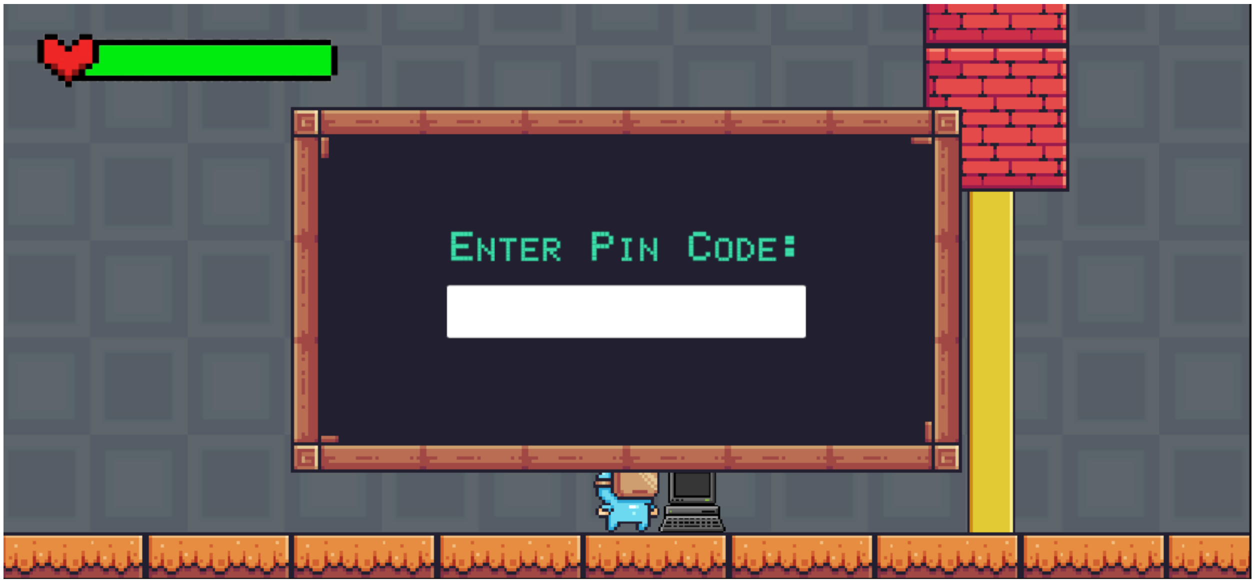
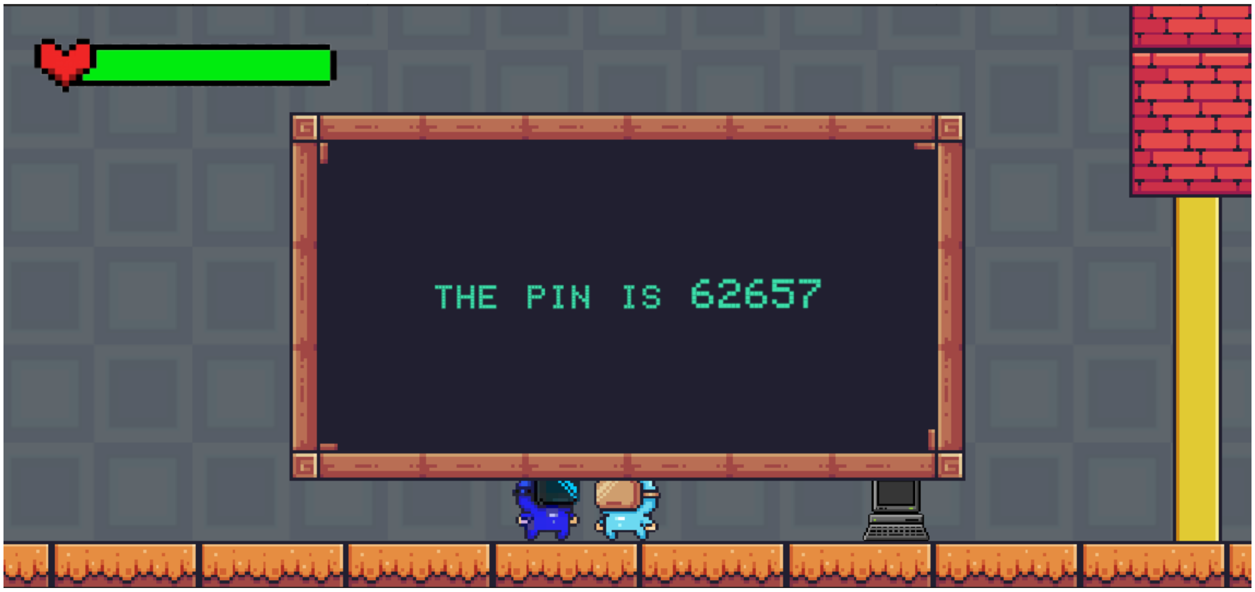

ENTER PIN CODE:

Figure 28 – Enter Pin code Final game level 3

6.6 – Pin code v2.0

The anonymous person will give you the pin code to pass through the gate.

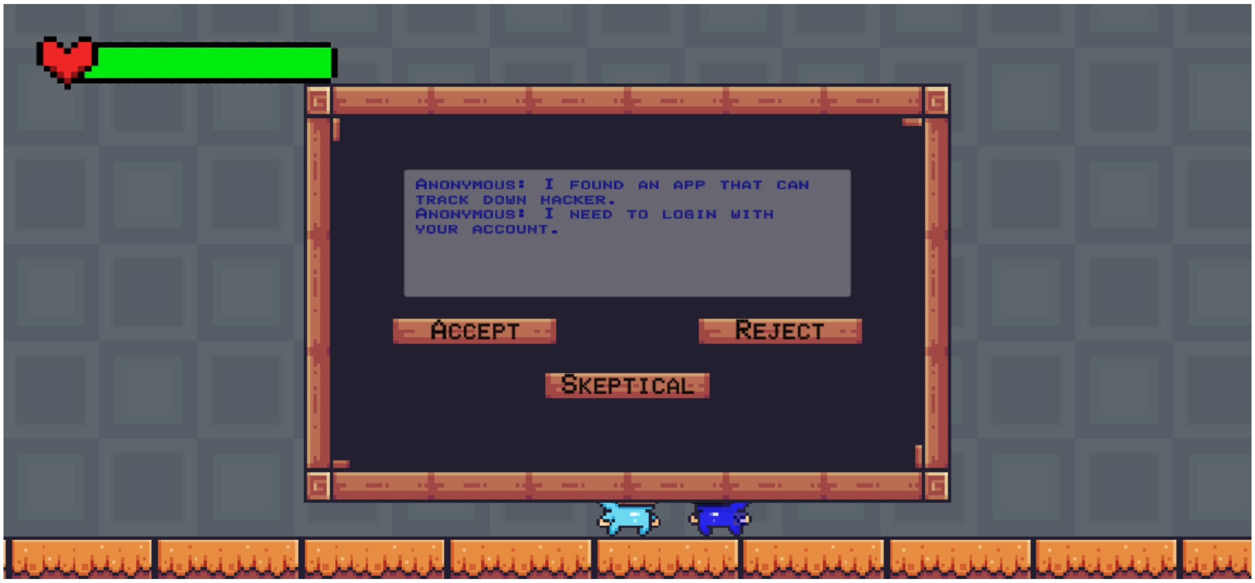


THE PIN IS 62657

Figure 29 – Pin Code Final game level 3

6.7 – Hacker Tracker v1.0

In this screen, a conversation between the player and the anonymous person where he offers a hacker tracker application but he needs your login information.

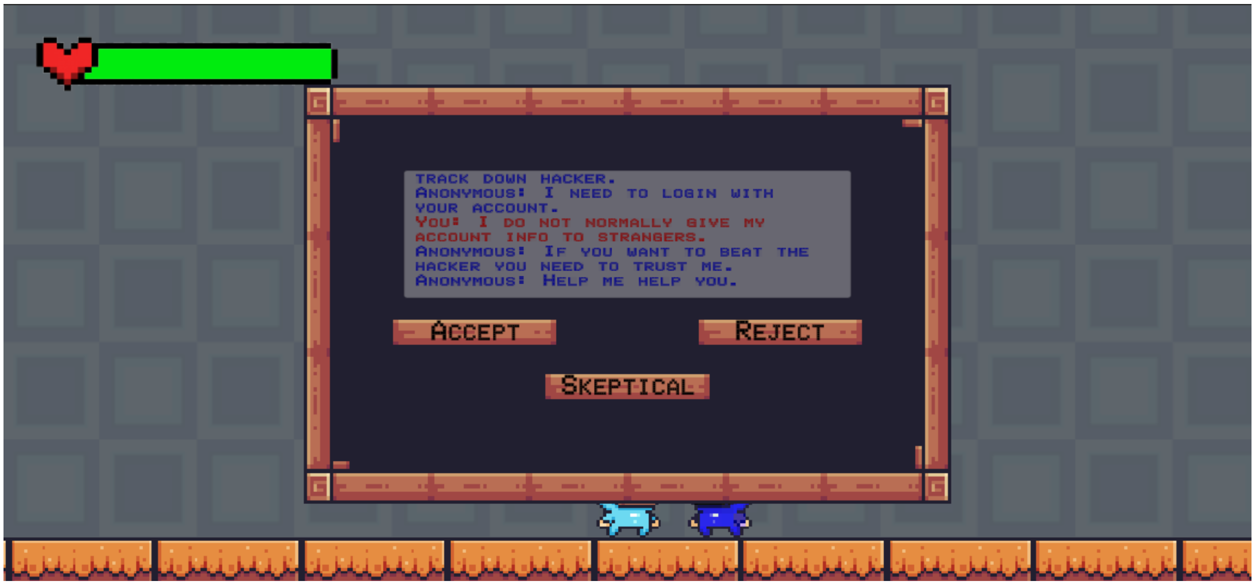


ANONYMOUS: I FOUND AN APP THAT CAN TRACK DOWN HACKER.
ANONYMOUS: I NEED TO LOGIN WITH YOUR ACCOUNT.

Figure 30 – Chatbot Final game level 3

6.8 – Hacker Tracker v2.0

In this screen, you have three choices to reply with on the anonymous person, if you reject he will try once again to convince you, if you choose skeptical you are trying to know why he needs your account information and if you accept another screen will be shown to enter your data.



TRACK DOWN HACKER.
ANONYMOUS: I NEED TO LOGIN WITH YOUR ACCOUNT.
YOU: I DO NOT NORMALLY GIVE MY ACCOUNT INFO TO STRANGERS.
ANONYMOUS: IF YOU WANT TO BEAT THE HACKER YOU NEED TO TRUST ME.
ANONYMOUS: HELP ME HELP YOU.

Figure 31 – Reply options Final Game level 3

6.9 – Login information

If you accept, this screen will open so you can enter your login information. Then your health will be 0 and you will lose.

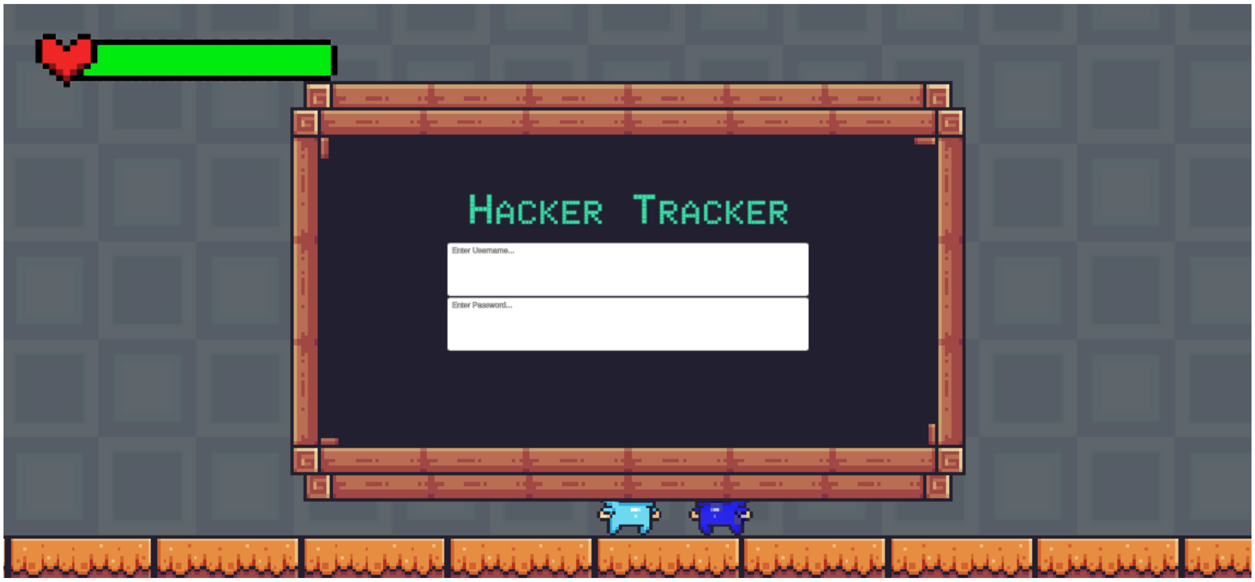
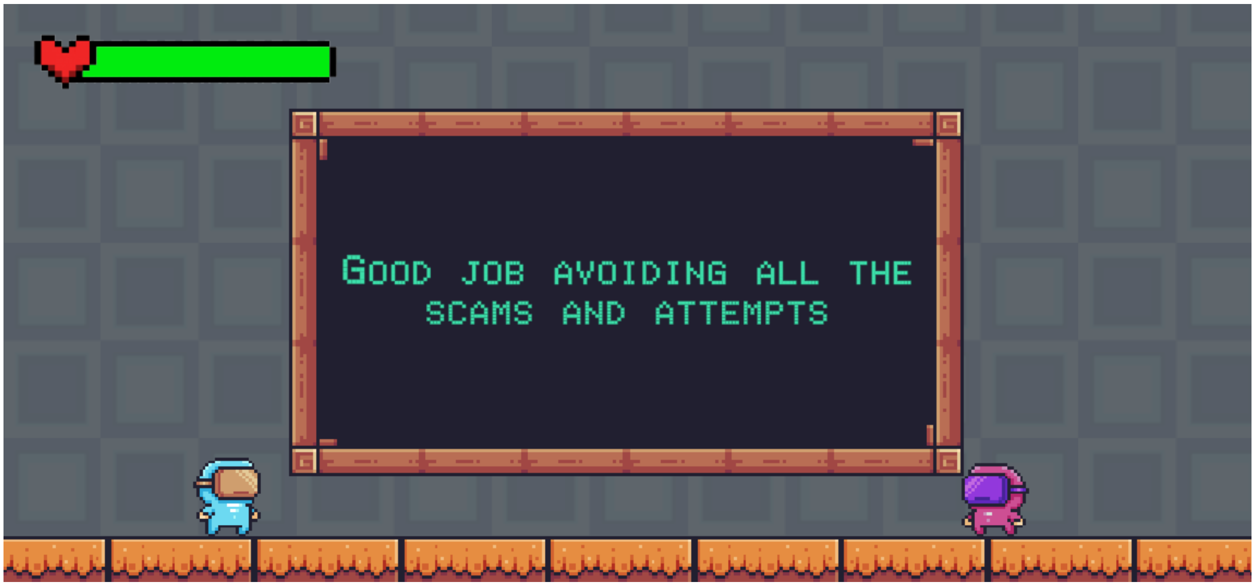


Figure 32 – Screen after acceptance Final Game level 3

7.0 – Good Job

If you insisted and rejected even after he tried to convince you, your friend will greet you.



Good job avoiding all the scams and attempts

Figure 33 – Screen after rejection Final Game level 3

7.1 – Skins

This skins are implemented as a rewarding system to motivate the players. As the players progress in the game they can unlock more skins according to different requirements.

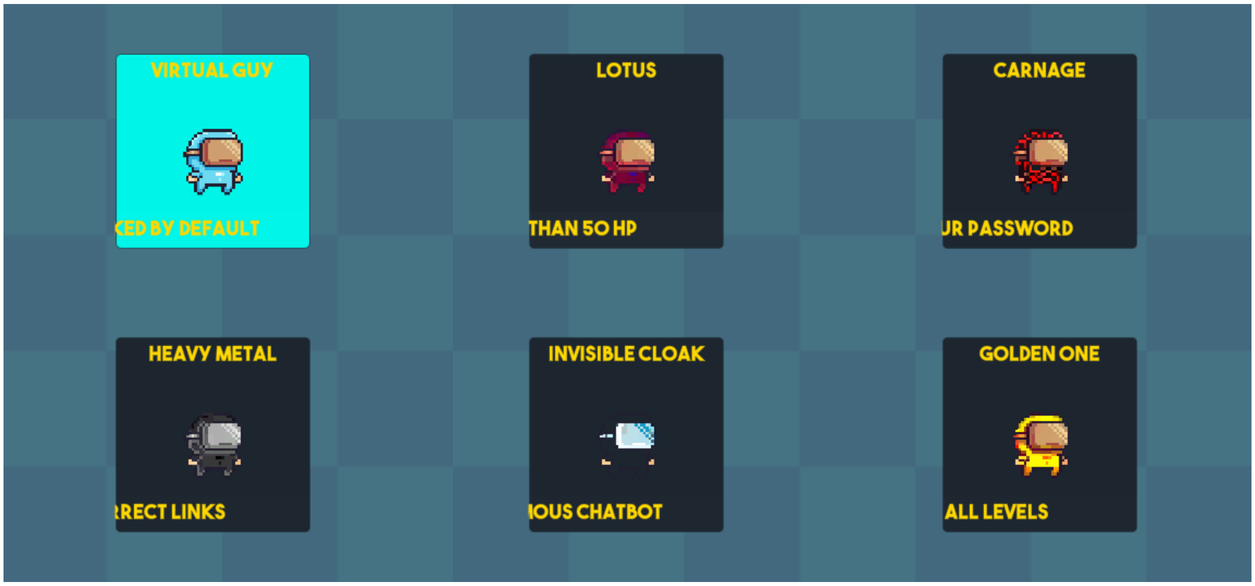


Figure 34 – Skins of the player

5- Conclusion and Future Work

5.1 Conclusion

Today, internet became an essential part of everyone’s life and it can not be replaced because its huge benefits regarding education for example. It is clear that the dependance on internet increased enormously after covid-19 outbreak and everyone regardless their ages use it in their studies, work, etc. This highlights the importance of awareness while using the internet to be able to deal with any threat that appears online. Luckily, there are many resources that offers large amount of information about dealing with internet. However, the majority of these resources are directed to the adults and provide the information in a complicated way that does not suit every age group.

Our application works on solving this problem by offering information about the most common threats any one can face online and how to handle them in a simple way that can be fully understood by the kids. The application trains the kids on how to create strong passwords so they can protect their personal information. Moreover, kids will learn how to differentiate between malicious and valid links or advertisements to prevent being scammed online. While chatting, the kid will learn how to detect if the other person is acting suspicious and will know whether to trust him or not with their personal information. This education comes with a gamified and enjoyable experience so the kid will not feel bored and will like to spend a lot of time playing the game with his own willingness.

5.2 Future Work

We aim to implement more levels in the game to increase the difficulty to appeal to players with different skill levels. Each level may present new concepts and challenges to keep a player's interest high and to make it more useful by increasing the educational benefits the kids can get while playing the game.

We are working on improving the gamification to make the game more enjoyable and attractive for the kids, so they spend more time playing without feeling bored. Better gamification means that the game will be more likeable by the kids, and they will surely get maximum benefit from it.

Leader boards rank players according to their relative success, measuring them against a certain criterion. As a result, leader boards can be used to identify the best performers of a certain activity. Ultimately, they can be used as a competitive indicator of progress, relating the player’s own performance to the performance of others. So, we are planning to create leader board to motivate the kids to spend more time playing the game.

Added to the attacks already mentioned in the game, it is important to add more attacks like man-in-the-middle, pharming, cyber stalking, etc, to expand their information and to get them ready to deal with any attack that they might face.

References

- [1] "Screen time 'may harm toddlers'", BBC News, 2019. [Online]. Available: https://www.bbc.com/news/health-47026834. [Accessed: 06- Dec- 2021].
- [2] "Cybersecurity in Education: What Teachers, Parents and Students Should Know | Berkeley Boot Camps", Berkeley Boot Camps, 2021. [Online]. Available: https://bootcamp.berkeley.edu/blog/cybersecurity-in-education-what-teachers-parents-and-students-should-know/. [Accessed: 06- Dec- 2021].
- [3] Kaspersky, "Kaspersky," Kaspersky, [Online]. Available: https://usa.kaspersky.com/resource-center/threats/top-seven-dangers-children-face-online. [Accessed 08 November 2021].
- [4] J. Johnson, "Statista," 06 May 2021. [Online]. Available: https://www.statista.com/statistics/1189204/us-teens-children-screen-time-daily-coronavirus-before-during/. [Accessed 08 November 2021].
- [5] DQ Institute, "DQ Institute," DQ Institute, [Online]. Available: https://www.dqinstitute.org/child-online-safety-index/. [Accessed 08 November 2021].
- [6] G. Kiryakova, N. Angelova and L. Yordanova, "GAMIFICATION IN EDUCATION," in 9th International Balkan Education and Science Conference, Edirne, 2014.
- [7] "Cybertalentskids » CyberTalents", CybertalentKids, 2021. [Online]. Available: https://cybertalentskids.com/. [Accessed: 06- Dec- 2021].
- [8] "Cybersmart Challenge", 2021. [Online]. Available: https://www.esafety.gov.au/educators/classroom-resources/cybersmart-challenge. [Accessed: 06- Dec- 2021].

- [9] "Hacking Training For The Best", Hack The Box, 2021. [Online]. Available: https://www.hackthebox.com/. [Accessed: 06- Dec- 2021].
- [10] "OWASP Foundation | Open Source Foundation for Application Security", Owasp.org, 2021. [Online]. Available: https://owasp.org/.
- [11] C. Li, "Weforum," World Economic Forum, 29 April 2020. [Online]. Available: https://www.weforum.org/agenda/2020/04/coronavirus-education-global-covid19-online-digital-learning/. [Accessed 08 November 2021].
- [12] H. M. Jawad and S. Tout, "Introducing a Mobile App to Increase Cybersecurity Awareness in MENA," 2020 3rd International Conference on Signal Processing and Information Security (ICSPIS), 2020, pp. 1-4, doi: 10.1109/ICSPIS51252.2020.9340128. [Accessed: 06- Dec- 2021].
- [13] C. Davin, "Password requirements - GDPR, ISO 27001/27002, PCI DSS, NIST 800-53," Davin Tech Group | The Toolkit, 26-Feb-2020. [Online]. Available: https://davintechgroup.com/toolkit/password-requirements-gdpr-iso-27001-27002-pci-dss-nist-800-53/. [Accessed: 06-Dec- 2021].
- [14] S. Gordon, "Phishing and online scams: What your kids need to know," Verywell Family, 05-May-2022. [Online]. Available: https://www.verywellfamily.com/teach-kids-about-phishing-and-online-scams-5248479. [Accessed: 16-Nov-2021].
- [15] K. Brush and J. Scardina, "What is a chatbot and why is it important?," SearchCustomerExperience, 18-Nov-2021. [Online]. Available: https://www.techtarget.com/searchcustomerexperience/definition/chatbot. [Accessed: 08-Dec-2021].