Gamified Design for Creating Strong Passwords

Target Group: 8 – 11-year olds

Course: F20AD Advanced Human Interaction Design

Group 11:

Aarthi Raju – ar2014@hw.ac.uk - H00354041

Shravan Sankar Narayanan -ss2034@hw.ac.uk - H00352627

Soham Kakra – sk2015@hw.ac.uk - H00360439

Varun Senthil – vs55@hw.ac.uk – H00332328

Link to prototype:

https://www.figma.com/file/xhmoMVdpuS2mXo3TXDRo4c/Game-of-Password-Security-Awareness?node-id=0%3A1&t=OJKIyKONEeDmLeYb-1

Student Declaration of Authorship

HERIOT WATT UNIVERSITY
UK | DUBAI | MALAYSIA

Course code and name:	F20AD – Advanced Human Computer Interaction
Type of assessment:	**Group**
Coursework Title:	Coursework A
Student Name:	Varun Senthil Kumar
Student ID Number:	H00332328

Declaration of authorship. By signing this form:

- **I declare** that the work I have submitted for individual assessment OR the work I have contributed to a group assessment, is entirely my own. I have NOT taken the ideas, writings or inventions of another person and used these as if they were my own. My submission or my contribution to a group submission is expressed in my own words. Any uses made within this work of the ideas, writings or inventions of others, or of any existing sources of information (books, journals, websites, etc.) are properly acknowledged and listed in the references and/or acknowledgements section.

- I confirm that I have read, understood and followed the University's Regulations on plagiarism as published on the University's website, and that I am aware of the penalties that I will face should I not adhere to the University Regulations.

- I confirm that I have read, understood and avoided the different types of plagiarism explained in the University guidance on Academic Integrity and Plagiarism

Student Signature *(type your name):* *Varun Senthil Kumar*

Date: *06/03/2023*

Student Declaration of Authorship

HERIOT WATT UNIVERSITY
UK | DUBAI | MALAYSIA

Course code and name:	F20AD – Advanced Human Computer Interaction
Type of assessment:	**Group**
Coursework Title:	Coursework A
Student Name:	Aarathi Raju
Student ID Number:	H00354041

Declaration of authorship. By signing this form:

- **I declare** that the work I have submitted for individual assessment OR the work I have contributed to a group assessment, is entirely my own. I have NOT taken the ideas, writings or inventions of another person and used these as if they were my own. My submission or my contribution to a group submission is expressed in my own words. Any uses made within this work of the ideas, writings or inventions of others, or of any existing sources of information (books, journals, websites, etc.) are properly acknowledged and listed in the references and/or acknowledgements section.

- I confirm that I have read, understood and followed the University's Regulations on plagiarism as published on the University's website, and that I am aware of the penalties that I will face should I not adhere to the University Regulations.

- I confirm that I have read, understood and avoided the different types of plagiarism explained in the University guidance on Academic Integrity and Plagiarism

Student Signature *(type your name):* *Aarathi Raju*

Date: *06/03/2023*

Student Declaration of Authorship

HERIOT WATT UNIVERSITY
UK | DUBAI | MALAYSIA

Course code and name:	F20AD – Advanced Human Computer Interaction
Type of assessment:	**Group**
Coursework Title:	Coursework A
Student Name:	Soham Kakra
Student ID Number:	H00360439

Declaration of authorship. By signing this form:

- **I declare** that the work I have submitted for individual assessment OR the work I have contributed to a group assessment, is entirely my own. I have NOT taken the ideas, writings or inventions of another person and used these as if they were my own. My submission or my contribution to a group submission is expressed in my own words. Any uses made within this work of the ideas, writings or inventions of others, or of any existing sources of information (books, journals, websites, etc.) are properly acknowledged and listed in the references and/or acknowledgements section.

- I confirm that I have read, understood and followed the University's Regulations on plagiarism as published on the University's website, and that I am aware of the penalties that I will face should I not adhere to the University Regulations.

- I confirm that I have read, understood and avoided the different types of plagiarism explained in the University guidance on Academic Integrity and Plagiarism

Student Signature *(type your name):* *Soham Kakra*

Date: *06/03/2023*

Student Declaration of Authorship

HERIOT WATT UNIVERSITY
UK | DUBAI | MALAYSIA

Course code and name:	F20AD – Advanced Human Computer Interaction
Type of assessment:	**Group**
Coursework Title:	Coursework A
Student Name:	Shravan Sankar Narayanan
Student ID Number:	H00352627

Declaration of authorship. By signing this form:

- **I declare** that the work I have submitted for individual assessment OR the work I have contributed to a group assessment, is entirely my own. I have NOT taken the ideas, writings or inventions of another person and used these as if they were my own. My submission or my contribution to a group submission is expressed in my own words. Any uses made within this work of the ideas, writings or inventions of others, or of any existing sources of information (books, journals, websites, etc.) are properly acknowledged and listed in the references and/or acknowledgements section.

- I confirm that I have read, understood and followed the University's Regulations on plagiarism as published on the University's website, and that I am aware of the penalties that I will face should I not adhere to the University Regulations.

- I confirm that I have read, understood and avoided the different types of plagiarism explained in the University guidance on Academic Integrity and Plagiarism

Student Signature *(type your name):* *Shravan Sankar Narayanan*

Date: *06/03/2023*

Table of Contents

1. Introduction

The significance of password security cannot be emphasized in today's environment where digital gadgets and online activities are an essential part of our everyday lives. Nevertheless, young children frequently do not completely understand the dangers of using weak passwords or the need of using strong passwords. This problem can be solved by using a gamified method to make the learning experience more interesting and fun. The goal of this strategy is to assist young youngsters between the ages of 8 and 11 in comprehending the significance of password security. To accommodate various learning styles and to offer a more immersive experience, the method uses at least three separate modalities, including voice.

As passwords are still the main form of authentication for accessing numerous services, it is critical to always keep users' online security in mind. There are numerous ways people can put themselves in danger while exploring the web. This can include using websites with bad coding, coming up with flimsy passwords, and downloading information from websites that have harmful files.

In the 21st century, people are highly reliant on the internet for performing a variety of tasks. For e.g., Banking, E-commerce, Socializing, etc. The internet is used for a variety of purposes. And due to this, an individual knowingly or unknowingly uploads a lot of personal information onto the web. This can pose a lot of risks and issues if the information is not protected or secured. The widely adopted method in order protect a user's personal information from unauthorized access, is by using authentication methods. This authentication is what we popularly call 'Password.'

Even though passwords are the primary authentication method widely used, it has its own limitations. One of the biggest usability issues is how hard it is to enter passwords using virtual keyboards. Additionally, users often adopt less secure habits like using the same password for many accounts and selecting passwords that are less complicated and straightforward for a hacker to obtain.

Despite all these, adults are quite mature enough or have an idea of how to keep themselves away from most cybercrimes or bullies. Most adults keep all their information, password protected. But the internet and the web is not only available and used by adults. Kids from a very young age are exposed to the web and the internet. They have access to all kinds of content. They visit all kinds of apps.

2. Requirements Analysis

In this section will look at the functional and non-functional requirements to proceed with this project. For the prioritization of the requirement, we have used the MoSCoW method to be able to keep track of the progress.

2.1 MoSCoW Method

The Moscow prioritization method is a prioritization technique used in requirements analysis to prioritize and classify user requirements.

- "Must have" requirements are considered essential to the success of the project and are non-negotiable. These requirements must be met in order for the project to be considered complete.
- "Should have" requirements are considered important, but not as critical as "Must have" requirements. These requirements are desirable, but the project can still be considered complete without them.
- "Could have" requirements are optional and considered nice-to-have, but not necessary. They can be deferred or omitted without affecting the success of the project.
- "Won't have" requirements are considered out of scope and will not be included in the project.

The Moscow prioritization method provides a simple and straightforward way to classify and prioritize user requirements, helping to ensure that the most important requirements are addressed first and that resources are allocated efficiently.

The requirements for a gamified approach to a strong password creation information design for young kids between 8-11 years include:

2.2 Functional Requirements

	Functional Requirements	**Priority**
FR1	The game should have a **password strength assessment** tool to help children create strong password and provide feedback on the strength of their password choices.	M
FR2	The game should allow children to **personalize** their password creation experience by allowing them to choose their own characters, symbols, and numbers and to customize their rewards.	S
FR3	The game should include **interactive tutorials** that explain password safety concepts and best practices in an engaging and age-appropriate manner.	M
FR4	The game should have a **reward system** that incentivizes children to participate and learn about password safety, such as virtual badges or rewards for creating strong passwords or answering password-related questions correctly.	S
FR5	The game should **securely store** children's passwords and personal information, using encryption and other security measures to protect their privacy.	M
FR6	The game should allow children to provide **feedback** on their experience, such as rating the game or offering suggestions for improvements	S
FR7	The game should be **compatible** with various devices, and should be **accessible** to children with various disabilities, using assistive technologies where necessary.	M

2.3 Non-Functional Requirements

	Non-Functional Requirements	Priority
nFR1	The game should have user-friendly interface and be easy to navigate, providing a positive and engaging experience for children.	M
nFR2	The game should have fast load times and be responsive, providing a smooth and seamless experience for children.	S
nFR3	The game should be scalable to accommodate growth and future changes, such as increasing numbers of users or new features.	S
nFR4	The game should be maintainable, with a clear and organized codebase and documentation, to ensure that it can be easily updated and improved in the future.	S

By incorporating these requirements, we can create a gamified approach to strong password creation that is accessible, engaging, and effective in teaching children about digital safety.

3. Literature Review

3.1 Gamification

The process of using any kind of gaming technique in a non-game activity is called gamification. Gamification is mainly used to interact better with the user and make the user more interested in performing a particular task. This gives us better and a stronger output. It also used to increase the concentration levels of the user in performing these tasks.

George E. Raptis et al has observed that people who adopt a gaming mechanism into their non-gaming tasks tend to be more involved and motivated in performing those certain tasks. George E. Raptis spoke about using gamification techniques in password creation, he also observed an increase in the performance of the user as well as noted it influenced their behaviour. George E. Raptis considered using Graphical User Authentication(GUA) as the best form of security. In the process of GUA, users generate graphical passwords either by sketching symbols onto a backdrop picture or by the process of picking a portion of an image library. Similar to or larger than alphanumeric passwords are the password space of draw-a-secret systems. As a result, they present a possible substitute for authentication since they are thought to make the authentication method more secure and simpler to recall. [1]

Sam Scholefield et al implemented the method of using gamification in regard to password security, in which he had created a game wherein there would be 2 knights fighting each other. A dark knight and a golden knight and the user would be the golden knight. The system would then ask questions covering certain topics of password security. If the user answers the questions right the dark knight would eventually die and the golden knight would win the game. This experiment was later then put into trial by involving 17 participants of various gender, and levels of education. After the experiment, it was noticed that the participants did not have great knowledge of password security and they ended up setting passwords that are quite easy to be hacked by cyber attackers. It was also observed that the participants seemed a lot more interested in acquiring knowledge on password security through this method. [2]

3.2 Gamification for Kids

Gamification is something that is a really valuable tool for kids. Kids are often too playful and have a short attention span. Hence to keep them interested in a certain task is an arduous task. Hence adopting methods such as gamification for tasks that are not very intriguing can prove to be extremely effective in teaching kids about different information they require to know.

Victoria Vigilanti et al explained the importance of gamification in their blog. From the blog, we can understand that using gamification techniques to teach a kid any kind of information can go long way in the development of the child as the child is almost not even realizing that is learning new information while enjoying. This results in high motivation to continue and do more, as it is a proven fact that kids learn through emotions. The blog continues to state how a small healthy competition can help the kid grasp more knowledge at a faster pace. [3]

Robin Brewer et al, conducted an experiment on kids to see the impact of gamification on kids. He conducted 2 study experiments on a few kids. Experiment 1 was just a normal task given to the kids such as drawing certain gestures and also he gave a target task wherein the kids would have to keep finding different targets of different dimensions around the screen at different speeds. Experiment 2 was the same except he added 2 modifications. He used a gamification approach of first providing scores for the tasks and second providing small gifts for high scores. After completing both experiments, he was able to conclude that in experiment 1 only 2 out of 7 completed the experiment and some of the kids found it really boring that they requested to quit the experiment. It was completely the opposite after performing experiment 2. This time 5 out of 6 kids completed the experiment and the 1 kid had attempted the experiment. [4]

Rubén Camacho-Sánchez et al, had also conducted an experiment with 126 students which went along for 2 months. In his experiment, he divided students into 2 main groups: Control groups and Experimental group. Only 30% of students agreed to be in experimental groups and the rest 70% were in the control groups. The experimental groups were further divided into 2 other groups: The competitive experiment group and the individual experimental group. The control group had a more traditional type of teaching techniques such as lectures and classroom exercises. In the contrary, the experimental group had a more gamified approach. But in both groups the teaching content, number of classes, evaluation and grading criteria were the same. The 2 experiment groups had almost similar gamified approaches except for the individual experiment groups would have to complete individual activities. Whereas the other group would have group type experiments. This experiment was conducted for about 2 months. After the experiment, he was able to conclude that the students in the experimental groups performed significantly better than the control group students. Whereas, the 2 experimental groups performed quiet similar to each other and did not show a lot of difference. [5]

4. Personas

Persona 1

Name: Jack Dunn

Age: 11 Years

Hobbies: Reading, Sports, Video Games

Bio:

Jack likes to read comics. He spends a lot of his free time reading different comics. He also loves watching movies in the superheroes genre. His dad introduced him to football when he was young and he has been engrossed ever since. He also likes to play video games on his PS4 with his elder brother.

Problems:

His school has introduced the concept of email creation for the students to learn professionalism and how emails work. All students have been given assignments to create an email id, but the students haven't been taught to create strong passwords. His teacher wants all students to learn the importance of strong passwords but she hasn't been able to make all of them understand the concept.

Persona 2

Name: Rachel Jones

Age: 9 Years

Hobbies: Art, Reading, Music

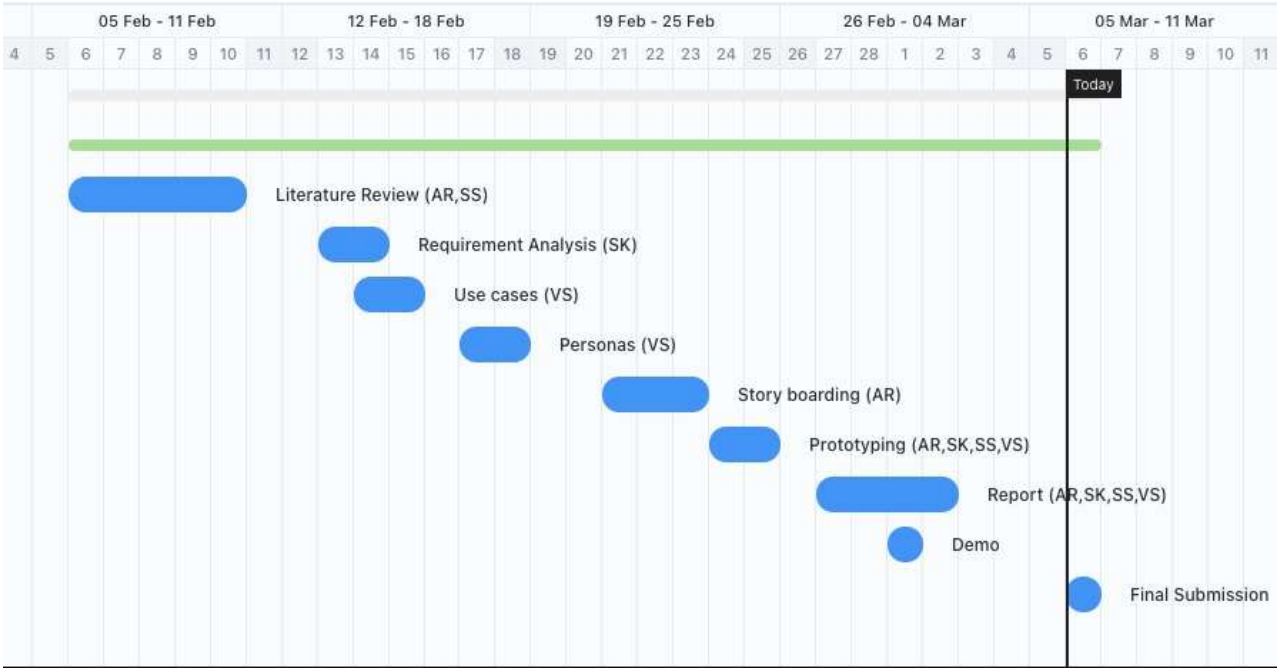
Bio:

Rachel likes to draw and listen to music. She also likes to read a lot of comic books. She likes to read anime and other comics that have a lot of humour. Rachel has a reading problem, as she was born with an eye defect that restricts her reading capabilities, so she uses a special eye glass to read.

Problems:

Rachel's mom wants to teach Rachel about the importance of strong passwords, as her account was recently hacked due to poor password strength. Considering Rachel's short span of attention, her mom is looking for a way to teach Rachel about password security. She also wants an app that is accessible for Rachel, to support her eye defect.

5. Gantt Chart



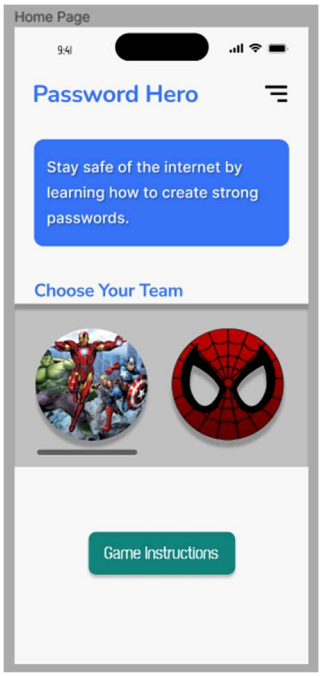
The tasks were assigned equally to each individual member according to their strengths.

The prototyping and report were done by all the members together.

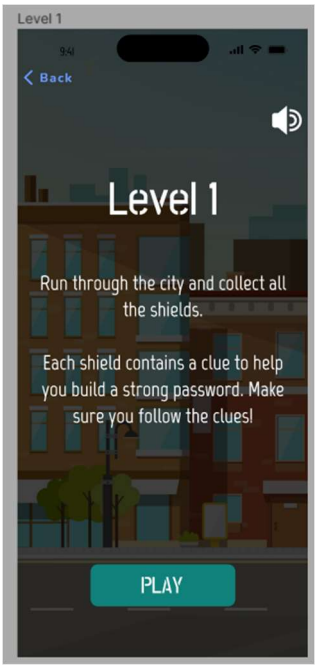
6. Prototype Design

6.1 Design

Opening Page

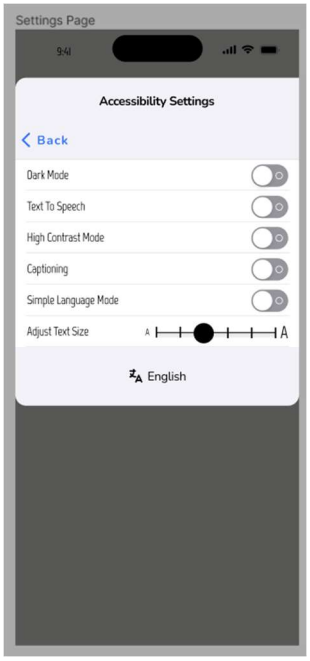


Choosing avatar to play the game.

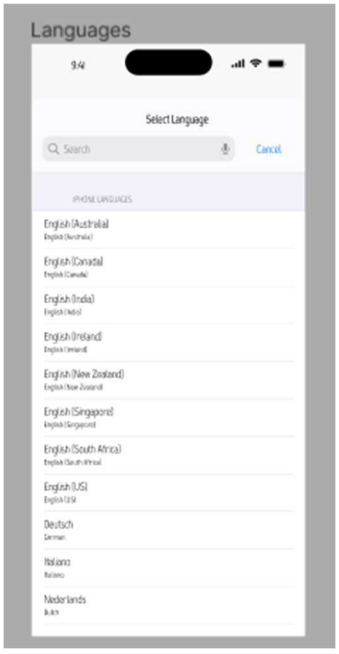


Level 1 instructions

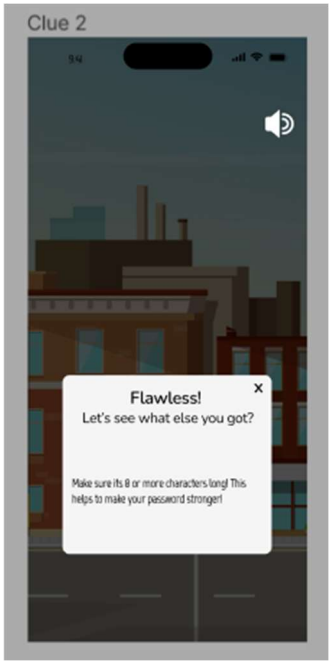
There is a voice modality included in this page that reads the text on the screen.



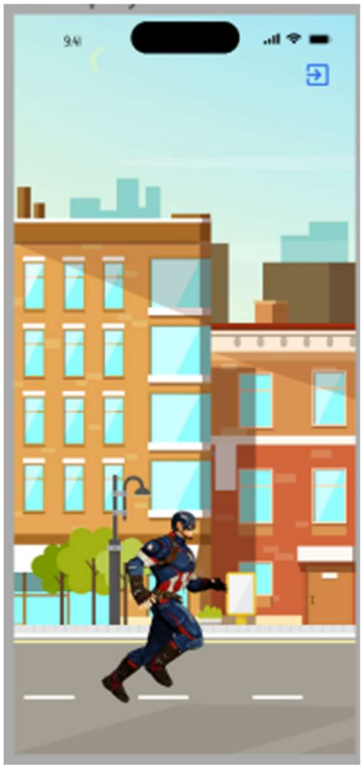
Settings Page where the user can change the game settings according to their preferences.



Languages Page where the user can change the language for the game according to their preferences.

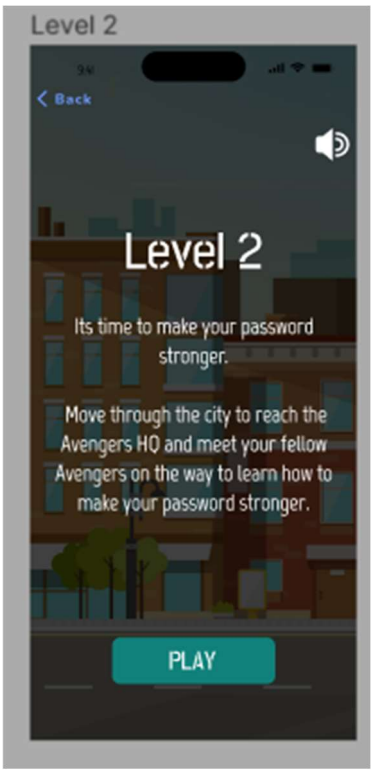


A clue in-game given to the user to create a password. A *'cross'* button is present to let the user close the box.



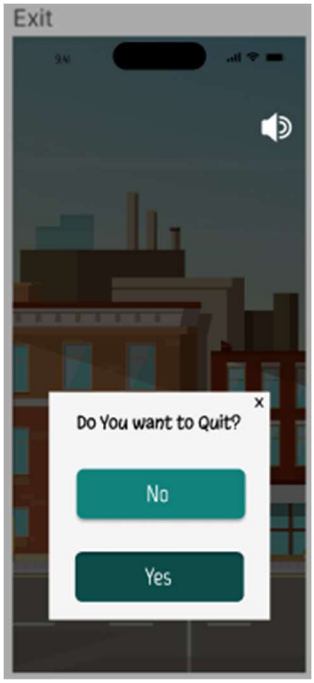
Gameplay scene.

The player avatar moves through the city. A exit button is given to allow the user leave the game at any time.



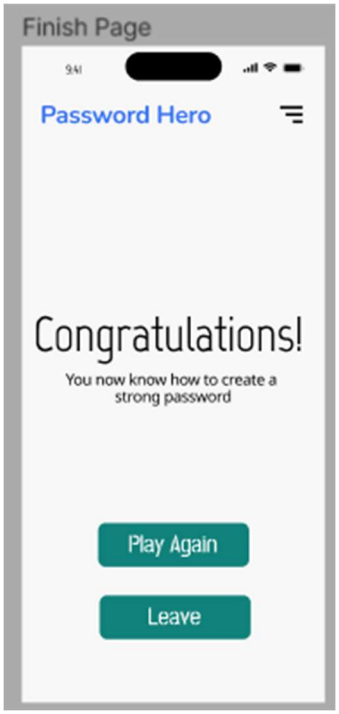
Level 2 instructions.

A clue in Level 2 to make the password stronger..



Exit Page.

The user is given a choice to either exit or get back to the game.



Finish Page.

This page is after completing the game. The user can either play again or leave the game.

6.2 Advanced Human Computer Interaction Concepts

We have used 4 modalities in our prototype. The four modalities are voice, colour, text and language.

Voice: We have added a button for the text on the screen to be read out. This helps people who have reading difficulties like cataract or dyslexia.

Colour: We have an option to change the colours in the game. The *'Colour Contrast'* option changes the existing colours to contrasting colours which helps in visibility for people who have colour blindness. The 'Dark Mode' option changes the screen to a darker screen, which helps people who can't tolerate bright lights.

Text: This option enables the user to change the text size to make it visible for the user according to their preferences.

Language: This makes the game accessible for people whose first language is not English and lets them choose their language of choice.

APPENDIX

Use Cases

Use Case:	Choose player avatar
Goal:	Choose an avatar to play the game
Primary Actor:	User
Precondition:	None
Postcondition:	An avatar is chosen to play the game
Main Flow:	• Step 1: Scroll through the avatar list. • Step 2: Choose an avatar. • Step 3: Continue to game instructions page.
Alternative Flow:	• Step 1: Exit the page. • Step 2: Goes to home page

Use Case:	Adjust settings according to preference
Goal:	Making changes according to user preference
Primary Actor:	User
Precondition:	None
Postcondition:	Changes made according to the user
Main Flow:	• Step 1: Open settings page • Step 2: Adjust game settings according to preference (Text size, colour etc.) • Step 3: Confirm settings. • Step 4: Continue with the game
Alternative Flow:	None

Use Case:	Create a password
Goal:	Learn to make a password that follows all rules in Level 1
Primary Actor:	User
Precondition:	Choose an avatar
Postcondition:	A password is created.
Main Flow:	• Step 1: Move through the city. • Step 2: Find clues to create a password. • Step 3: Create a password using the clues found. • Step 4: Continue to Level 2.
Alternative Flow:	• Step 1: Exit the game. • Step 2: Goes to home page.

Use Case:	Make the password stronger
Goal:	Learn to make the password stronger in Level 2
Primary Actor:	User
Precondition:	Level 1 is completed.
Postcondition:	Password is made stronger.
Main Flow:	• Step 1: Move through the city. • Step 2: Find clues to strengthen the

	password. • Step 3: Strengthen the password using the clues found. • Step 4: Exit.
Alternative Flow:	• Step 1: Exit the game. • Step 2: Goes to home page.

Storyboard

Opening page

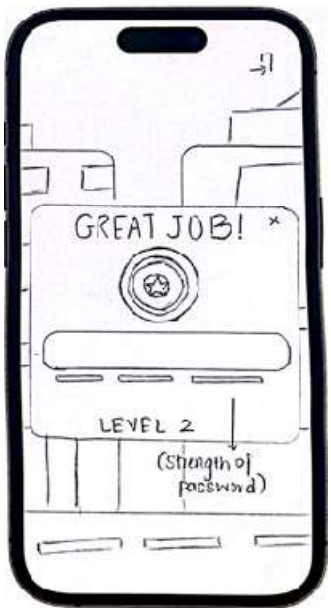
Main page: The user can access the accessibility setting as well as select their preferred team. Once they choose their preferred team they can proceed to read the game instructions.

Accessibility setting: This page aids the users to use their preferred and required settings. Through this page we also offer accessibility choices for people of determination.

Language setting: This page helps the users of different nationalities with language barriers to choose their preferred language for their convenience. We have also provided voice modalities in case the user wants to speak into the mic.

This page helps the user to understand the rules and regulations of the game. This is very important for the kids as it helps them to know all the necessary information before playing the game.

This page is just before the level 1 gameplay begins. Through this page the users can understand the necessary information to play level 1.



The character runs through the city to collect the shield. Each shield contains a password cue that helps the user to learn and create a secure password.

The user must enter a password with the help of those password cues at the end of level 1. Only if the password is strong enough will they be able to move on to the next stage.

The character runs through the city to meet his fellow Avengers. Each Avenger will provide a password cue that helps the user to learn and create a secure password.

The user must enter a password with the help of those password cues at the end of level 2. Only if the password is strong enough will they be able to complete the game.

REFERENCES

[1] G. E. Raptis, C. Katsini, A. J.-l. Cen, N. A. G. Arachchilage, and L. E. Nacke, "Better, Funner, Stronger: A Gameful Approach to Nudge People into Making Less Predictable Graphical Password Choices," presented at the Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, Yokohama, Japan, 2021. [Online]. Available: https://doi.org/10.1145/3411764.3445658.

[2] S. Scholefield and L. Shepherd, "Gamification Techniques for Raising Cyber Security Awareness," presented at the 1st International Conference on HCI for Cybersecurity, Privacy and Trust, Orlando, Florida, USA, July 31, 2019, 2019. [Online]. Available: https://arxiv.org/ftp/arxiv/papers/1903/1903.08454.pdf.

[3] V. Vigilanti, "The Benefits of Gamification in Children's Education," vol. 2023, ed, 2019.

[4] R. Brewer, L. Anthony, Q. Brown, G. Irwin, J. Nias, and B. Tate, "Using Gamification to Motivate Children to Complete Empirical Studies in Lab Environments," presented at the International Conference on Interaction Design and ChildrenAt, New York City, New York 2013. [Online]. Available: https://www.researchgate.net/publication/263009331_Using_Gamification_to_Motivate_Children_to_Complete_Empirical_Studies_in_Lab_Environments.

[5] R. Camacho-Sánchez, A. Rillo-Albert, and P. Lavega-Burgués, "Gamified Digital Game-Based Learning as a Pedagogical Strategy: Student Academic Performance and Motivation," *Applied Sciences,* vol. 12, no. 21, p. 11214, 2022.