

**A Capstone Project Submitted to the Faculty of the**

**Department of Computer Science and Information Systems**

**College of Arts and Sciences**

**American University of Kuwait**

**In Partial Fulfillment of the Requirements for the degree**

**Bachelor of Science in Computer Science**

**CyberSecTNT**

**By**

**Abdulaziz Karam, 35621**

**Abdulhameed Salama, 33292**

**Anas El-Ghabra, 42531**

**Mohammad Masoud, 34706**

**Advisor**

**Dr. Nooh Bany Muhammad**

**Course Coordinator**

**Dr. Iyad T. Doush**

**Spring, 2020**

****

**Department of Computer Science and Information Systems**

**College of Arts and Sciences**

**American University of Kuwait**

**Approval Sheet – CSIS 490 Capstone I**

The Capstone Project entitles **CyberSecTNT** Prepared and submitted by **Abdulaziz Karam:35621 ,Abdulhameed Salama:33292, Anas El-Ghabra:42531, Mohammad N Masoud:34706** has been examined and is recommended for approval and acceptance

Recommended: Date:

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

(Signature of Advisor over printed name)

Approved by the Oral Defense Panel with a grade

Approved: Date:

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

(Signature of the Panel Chair over printed name)

Accepted and approved in partial fulfillment of the requirements in Bachelor of Science in Information Systems

Approved: Date:

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

(Signature of the Course Coordinator over printed name)

# Dedication

This project is dedicated to the CSIS department of AUK and to the people who have interests in educational mobile applications. Thinking of a project idea, we wanted to do something completely different and impressive that would stand out amongst the other projects that have been developed over the years and to provide proper knowledge to our users to use in their life, as a result, we have come up with this project. Also, we would like to dedicate this project to Dr. Nooh Muhammad, our capstone advisor, as he is the key to our motivation and helped us come up with this idea and encouraged us to think outside the box.

# Acknowledgement

We would like to express our gratitude by saying thank you to Dr. Nooh Muhammad for agreeing to be our advisor for our capstone project. His wisdom and knowledge have guided us through our struggling phases of this capstone project and motivated us to perform at a high rate to bring our idea to life. We appreciate the time he has taken to help keep track and monitor our work as we would have been lost without him. We would also like to thank the Computer Science department as a whole for building us to become the people we always aspired to be.

# Abstract

The purpose of this paper is to research the idea of developing an application that will assist non-technical users in gaining more knowledge about cybersecurity, as part of this Capstone project in the department of Computer Science and Information Systems at the American University of Kuwait. This paper begins by addressing the importance of cybersecurity and the escalating importance of it. Moreover, we examine the different methods of hacking and simple techniques of adding extra layers of security. Which all comes to the development of an application that would help raise the awareness of non-technical users about cybersecurity and its main threats.

# Table of content

Contents

Table of Contents

[**Dedication 3**](#_heading=h.gjdgxs)

[**Acknowledgement 3**](#_heading=h.30j0zll)

[**Abstract 3**](#_heading=h.1fob9te)

[**Table of content 4**](#_heading=h.3znysh7)

[**List of Figures 5**](#_heading=h.3dy6vkm)

[**List of Tables 6**](#_heading=h.1t3h5sf)

[**Chapter 1 7**](#_heading=h.4d34og8)

[1.1 Introduction 7](#_heading=h.2s8eyo1)

[*Research Context 7*](#_heading=h.17dp8vu)

[1.2 Research Objectives 9](#_heading=h.3rdcrjn)

[*Project Questions 9*](#_heading=h.26in1rg)

[1.4 Significance of the Research 10](#_heading=h.lnxbz9)

[**Chapter 2 Review of Related Literature 11**](#_heading=h.35nkun2)

[2.1 Theoretical Background 11](#_heading=h.1ksv4uv)

[2.2 Related Literature 12](#_heading=h.44sinio)

[2.3 Related Projects 12](#_heading=h.2jxsxqh)

[2.4 Issues with prior Projects 23](#_heading=h.19c6y18)

[**Chapter 3 Technical Background 24**](#_heading=h.3tbugp1)

[3.1 Technicality of the project 24](#_heading=h.28h4qwu)

[3.2 Details of the technologies to be used 24](#_heading=h.37m2jsg)

[3.3 How the project will work 25](#_heading=h.46r0co2)

[**Chapter 4 Methodology 26**](#_heading=h.2lwamvv)

[4.1 Requirements Specifications 26](#_heading=h.2zbgiuw)

[*4.1.1 Operational Feasibility 26*](#_heading=h.1egqt2p)

[*4.1.2 Technical Feasibility 29*](#_heading=h.4h042r0)

[*4.1.3 Schedule Feasibility 30*](#_heading=h.1baon6m)

[*4.1.4 Economic Feasibility 33*](#_heading=h.1opuj5n)

[*4.1.5 Requirements Modeling 35*](#_heading=h.11si5id)

**Chapter 5 Capstone two 47**

5.1 Design 47

*5.1.1 Sequence Diagram 47*

*5.1.2 Application Screenshots 48*  
[5.2 Development Environment](#_heading=h.2zbgiuw) 52

[*5.2.1 Front end and back end*](#_heading=h.1egqt2p) *52*

[*5.2.2 Deployment Diagram*](#_heading=h.4h042r0) *53*

[5.3 Testing](#_heading=h.1opuj5n) 54

[*5.3.1 Unit Testing*](#_heading=h.11si5id) *54*[*5.3.2 Integration Testing*](#_heading=h.1egqt2p) *54*

[5.4 Implementation Table](#_heading=h.1baon6m) 56

[5.5 Recommendation](#_heading=h.1opuj5n) 57

[5.6 Brief Manual 57](#_heading=h.11si5id)[[5.7 Conclusion](#_heading=h.11si5id)](#_heading=h.1opuj5n) [58](#_heading=h.11si5id)

[5.8 Task Devision](#_heading=h.11si5id) 59

[**Bibliography**](#_heading=h.1smtxgf) **60**

[**5 Survey**](#_heading=h.4cmhg48) **61**

# 

# List of Figures

[Figure 1 Survey question1: To determine the target age group 6](#_heading=h.3l18frh)2

[Figure 2 Survey question2: To determine subject knowledge of the group](#_heading=h.206ipza) 62

[Figure 3 To determine the user's level of interest in our application](#_heading=h.261ztfg) 63

[Figure 4 To determine the impact of our application](#_heading=h.l7a3n9) 63

[Figure 5 To determine the users awareness of cyber-attacks](#_heading=h.356xmb2) 64

[Figure 6 To understand whether people care about being secure or not](#_heading=h.1kc7wiv) 64

[Figure 7 To see if people are interested in a application that mirrors real life attack](#_heading=h.1664s55) 65

[Figure 8 Targeted Attack Screenshot 1](#_heading=h.z337ya) 15

[Figure 9 Targeted Attack Screenshot 2](#_heading=h.3j2qqm3) 15

[Figure 10 Hackex Screenshot 1](#_heading=h.3vac5uf) 18

[Figure 11Hackex Screenshot 2](#_heading=h.pkwqa1) 18

[Figure 12 Hackex Screenshot 3](#_heading=h.48pi1tg) 18

[Figure 13 Hackex Screenshot 4](#_heading=h.2nusc19) 18

[Figure 14 Hackbot Screenshot 1](#_heading=h.vx1227) 20

[Figure 15 Hackbot Screenshot 2 2](#_heading=h.3fwokq0)0

[Figure 16 Hackbot Screenshot 3 2](#_heading=h.1v1yuxt)0

[Figure 17 Hackbot Screenshot 4 2](#_heading=h.4f1mdlm)0

[Figure 18 System Architecture 2](#_heading=h.nmf14n)4

[Figure 19 Fishbone Diagram](#_heading=h.sqyw64) 26

[Figure 20 Fishbone Diagram2](#_heading=h.3cqmetx) 27

[Figure 21 Functional Decomposition Diagram](#_heading=h.25b2l0r) 28

[Figure 22 Gantt Chart 3](#_heading=h.39kk8xu)2

[Figure 23 Context Diagram](#_heading=h.3oy7u29) 38

[Figure 24 Data Flow Diagram](#_heading=h.20xfydz) 38

[Figure 25 System Flowchart](#_heading=h.4kx3h1s) 39

[Figure 26 Use Case Diagram](#_heading=h.302dr9l) 40

[Figure 27 High-Level Class Diagram 4](#_heading=h.1f7o1he)1

[Figure 28 Activity Diagram 4](#_heading=h.2uxtw84)2

[Figure 29 ER Diagram 4](#_heading=h.3u2rp3q)3

Figure 30 Sequence Diagram 47

Figure 31 Deployment Diagram 53

# List of Tables

[Table 1 Table of surveys](#_heading=h.2rrrqc1) 61

[Table 2 Feature comparison 2](#_heading=h.2u6wntf)2

[Table 3 Gantt Chart 3](#_heading=h.2afmg28)1

[Table 4 CyberSecTNT Cost 3](#_heading=h.47hxl2r)3

[Table 5 Cost Over 5 Years 3](#_heading=h.2mn7vak)4

[Table 6 Requirement Modeling](#_heading=h.3ls5o66) 35

[Table 7 Risk Register 4](#_heading=h.3z7bk57)5

[Table 8 Probability/Impact Matrix](#_heading=h.2eclud0) 46

Table 9 Project Implementation Checklist 56

Table 10 Task Division 59

# Chapter 1

## **1.1 Introduction**

### **Research Context**

In today’s world everything revolves around computer technology and computer networks. The increasing dependency on computer networks makes cyber-attacks rates skyrocket as well. According to an article by the Security Magazine, “An estimated two million cyber-attacks in 2018 resulted in more than $45 billion in losses worldwide as local governments struggled to cope with ransomware and other malicious incidents.” Also, according to Symantec by 2023 it is estimated that 33 billion records will be stolen in 2019 compared to the 12 billion records stolen in 2018. [[5](#_heading=h.2jh5peh)]

The reason behind cyber-attacks being so popular is that it is safer, cheaper, less time consuming and overall more convenient than attacking a target physically. It is also harder to trace and sometimes the targets do not even realize that they have been a victim of a cyber-attack. Finally, they have no restrictions when it comes to the physical place of the victim since it is over the internet.

Cyber-attacks come in many different forms like, denial-of- service (DOS) or disrupted denial-of-service (DDOS) attacks, Phishing, Pharming, Spam, Malwares and many more. What they all have in common is the fact that they all attack the confidentiality, integrity and availability of the victim.

DOS and DDOS attacks focus on tiring the victim’s system or server by sending a large number of service requests making it inaccessible and extremely slow during the attack. The requests mainly come from machines controlled by the attacker via malicious software. In the year 2018 traffic via DDOS/DOS on GitHub, peaked at 1.3 terabytes per second setting a new world record that was then broken five days later with traffic peaking 1.7 terabytes per second. This type of attack does not benefit the attackers in any way unless they were a competitor trying to sabotage the competition. The most common ways of DOS/DDOS attacks are TCP SYN Flood attack, Teardrop attack, Smurf attack, Ping of Death Attack and Botnets.

Phishing attacks is sending an email or message to a victim making it appear like it is from a trusted source but instead the attacker gets access to the victim’s personal information. It could include downloading an attached folder or it could send you to an illegitimate website with the goal of stealing personal information through email or instant messaging. According to Symantec 54.6 percent of all email is spam that could lead to phishing and the number is growing increasingly [5].

Pharming attacks are quite like phishing attacks. They occur when the attacker prompts the victim to a fake website that looks exactly like the legitimate one and asks the victim to input personal information that benefit the attacker. 76 percent of organizations say they experienced phishing/pharming attacks in 2018.

Malware attacks are the most common attacks, they are unwanted software that can be attached to legitimate downloadable software that will provide the attacker illegitimate access to the victim's personal information. The types of malwares include, Macro Viruses, File Infectors, System or Boot-record Infectors, Polymorphic Viruses, Stealth viruses, Trojans, Logic Bombs, Worms, Droppers, Spyware and many more.

## **1.2 Research Objectives**

The objective of this research is to raise the awareness of non-technical users about the importance of cybersecurity, by addressing the threats and ways to protect the users from such threats, which can help the users in their daily life. By applying the knowledge grasped from our game-based application users are able to protect themselves and the network environment around them. If a company gives its employees the opportunity to learn from the application, the overall security of the company would be affected positively. Its employees will be able to identify an attack happening and take appropriate measures to minimize the damage.

### **Project Questions**

In this paper we researched the main security risks, which raises the questions of:

* How can we help non-technical users gain knowledge of cybersecurity in the simplest way?
* What are the main practices for people to add an extra layer of security to their life?
* How to make the application as simple as it can for non-technical users?
* How will this application help the companies’ security standards?
* What are the main features that our application should have?

These questions will play a huge role throughout the process of planning and developing our software. This will guarantee that the application will have a very positive impact on its users and help them with their lack of knowledge with cybersecurity in a fun and interactive way.

The positive impact we are trying to achieve is aimed at two aspects mainly which are industries and individuals. No matter the number of security layers the company adds or how strong their firewalls are, one employee who does not have enough knowledge about cybersecurity would give access to hackers in the simplest ways without realizing it. That is why our focus is to raise the knowledge of the non-technical users

## **1.4 Significance of the Research**

CyberSecTNT is an application that targets non-technical users, the application’s main goal is to provide awareness and teach basic security in the form of both a competitive and a non-competitive gaming environment. Our research was conducted in the form of a survey that will help us better understand what the consumers want to see in our application. Another form of research we have done is looking at our competitors and creating a table of features that will be shown later on.

# Chapter 2 Review of Related Literature

## **2.1 Theoretical Background**

While the number of security attacks is increasing, with an increase of around 67% in security breaches, 72% increase in the annual costs of cybercrime within the last five years, yet the human aspect remains the weakest link [1]. The lack of knowledge and false practices that most non-technical users are doing are costing the companies large amounts of money and resources.

CyberSecTNT is a platform that allows users to learn the basics of cybersecurity. The game is going to consist of different levels, each level is going to teach the user different skills and tools that are involved in cyber-crimes. Some attacking tools that we will be including are, phishing tool, scanning tool, bypassing tools and finally hacking tools like brute force and social engineering. Scanning will be used to scan possible targets to hack. Phishing tool will be used to send the selected users and email with the intent of them falling into the trap. Some defending tools will include an anti-virus and a firewall. Educational games can be classified into two categories, either boring educational games, that are usually very informative, or interesting games that do not deliver proper knowledge. On the other hand, CyberSecTNT’s goal is to educate the user while enjoying the aspects of the game. According to a survey we undertook, 78% of people were interested in learning more about cybersecurity through an application. Thus, having the application on a smartphone will make it easily accessible to the users.

## **2.2 Related Literature**

Raising awareness about cybersecurity is becoming more and more important in time, due to the integration of technology into our lives. However, regardless of the significance of educating people about cybersecurity, training employees to think about security is “one of the most underfunded activities in cybersecurity budgets [[1](#_heading=h.2jh5peh)]”. Attackers use of social engineering is increasing dramatically over the last few years, this puts companies at risk of being attacked due to the art of understanding how humans think [[2](#_heading=h.2jh5peh)]. Although, some companies are starting to increase their investments in cybersecurity [[2](#_heading=h.2jh5peh)], it is still not enough. A study was conducted to see how well the employees will react to a phishing attack, the results were shocking as 58% of the employees revealed their passwords if the caller said that they were from the IT department [[3](#_heading=h.2jh5peh)]. These statistics and more, show us the importance of raising the awareness of cybersecurity, because most of the non-technical users fall victim for the simplest hacking techniques.

CyberSecTNT is an application with the aim of solving these issues by tackling all the basic knowledge about cybersecurity in a fun and interactive way. Also, games have great impact on the learning process of the users, because of the simple, interactive, fun and dynamic way of delivering information [[4](#_heading=h.2jh5peh)]. Thus, delivering the basic knowledge about a topic with rising importance would have much more positive impact if delivered through a game rather than other methods.

## **2.3 Related Projects**

Throughout our research we found various games that aim to teach security knowledge, each game has its advantages and disadvantages, and the way they delivered their message varied from one game to another. Our biggest competitors are:

**1. Targeted Attacks (Trend Micro)**

**Statistics:**

The website was created in 2015 with the intention of creating an educational environment. We estimate the website value of trendmicro.com is currently at 265,994 USD and reaches roughly 31,387 unique users each day that generate 121,458 daily pageviews.

**Game Biography:**

With all the bad things in life, we like to believe that “it will never happen to us”. Unfortunately, the reality of targeted attacks against commercial organizations is such that many in the security world are characterizing it as a “when” rather than an “if”.

The game wants to put you in the driving seat. You are the Chief Information Officer of a global organization called The Fugle, on the verge of making the first release of a biometrically authenticated mobile payment app. You will steer the project through its final stages, dealing with your internal security team, your colleagues in Marketing and Public Relations and of course your Chief Executive Officer.

There are many competitors and individuals out there who would love to get their hands on the data held by your organization at such a critical time. Can you make the right choices? Can you keep the project on time and on budget? Can you protect your company from attack?

Based on the format of the old “Choose Your Own Adventure” books, the game offers you the chance to step into someone else’s shoes and find out if you’re good enough to come out on top.

Game Specifications:

· Story line

· Different endings

· Real life situations

· Requires critical thinking

Advantages and disadvantages:

The game hooks the users into their storyline, and it gives you a real-life scenario feeling. Also, each decision needs to be calculated and you do not know how many levels are left, so you cannot tell if you should spend your money on a specific task or not. Also, the game tells the user what you did wrong and why it was wrong. On the other hand, the game scenarios are limited and there are not many decisions and it gets boring after a while.

Screenshots:

|  |
| --- |
| *Figure 8 Targeted Attack Screenshot 1* |
| *Figure 9 Targeted Attack Screenshot 2* |

**2. HackEx**

Statistics:

The game was released on 2015. It has around 500 online users every day on the IOS and much more on the Android devices. It has 79,633 users in total and it got more than one million downloads.

Game Biography:

The game was developed to create a hacking simulation. The game describes the player as the “ultimate hacker”, that would be asked to hack other players’ virtual devices and defend his own. The aim of this game is to build yourself a reputation in the hacking world, by cracking players’ bank accounts, uploading viruses to generate money, manipulate their logs and more. Also, the hacker should remove his trace completely, which according to the game designers is what a “ultimate hacker” is all about.

Game Specifications:

* Story line
* Upgrading hacking and defending tools
* Upgrading the hacking and defending tools
* Transfer and deposit amounts in your virtual bank account
* Hacking other player’s virtual banks and transfer their funds
* Uploading viruses
* Hiding activities by erasing the trace of the hacker from the log
* Scoreboard to record the achievements

Advantages and disadvantages:

The beauty of this game relies in its simplicity, and that it does not require any previous knowledge. Also, the tools used in the game are similar to the real life’s tools used in hacking, which would give the user a broad knowledge about cybersecurity, and it would give the feeling that the user is an actual hacker. On the other hand, the limited functionalities of the game and old user interface bring down the game’s quality and makes it less appealing to the users. Furthermore, there are a lot of dead accounts in the game, and some hacking processes require a lot of time due to this. Also, there are a lot of limitations to what you can do in the game, for example, the users cannot sort or label the machines that they intruded. Lastly, the very limited functionalities in the game makes it repetitive.

Screenshots:

|  |  |
| --- | --- |
| *Figure 10 Hackex Screenshot 1* | *Figure 11Hackex Screenshot 2* |
| *Figure 12 Hackex Screenshot 3* | *Figure 13 Hackex Screenshot 4* |

**3.**  **Hackbot**

Statistics and Game Biography:

The game was released in 2016. It has around over a million downloads on both platforms IOS and android. the game is about simulating attacks and challenging yourself to analyze the given hints and interpret it into real words which can be used as passwords to access a user account or a password to access a server. The game is futuristic, and it puts the players in year 2051 where the top hackers and hacking firms created Hackbot to steal passwords and secrets of their opponents.

There are two types of modes available in game, Ranked match and Quick match. Quick match is about guessing the passwords and enjoying yourself by discovering the target secrets in this play mode. Ranked match is about guessing as many passwords within a specified time frame and also it allows challenge between friends.

Advantages and disadvantages:

This game mainly relied on one function which is cracking passwords that teaches the users the basics of social engineering. This game also hooks users that are interested in solving mysteries and brain teasers. Also, by adding the statistics and the ranking that triggers the competitive attitude for its users. However, having only one functionality is not enough to prevent the users from getting bored. Moreover, the lack of attention to details such as the sounds effects made the game’s quality unimpressive.

Screenshots:

|  |  |
| --- | --- |
| *Figure 14 Hackbot Screenshot 1* | *Figure 15 Hackbot Screenshot 2* |
| *Figure 16 Hackbot Screenshot 3* | *Figure 17 Hackbot Screenshot 4* |

The game is considered to be a strong competitor as it challenges both non-technical and technical users because of how it utilizes one’s analytical and gambling skills when it comes to reading hints and analyzing them. Also, the user interface of the application is a typical hacker themes (0’s and 1’s in green raining and black background). This gives the end users the feeling of being a hacker which makes them devote more time on the application. This also motivates the end-users to research the given tools to actually know how to perform a real-world attack, this game also works as a motivation for the end-user to learn more about security and how those hacking tools function.

**Overall Summary:**

Those are three of the main competitors we chose because they are one of the most downloaded games and they were targeted for non-technical users. Each game approached the game in a different way, and each game has its own positives and negatives. Our aim from this is to take the advantages of every game and try to avoid all the negatives. Moreover, those games despite their negatives, did a fair job delivering valuable information for its users, and it made it interesting to some extent. Also, those games require critical thinking, and some gave the users a good sense of hacking. Moreover, the colors and user interface contributed positively to the overall experience in the games. Those things are more shows that every detail matter and sometimes few negative aspects might affect the game massively, even the smallest details have a decent effect on the overall experience of the users.

*Table 2Feature comparison*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **HackEx** | **HACKBOT** | **Targeted Attack** | **CyberSecTNT** |
| **Levels** | **Unlimited** | Close | Close | **Specified** |
| **Badges (Awards)** | Close | Checkmark | Close | Checkmark |
| **Hacking tools** | Checkmark | Close | Close | Checkmark |
| **Boost Hacking Tools** | Checkmark | Close | Close | Checkmark |
| **User statistics** | Close | Checkmark | Close | Checkmark |
| **Offline mode** | Close | Checkmark | Close | Close |
| **Online mode** | Checkmark | Checkmark | Checkmark | Checkmark |
| **Buy experience** | Close | Checkmark | Close | Close |
| **Log checking** | Checkmark | Close | Close | Checkmark |
| **Stage Result** | Close | Checkmark | Close | Checkmark |
| **Scoreboard** | Checkmark | Close | Close | Checkmark |
| **IP scanner** | Checkmark | Close | Close | Checkmark |
| **Hints** | Close | Checkmark | Close | Checkmark |
| **Real life scenarios** | Close | Close | Checkmark | Checkmark |
| **Different endings** | Close | Close | Checkmark | Close |
| **Surprise element** | Close | Close | Checkmark | Checkmark |
| **Explaining what went wrong & why** | Close | Close | Checkmark | Checkmark |
| **Time limitation** | Close | Close | Checkmark | Checkmark |

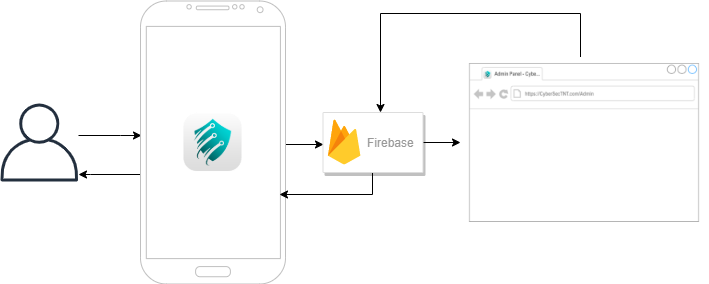
## **2.4 Issues with prior Projects**

Each game has its own positives and did a fair job in creating a fun game that taught the users few information about cybersecurity. However, each has its own share of negatives. For example: Targeted Attack had very few scenarios and it provided the user with very limited options, which resulted in the game being boring. HackEx also did a fair job teaching its users about hacking tools, but the limited functionalities of the game, the user interface, the dead accounts and the various limitations on the users brought down the games quality and made it less appealing. Furthermore, Hackbot is one of the games that really hooks the user, has many interesting levels and the user interface of the game gives the users a feeling that they are actual hackers. However, it had only one task to do in each level, which is to crack the password using social engineering and this made the users less interested in the game. All of those negatives are being considered in developing our application to avoid any of the issues talked about.

# Chapter 3 Technical Background

## **3.1 Technicality of the project**

In this chapter, we will be discussing the technicality and the functionality of the project. This will be done by using a detailed description of the type of project that we are creating and how it will be used.



*Figure 18 System Architecture*

## **3.2 Details of the technologies to be used**

**Development Tools**

* Android Studio: To develop mobile application using the Java Programming Language
* Illustrator: To design Logos and Icons
* XD: To design the User Interface
* Firebase: To develop the Database used for our application

**Software**

* Adobe Illustrator CC 2019
* Adobe XD 22.3 or Sketch 57.1
* Android 6.0 and higher
* Android Studio 3.5
* Java 8

**Hardware**

* Mobile Phone: 128GB 8GB RAM, Android 9.0
* Laptop: HP Omen15: 16GB RAM, 120GB SSD, 64-bits Windows 10, Intel Core i7 7700HQ

## **3.3 How the project will work**

Our project is aimed at non-technical users, it is going to teach them how cyber-attacks occurs and how to prevent them. There are five main phases for cyber-attacks, and we will be trying to teach the users these phases in a more general way. We will first prompt the user to log onto the game or create a new account. In order to start the attack users will have to scan and collect data about the target with the tools available. Then the user will try to gain unauthorized access and bypass the targets defense, each target will have their own defense mechanism depending on how long they have been playing the game. The user then must maintain their access by constantly checking on the target and how far they have progressed. Lastly the user must clean up their tracks so no evidence, from where the attack came, is left. In the case of defending from the attacks the user will have to check their logs from any attacks that have happened and constantly in the need to upgrade their defensive tools. Defenders must also have a strong password that will not get bypassed easily through brute force, therefore they will be able to upgrade their password with their defense/anti-virus system while progressing. The user will also have to understand the way cyber-attacks happen and not fall for any traps, like emails, that can breach their defense system. Users will also be able to learn from scenarios that have been made demonstrating attacking concepts.

# **Chapter 4 Methodology**

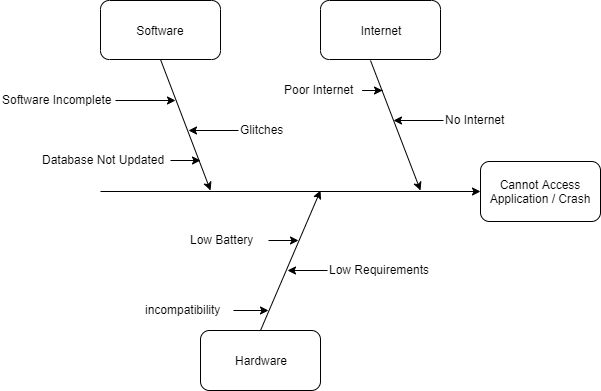
## 

## **4.1 Requirements Specifications**

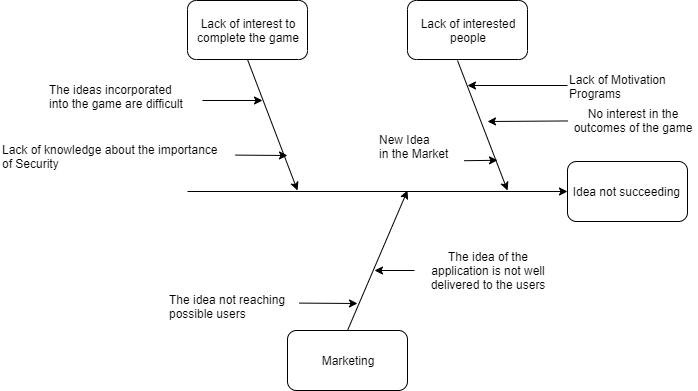
### **4.1.1 Operational Feasibility**

#### **Fishbone Diagram**:

The best way to keep track of a problem is by identifying the causes and effects. In order to know what are the possible interference that could cause our application to not work a fishbone diagram should be produced. The following diagram shows the causes of unable access of our application in the aspect of either software, hardware, or internet connection.



*Figure 19 Fishbone Diagram*



*Figure 20 Fishbone Diagram2*

#### **Functional Decomposition Diagram:**

*Figure 21 Functional Decomposition Diagram*

### 

### **4.1.2 Technical Feasibility**

#### Compatibility checking (hardware / software and other technologies)

**Maintenance:**

* The application will be using Firebase which has the Crashlytics feature that will be used to report crashes and the developers will check it frequently and update the codes of the application accordingly. In addition, adding features, improving user experience and increasing performance.

**Installation:**

* The application will be developed with Android Studio and it will be uploaded to the Google Play Store.

**Operating System:**

* Android is the operating system will be used and we are targeting Android 6.2 and above.

**Hardware:**

* Mobile phones.
* Laptop

#### **Relevance of the technologies**

CyberSecTNT will be built on Android Studio because it will be mainly on Android in its current stage and because Android Studio supports Java programming language since all our developers are familiar with Java. Our logos and icons will be designed on Adobe Illustrator to produce quality level graphic work. Adobe XD will be used to design the user interface since it is reliable and easy to use. Finally, Firebase will be used as our database back end service provider, it also had a feature called Crashlytics which will help with reporting crashes and it will be used for scheduling automated backups and for recovery.

### **4.1.3 Schedule Feasibility**

#### Gantt Chart:

Time management is of the essence and organizing the time for each task gives one the opportunity to dedicate the right amount of attention to each task; and as such, we have created this Gantt Chart to keep track of each step of our progress.

*Table 3 Gantt Chart*

|  |
| --- |
|  |
| *Figure 22 Gantt Chart* |

### **4.1.4 Economic Feasibility**

#### **Cost and Benefit Analysis:**

**Cost:**

Cost management is considered a sensitive topic due to its importance, therefore, a table has been constructed according to the needs of the project in close proximity. This can also help in future development of the project.

*Table 4 CyberSecTNT Cost*

|  |  |
| --- | --- |
| **Type** | **Cost** |
| 1.Software |  |
| 1.1 Adobe Illustrator CC 2019 | KWD 3 |
| 1.2 Adobe XD 22.3 | KWD 25 |
| 1.3 Firebase | KWD 150 |
| 2. Hardware |  |
| 2.1 OnePlus 7 | KWD 242 |
| 2.2 HP Omen 17 | KWD 500 |
| 2.3 HP Omen 17 | KWD 500 |
| 3. Maintenance | KWD 300 |
| 4. Server |  |
| 4.1 Retool | KWD 4 |
| 4.2 Server | KWD 23 |
| **Total** | **KWD 1747** |

Cost over 5 years:

*Table 5 Cost Over 5 Years*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Type/Cost** | **Year 1** | **Year 2** | **Year 3** | **Year 4** | **Year 5** |
| **Subscriptions** | KWD 150 | KWD 150 | KWD 200 | KWD 300 | KWD 500 |
| **Upgrades** | KWD 300 | KWD 300 | KWD 300 | KWD 300 | KWD 300 |
| **Updates** | KWD 0 | KWD 100 | KWD 100 | KWD 150 | KWD 150 |
| **Total** | KWD 450 | KWD 550 | KWD 600 | KWD 750 | KWD 950 |

#### Benefits (Profits) over 5 years

Our application’s main goal is to provide both awareness and education about security to everyone therefore we won’t be providing any pay to play advantage methods, one of the methods will be by hosting public seminars which will be sponsored to spread awareness and teach basic cybersecurity to everyone. Another way to benefit is adding advertisements in the application when released to the public and in order to remove those advertisements users will have to pay a registration fee which will be collected annually from the users.

#### Cost Recovery Scheme

The expected selling price of our application will be 6000 KWD based on the market value for similar apps. Profit = 6000– 1,747‬= 4253KWD.

### **4.1.5 Requirements Modeling**

#### **Requirement Modeling Table:**

*Table 6 Requirement Modeling*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Index** | **Process** | **Description** | **Input** | **Output** |
| **1** | Log In | Authenticates user into the platform if email-password authentication pair exists in Firebase | Email, password | User is forwarded to main menu page |
| **2** | Register | Creates a new email-password authentication pair in Firebase | Username, email, password | User is forwarded to main menu page and a new authentication pair is created |
| **4** | Leaderboard | Saves user data to display it to other players | Username | User will be able to see the scores of all other players in both competitive and none competitive mode. |
| **5** | View Profile | Ability to check your own profile | Username | Users can check his/her badges and current record on the leaderboard |
| **7** | View Tasks | Check different tasks | No input | User will be able to see a list of tasks to do, also the user will get an achievement for completing each task |
| **8** | View progress | Track progress statistics | No input | User able to check progress done so far from the available tasks |
| **9** | Live hack | Process of hacking other users | Target information | Gain unauthorized access to targeted device. |
| **10** | Log | Check for attacks | No input | Attacker information |
| **11** | Bank Account | Hold virtual money | Money | Money |
| **12** | Email | Send and receive emails | Messages | Messages |
| **13** | Find users | Find other users that play the game | No Input | List of vulnerable users |

#### **Performance:**

1. **Privacy:**

The user’s information will be safe and not shared with anyone

1. **Reliability:**

Our developers will insure their best practices while developing the application. The application will go through multiple layers for quality assurance. The system’s reliability is ensured up to standards, approximately 96%.

1. **Maintainability:**

The system will be supported by well-written documents that will help with the progress of modifying or adding new features. This will also facilitate the maintenance process on those who may wish to upgrade the system.

1. **Performance:**

The system should be fast and responsive to the users input with little to no delay.

1. **User Experience:**

Simple design and the applications contents will be non-technical friendly.

1. **Size:**

We will insure that the application does not take up too much space.

#### **Data and Process Modeling:**

##### **Context Diagram:**

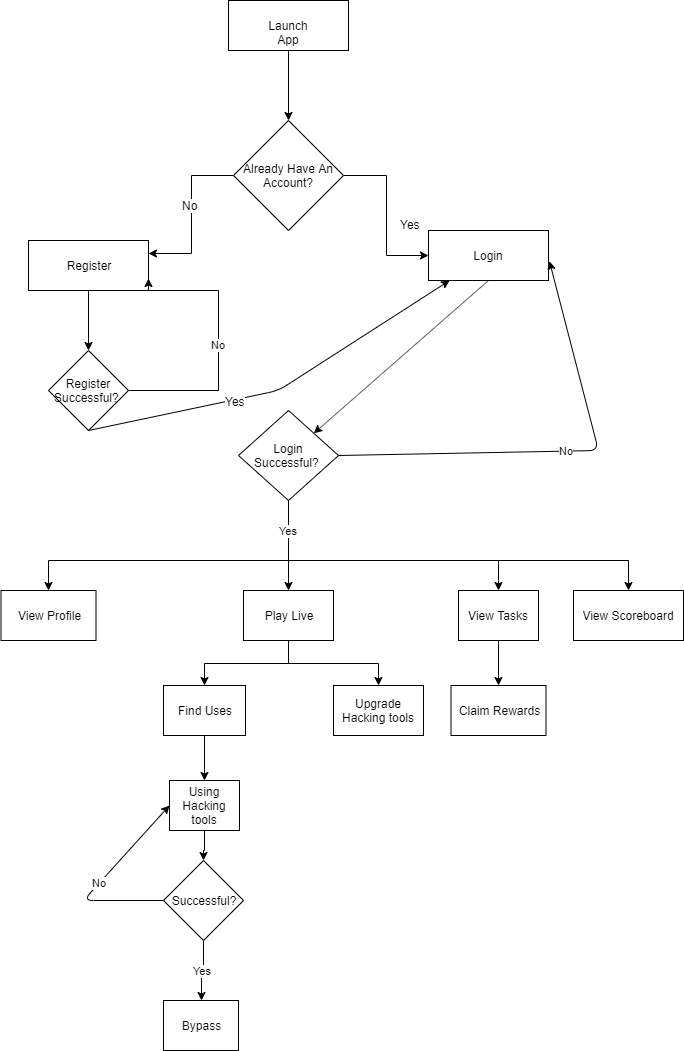
*Figure Context Diagram*

*Figure 23 Context Diagram*

##### **Data Flow Diagram:**

*Figure 24 Data Flow Diagram*

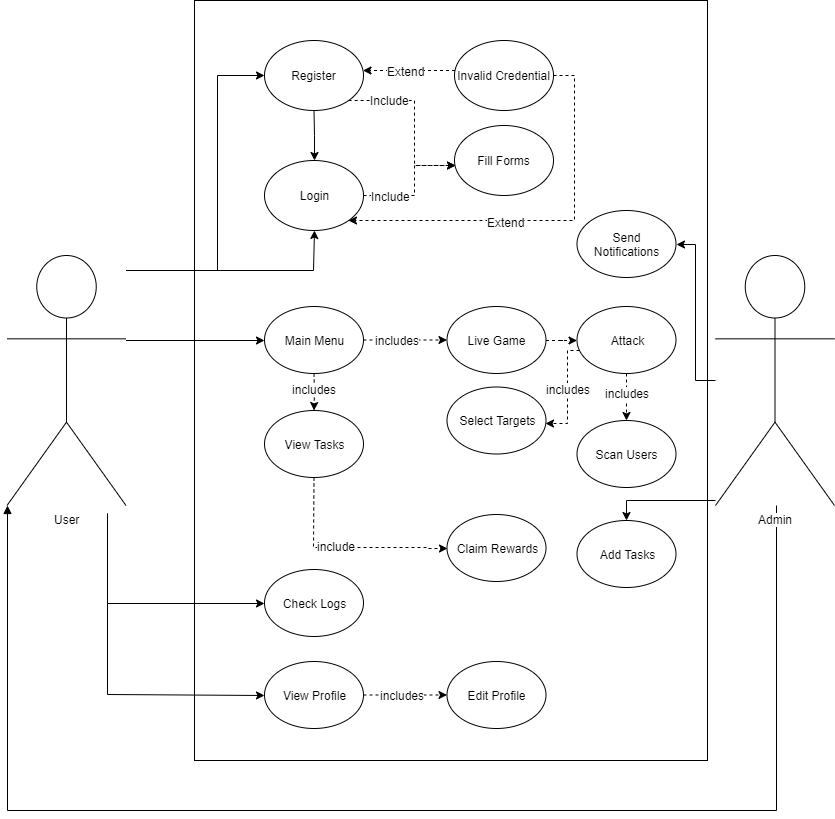
##### **System Flowchart:**



*Figure 25 System Flowchart*

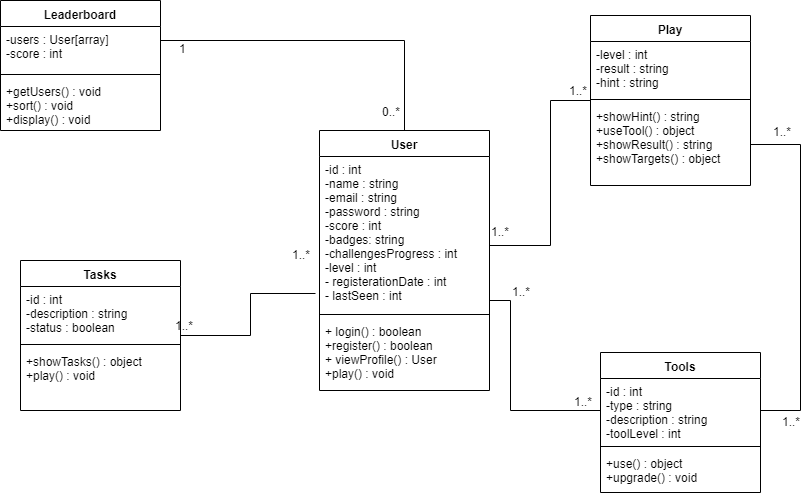
#### **Object Modelling:**

##### **Use Case Diagram:**



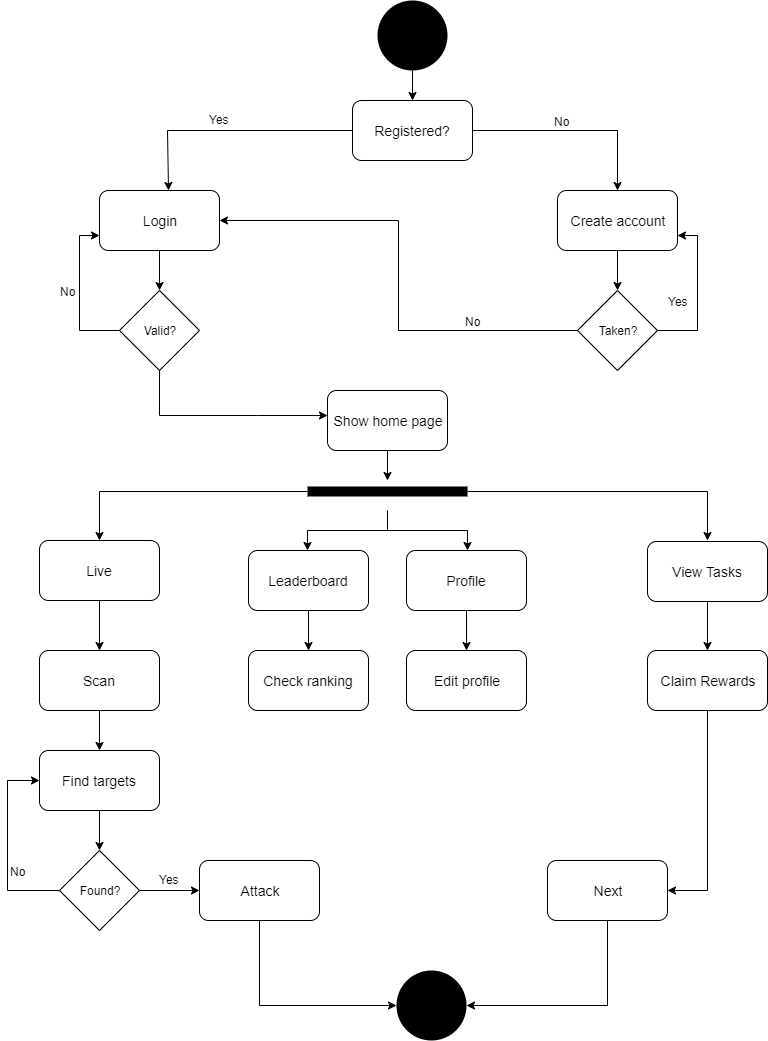
*Figure 26 Use Case Diagram*

##### **High -Level Class Diagram:**



*Figure 27 High-Level Class Diagram*

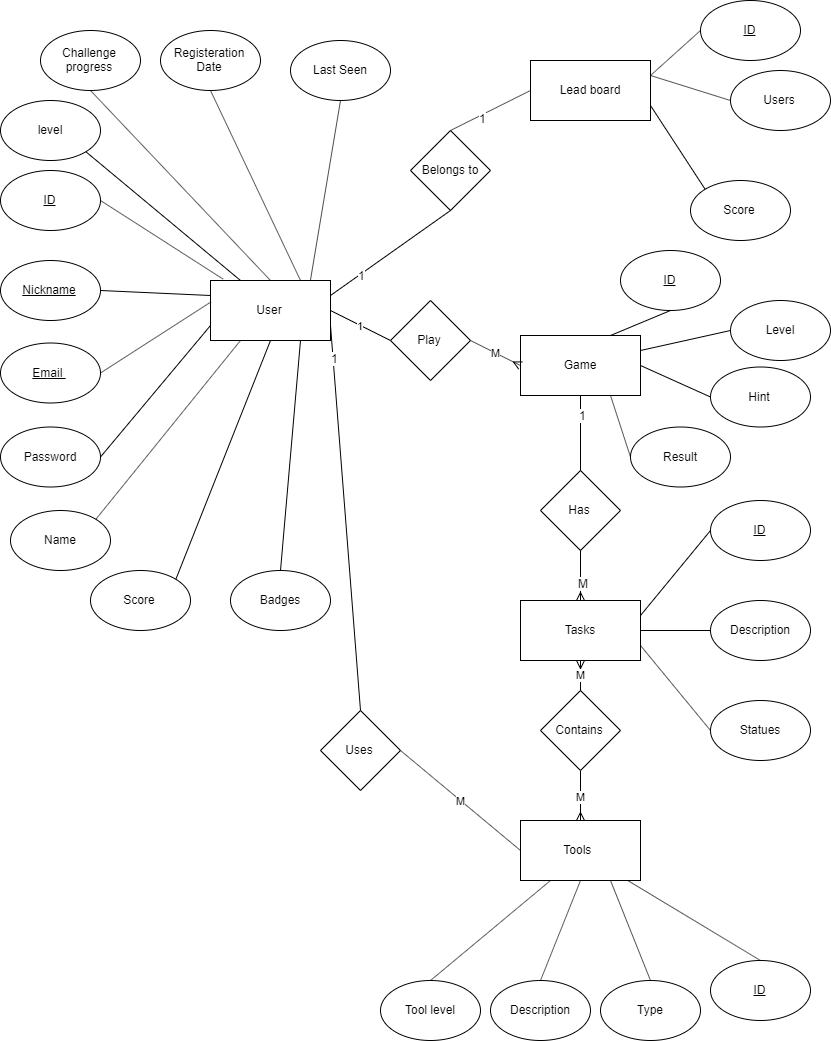
##### **Activity Diagram:**



*Figure 28Activity Diagram*

#### 

##### **ER Diagram:**



*Figure 29 ER Diagram*

#### **Risk Assessment/Analysis:**

Risks arise in every project, and we shouldn’t expect anything different in this project. However, anticipating the possible risks beforehand helps to solve and to recover from them with minimal damage. Risk Analysis helps to identify the possible risks throughout the life-cycle of the application, which includes the development stage and post launch stage. Moreover, identifying the risks might not be sufficient by itself. Thus, every risk should have the probability of its occurrence, impact, potential response, trigger, root cause, category, and the team that is responsible for each attack, which would help calculate the importance of each issue and rank them.

To deliver the Risk Register for CyberSecTNT application, all risks should be taken into consideration, the risks will be listed in the table below.

*Table 7 Risk Register*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Impact | Medium | Medium | High | Low | High | High |
| Probability | Low | Low | Medium | Medium | Low | Medium |
| Risk Owner | Marketing team | Technical team | Entire Team | Financial Team | Team Members | Database Manager |
| Potential Response | Developing new features to attract users. | Update platform | Loss of customers | Negotiate with product and service providers | Find a middle ground that satisfies all the members | Updating the database and fix the issue. |
| Triggers | The success of our application, and the possibility of adding more features. | Deprecated platform | Over sophisticated UI | The increase of prices and the number of users. | Different viewpoints about how the project should work | Glitches in the code |
| Root cause | Other companies get interested in our application | Not being up to date with future updates | Unfriendly user interface | Growth of our platform, which led to require more services | Different opinions | Database not being updated |
| Category | Market | Technical | Users | Financial | Communicating Risk | Technical |
| Risk Description | Possible competition | Operating System Updates | Platform’s ease to use | Service’s possible increase in price | Lack of unity between team members | Database issues |
| Rank | 4 | 5 | 1 | 6 | 3 | 2 |
| # | 1 | 2 | 3 | 4 | 5 | 6 |

The table below describes the risks, based on the probability and the impact of each risk. This is done by implementing the Risk Register table, to give a better image of the significance of each risk.

**Risk Traceability Matrix:**

*Table 8 Probability/Impact Matrix*

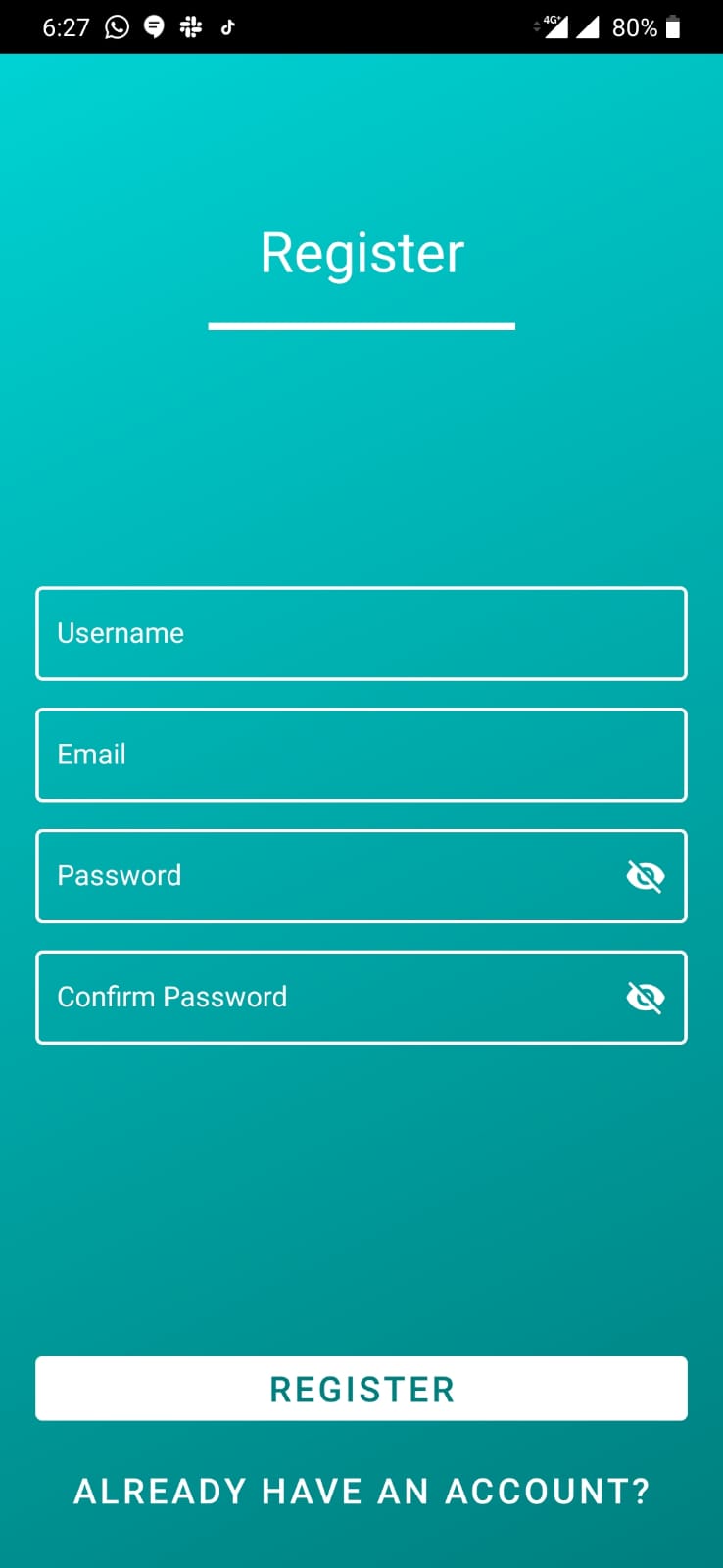
|  |  |  |  |
| --- | --- | --- | --- |
| Impact  Probability | Low | Medium | High |
| Low |  | 1 & 2 | 5 |
| Medium | 4 |  | 3 & 6 |
| High |  |  |  |

### **5.1 Design:**

**5.1.1 Sequence Diagram:**A screenshot of a cell phone

Description automatically generated

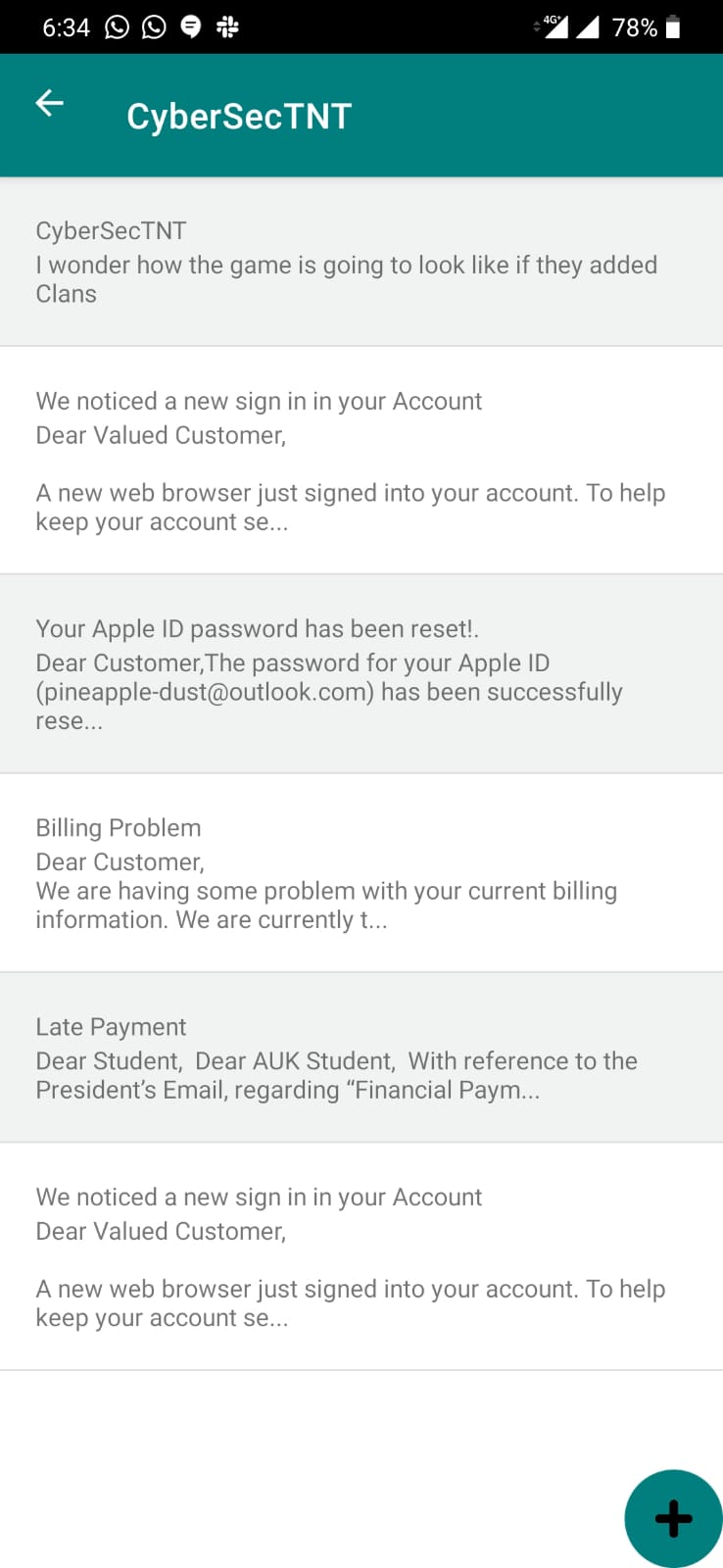
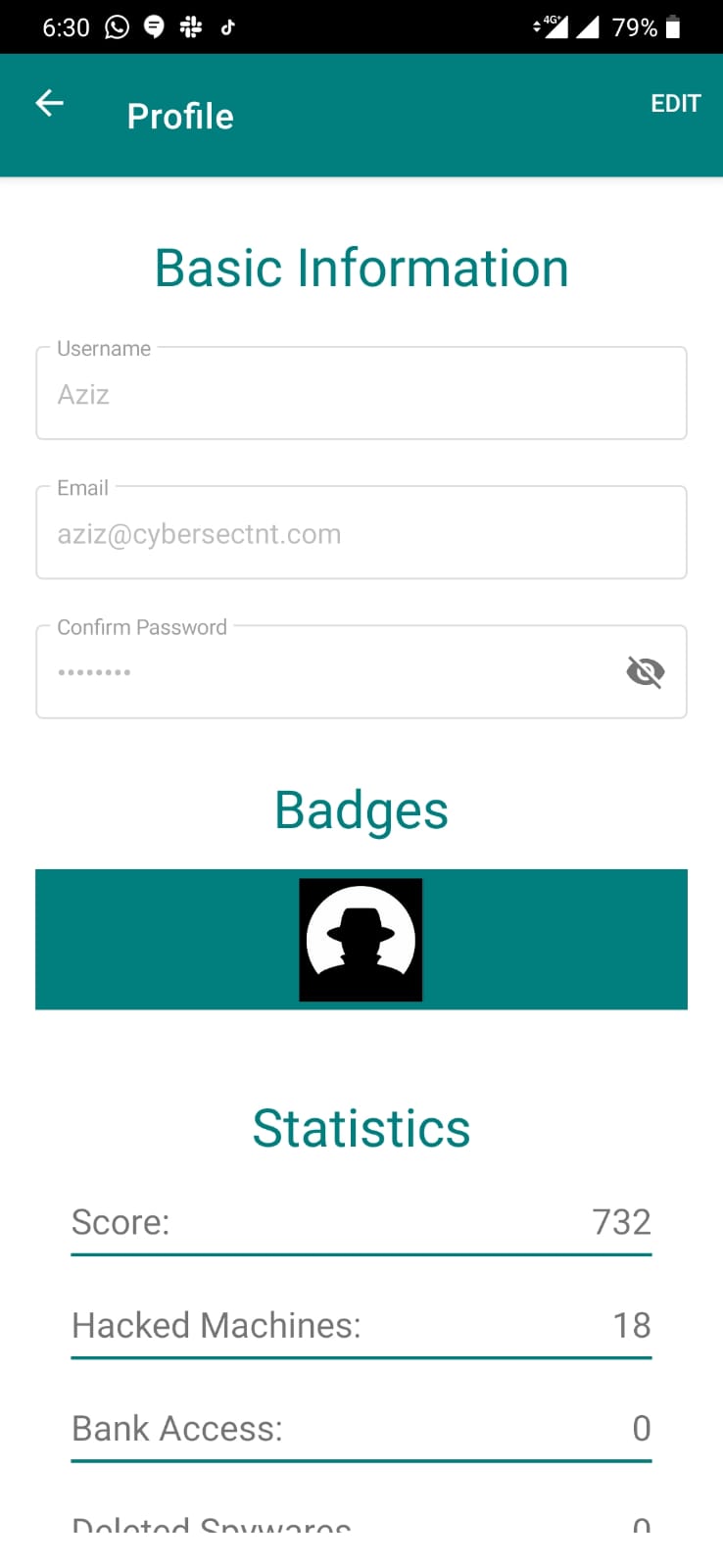
Figure 30 Sequence Diagram

**5.1.2 Application Screenshots:**

****

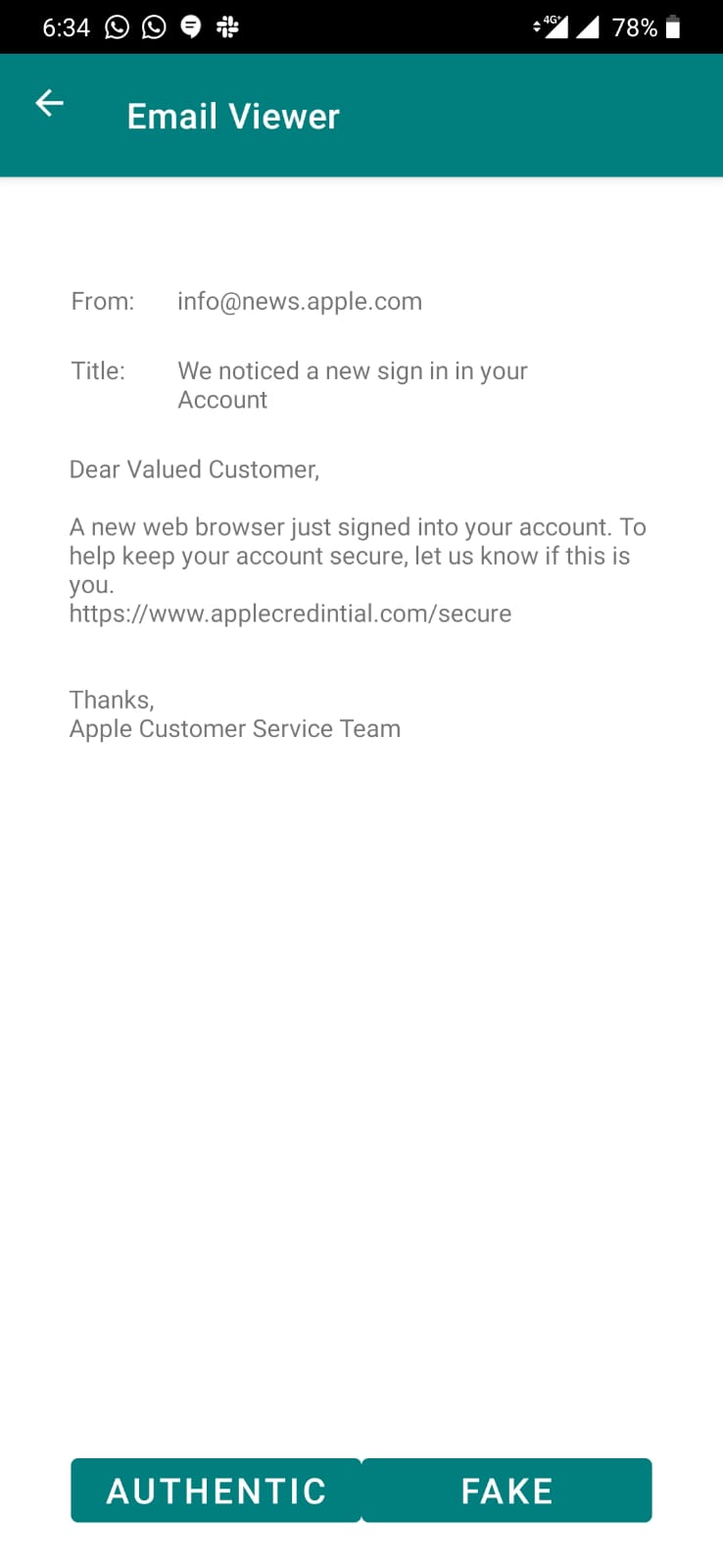
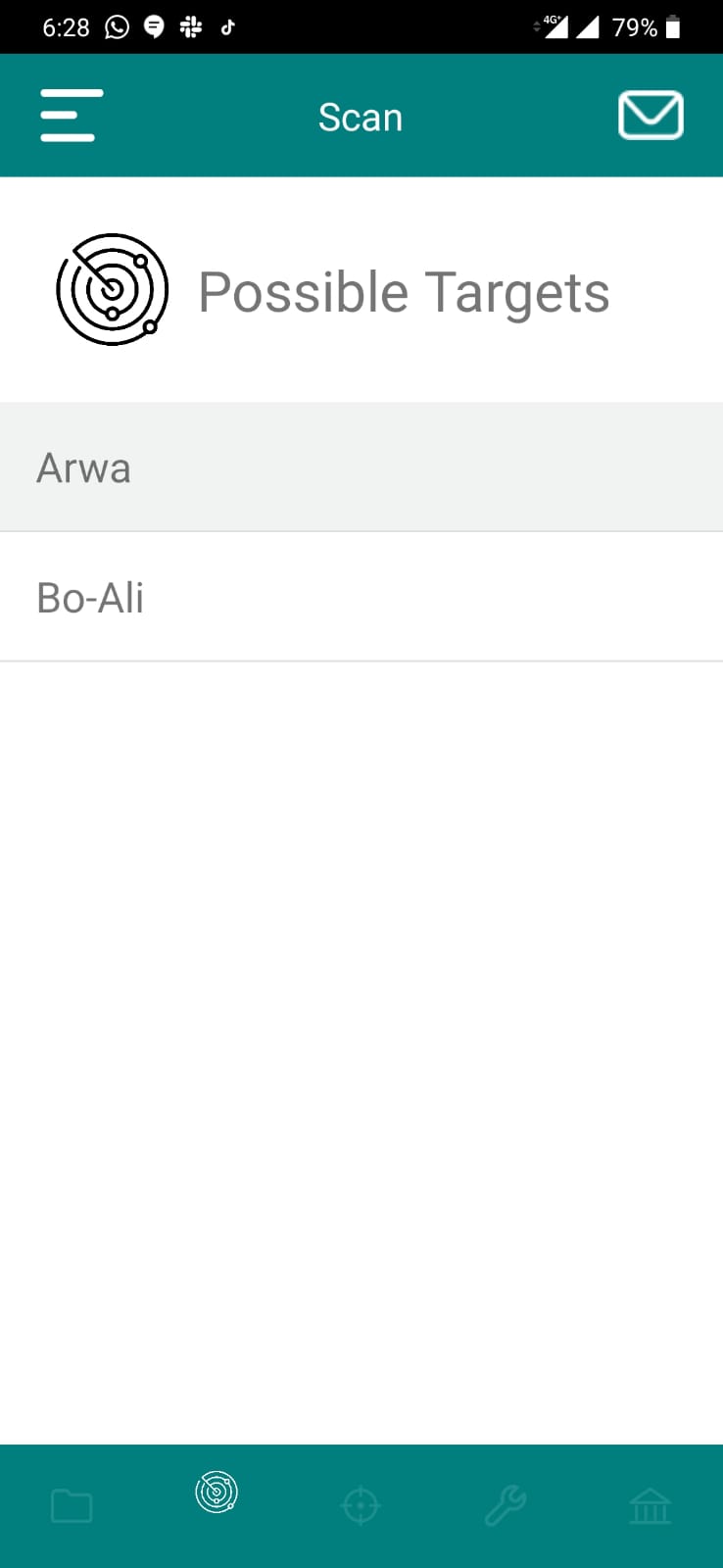
Screenshot 2 Registration

Screenshot 1 Application launch

****

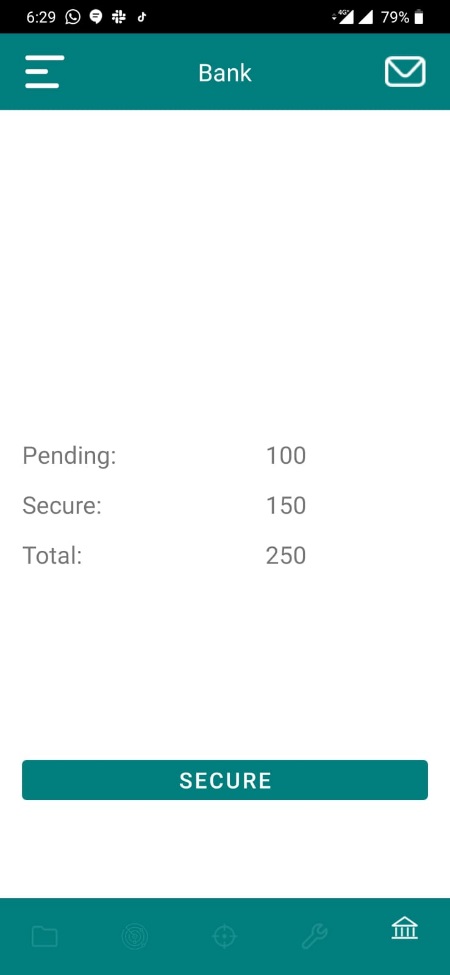
Screenshot 3 Profile

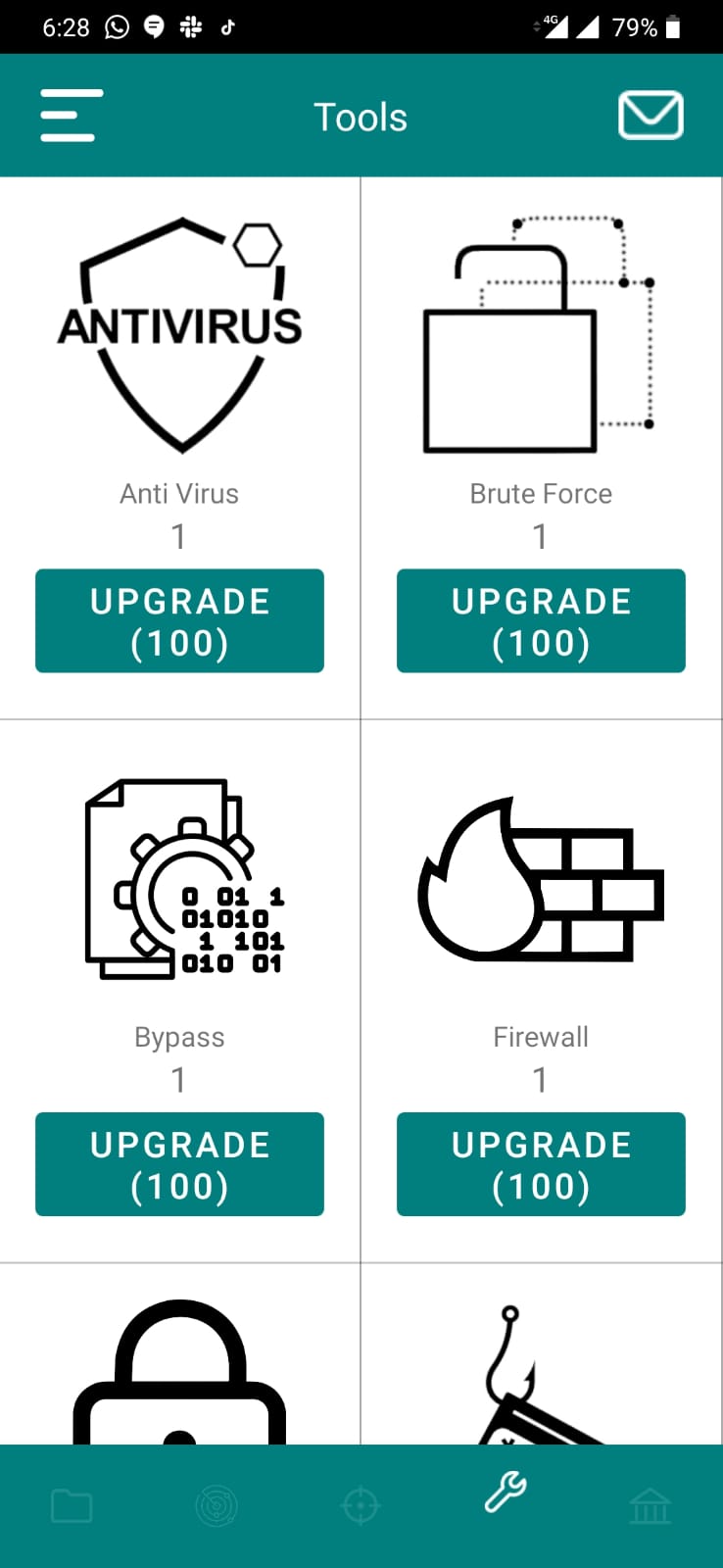
Screenshot 4 Mailbox

****

Screenshot 6 Possible targets

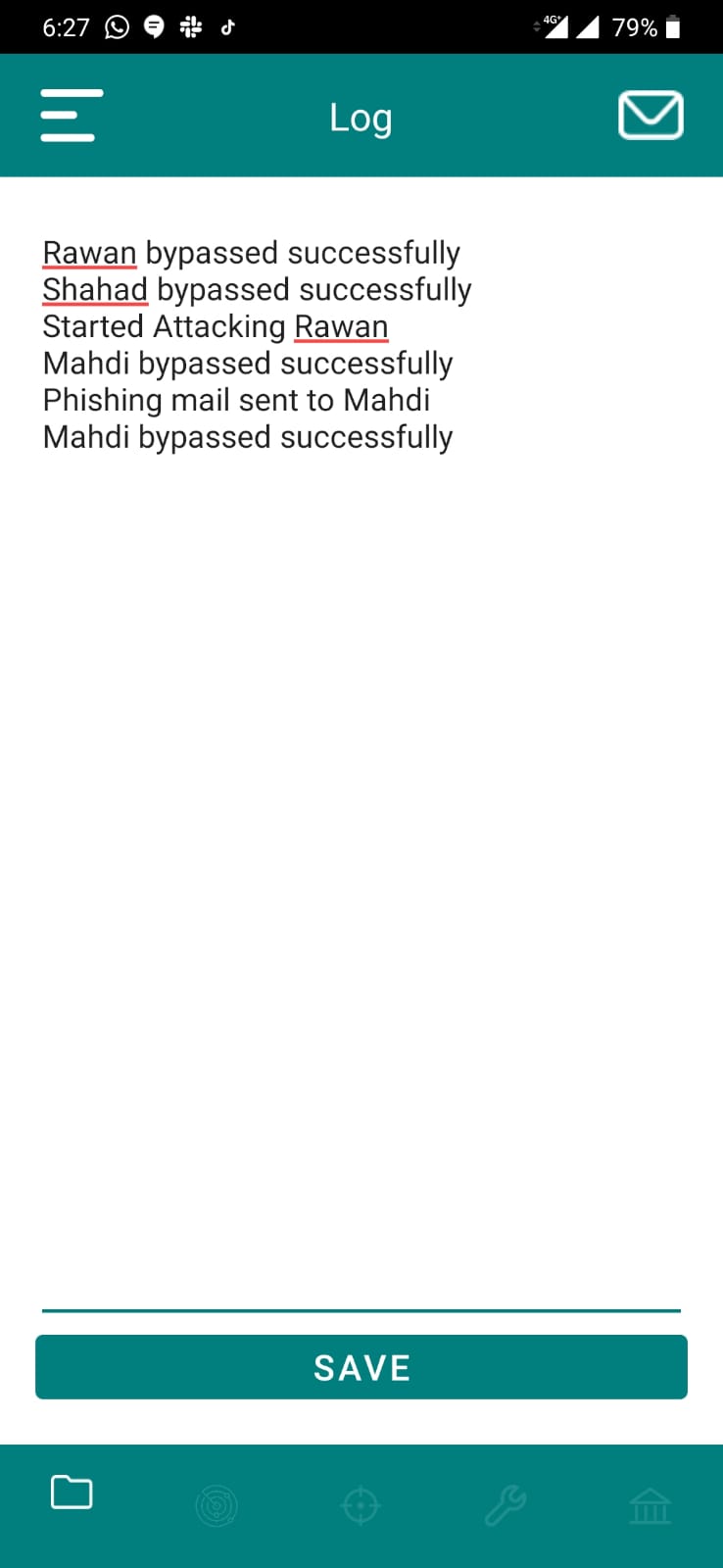
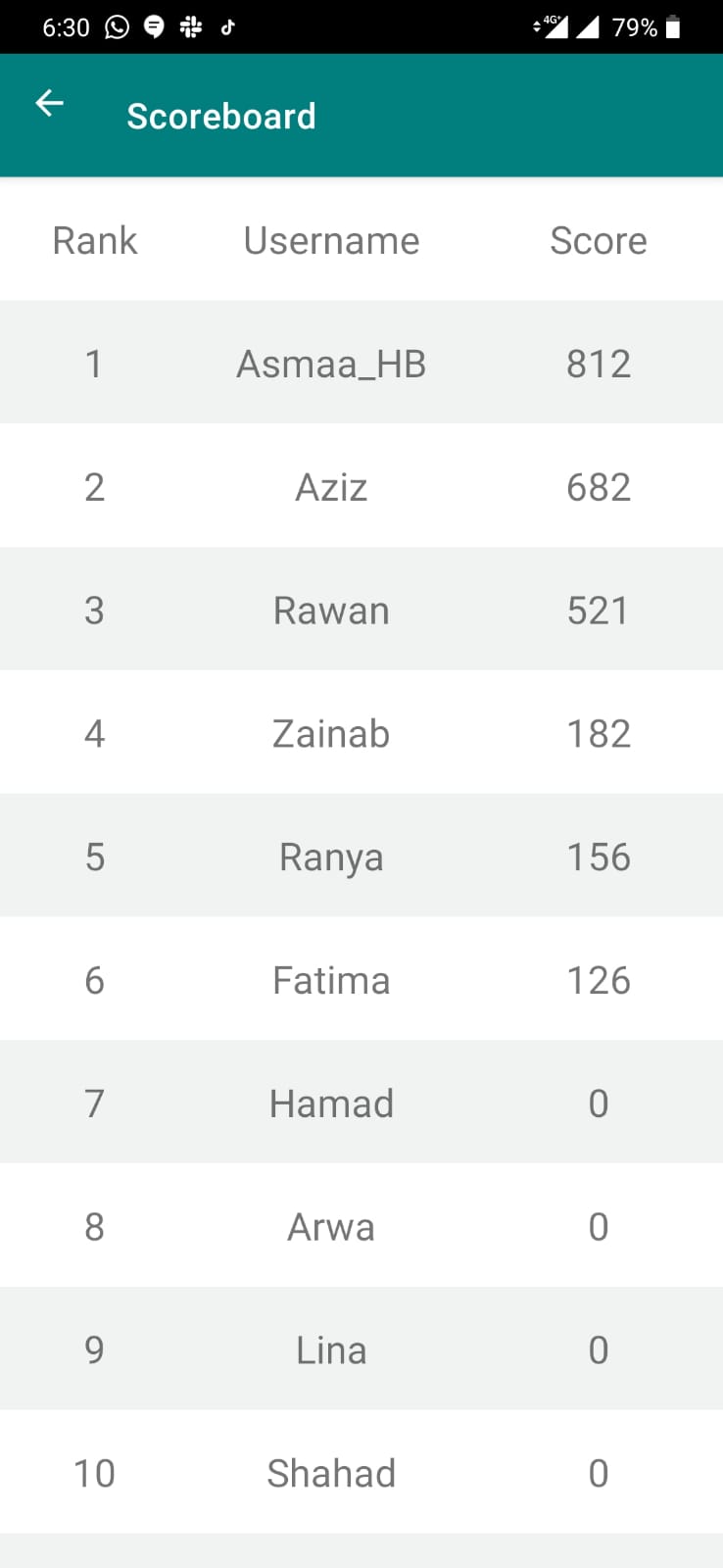
Screenshot 5 Scenario of reviewing phishing email

****

****

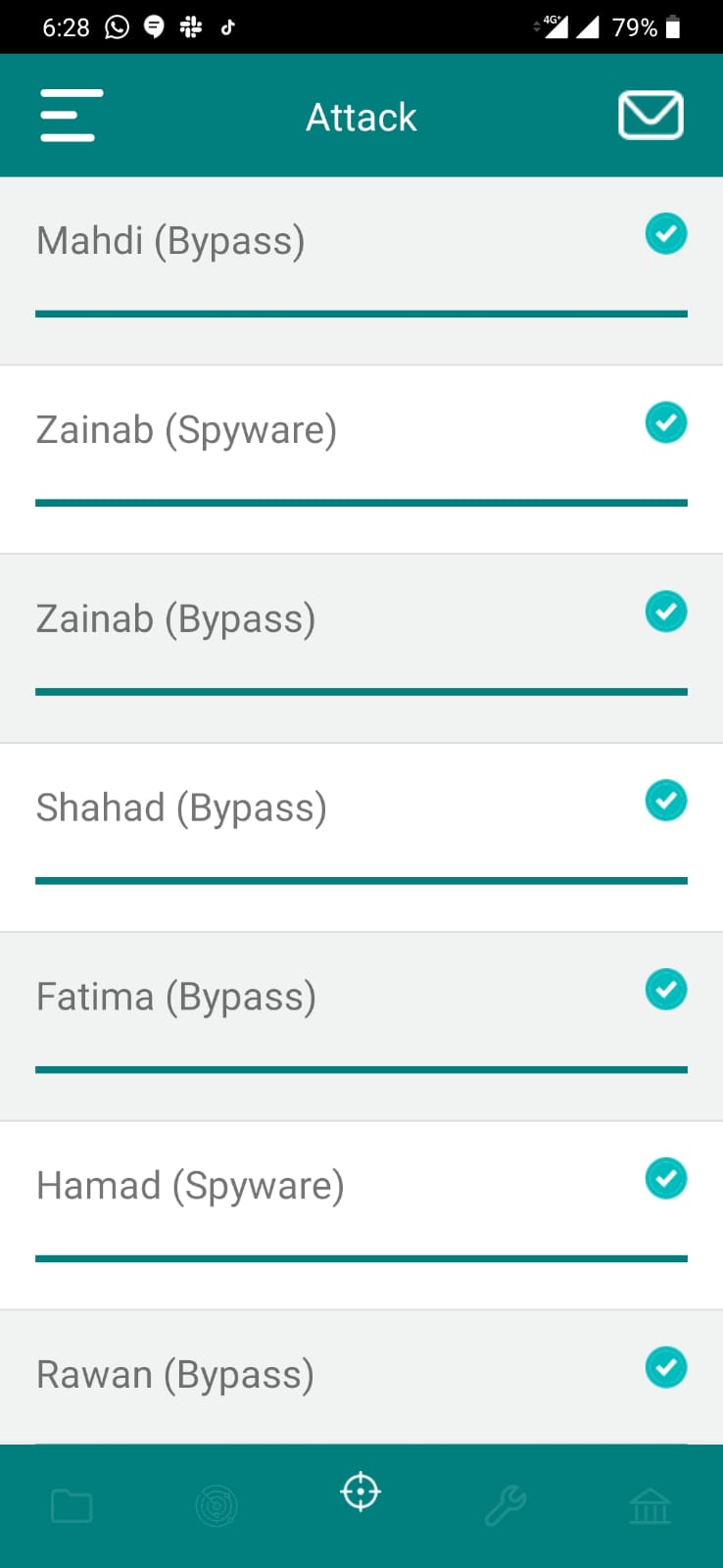
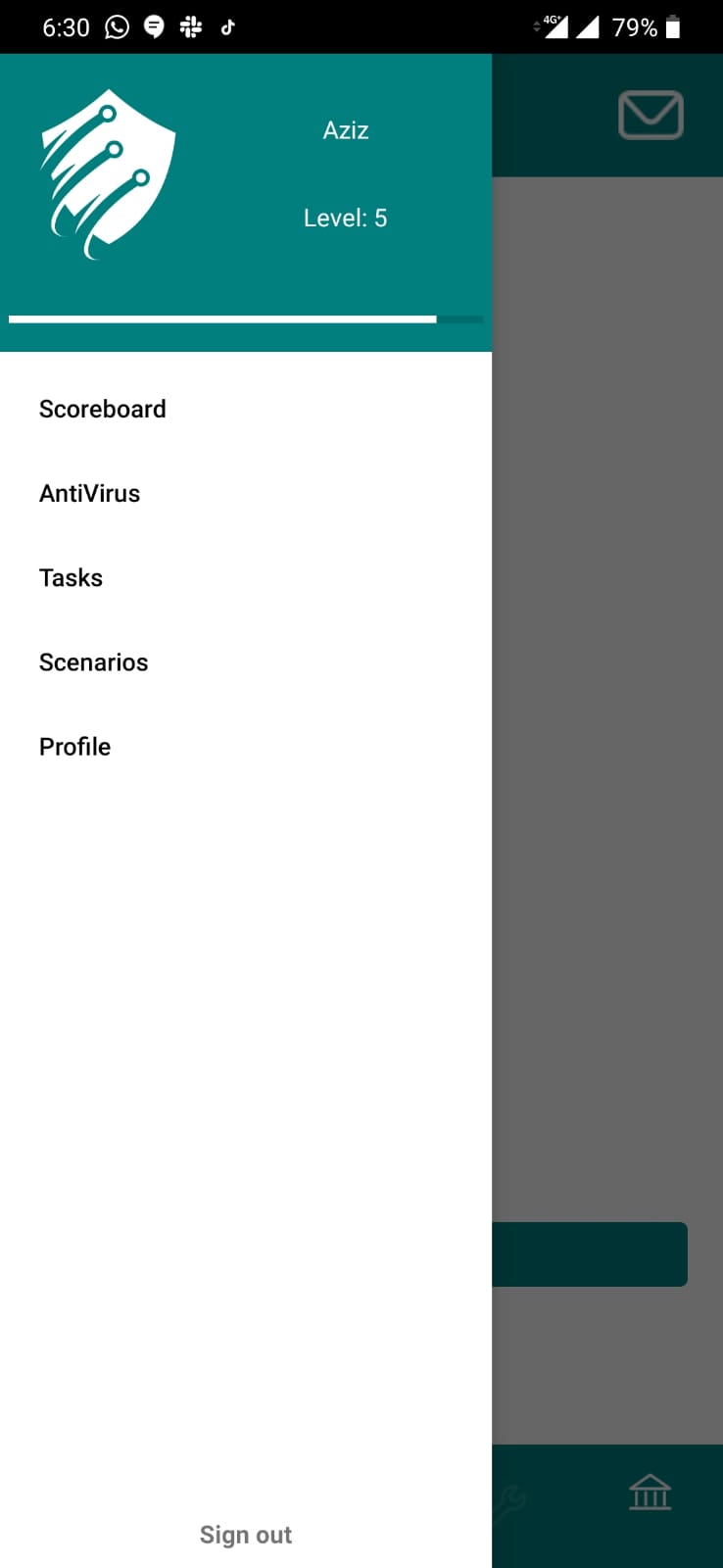
Screenshot 7 Shop for upgrading tools

Screenshot 8 Bank account

****

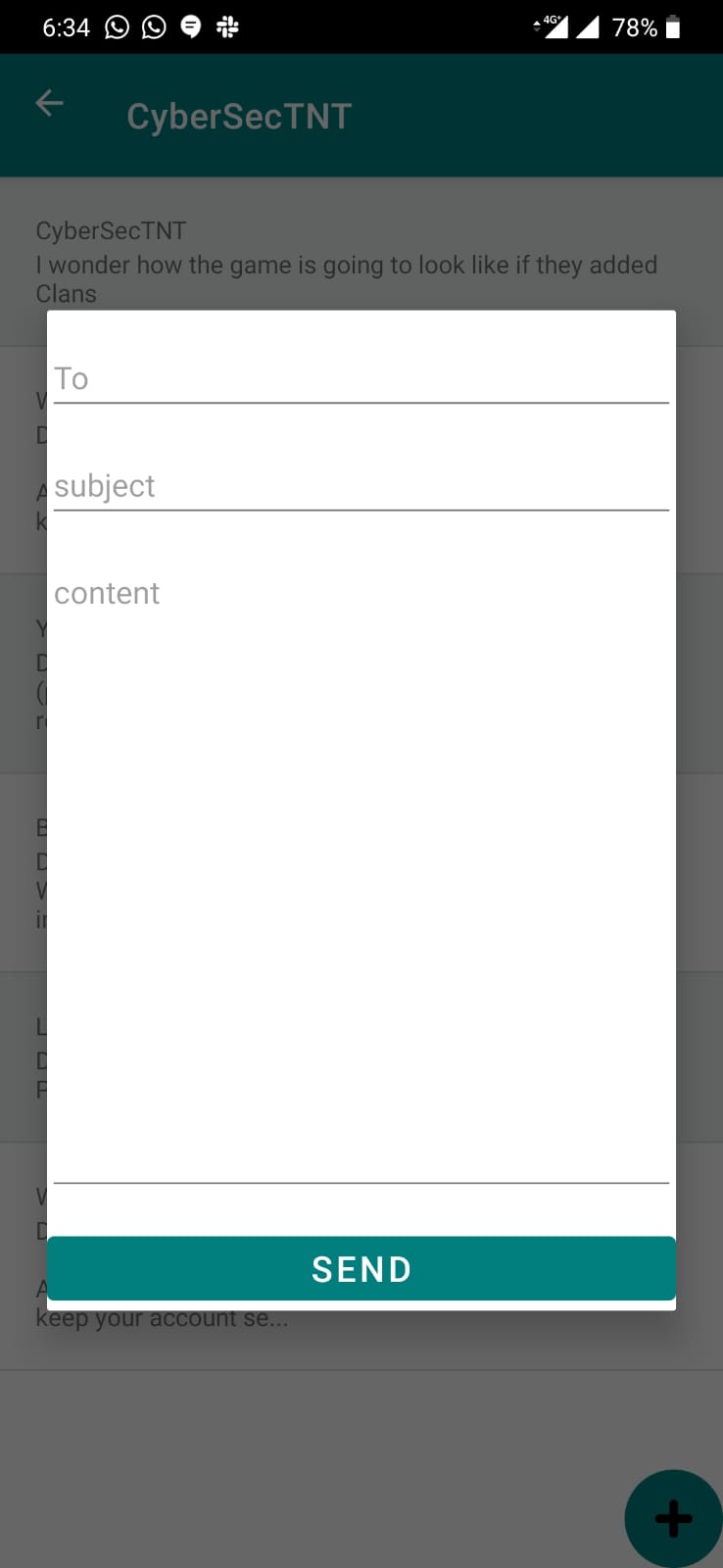
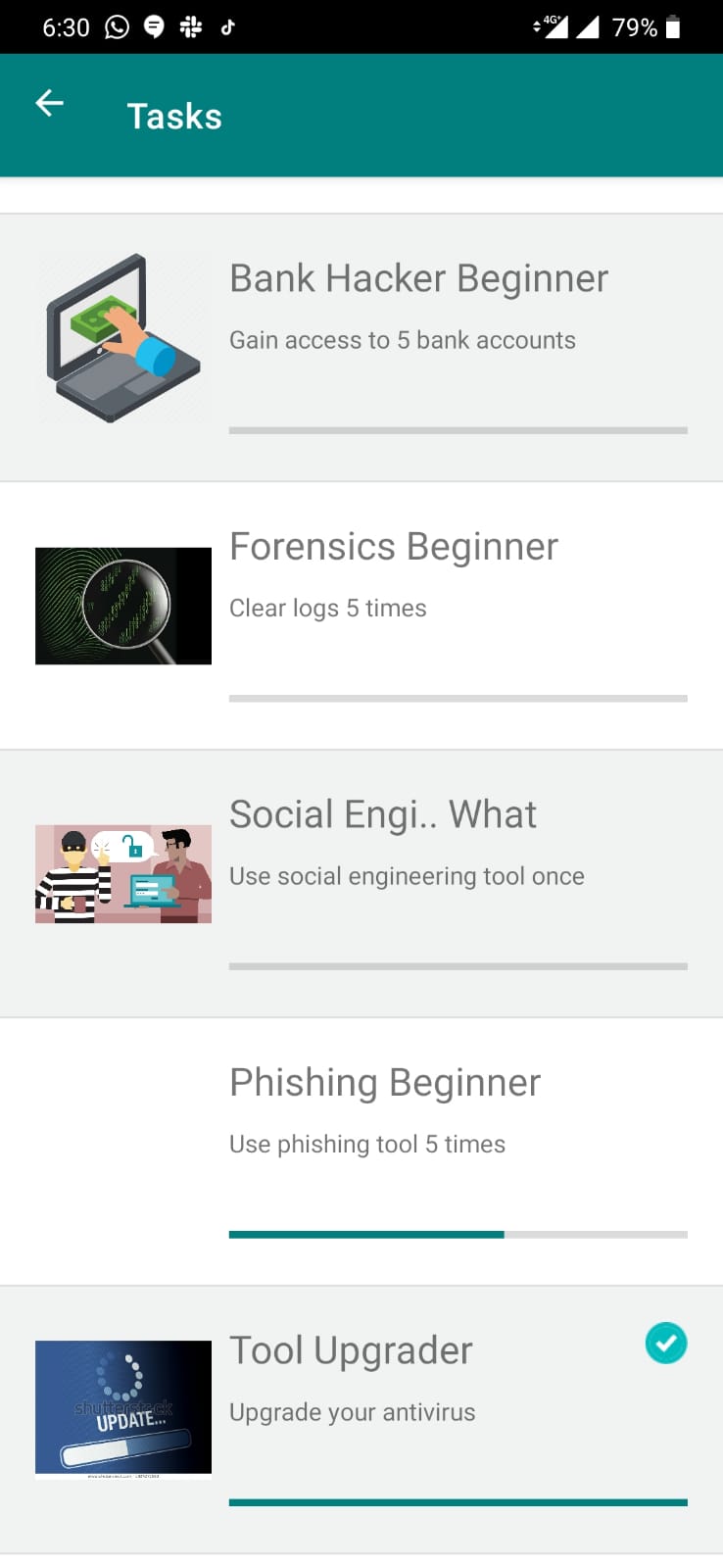
Screenshot 10 Leaderboard

Screenshot 9 Logs

****

Screenshot 12 Settings

Screenshot 11 Attacking timer

****

Screenshot 13 Sending an email

Screenshot 14 Tasks

**5.2 Development Environment:**

**5.2.1 Front end and back end:**

**Front End**

Since we are developing and android application, we are using XML a mark-up language, which defines a set of rules for encoding documents. We are also using CSS which describes HTML elements are to be displayed on screen. Bootstrap was also used which is a CSS Framework for developing responsive and mobile-first websites. JavaScript was also used as a scripting language to implement complex features on web pages.

**Back End**

For our back end we are using JAVA language to code our application. We also use Firebase as a connection between the server and device. Lastly PHP was also used which is a scripting language that is well suited for web development.

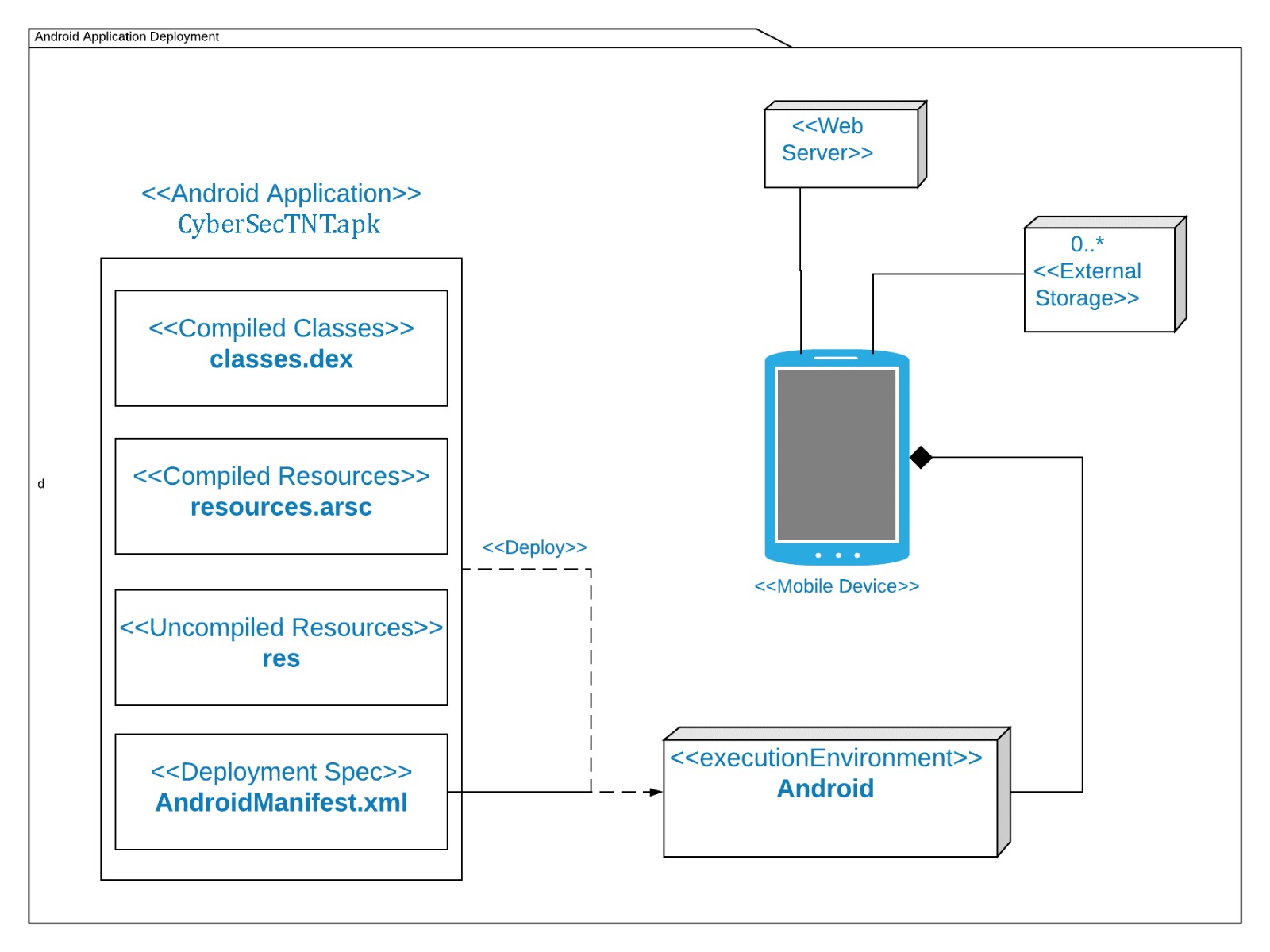
**5.2.2 Deployment Diagram**

Figure 31 Deployment Diagram

**5.3 Testing:**

**5.3.1 Unit Testing:**

We have tested each activity or added fragment before integrating it to our project. Because finding issues prior to the integration can be done more easily since the scope is lower. Also, we tried to improve the efficiency as much as possible before integrating it to our project. Testing each Activity, fragment, layout and other data before integration helped us identifying errors prior to crossing them with other data and fixing them to achieve their goals. Unit testing has been done multiple times in case any enhancements were needed.

**5.3.2 Integration Testing:**

We did our integration testing on multiple phases:

Phase 1: After adding any component to our application we tried to check if any similar algorithms will run in other places within our application. Thus, we created globalVars, which is a class containing the repetitive algorithm to ensure the efficiency and the simplicity of our code This would make maintaining the application and upgrading it easier.

Phase 2: We tried our application on multiple devices and multiple software versions to ensure its compatibility with various devices running on android version 7.0 and above. Also, we tested the network connection and the efficiency of those devices and if any issues might arise because of our application.

Phase 3: We tried to enhance the efficiency of our application after integrating as much as possible to meet the markets level in regards of size, network usage, memory usage and energy usage. The results were as following:

* Memory usage achieved: 10-20 with 60-80 spikes
* Network usage achieved: 5 kb send, and 12 kb receive
* Size of the APK: 10 mb
* Energy usage: Heavy but acceptable

Phase 4: Stress testing was carried on our application, such as running multiple applications in addition to ours, low network speed and on low power mode. Those things had impact as expected on the performance and the usability of the application but enhances were implemented to make running the application in those difficult scenarios possible without issues.

Phase 5: In this phase we focused on trying all the possible scenarios and case in every part of the application and took a look at how the application would react. This phase included people from outside of our team in addition to our team, to try everything the user might do in our application. This phase helped us handling all the exceptions that might occur to our application.

Phase 6: We gave out our application to different kinds of people with different backgrounds (Technical, Non-Technical) and we ensured for our application to deliver simple and fun layout for the users. This phase helped us identifying some of the command the users found difficult to find or understand and enhanced to give a better experience.

**5.4 Implementation Plan**

**Project Implementation Checklist**

|  |  |
| --- | --- |
| Task | Status |
| Initiation | |
| Collect ideas | Completed |
| Research | Completed |
| Risk development | Completed |
| Requirement Gathering | |
| Survey | Completed |
| Add user requirements | Completed |
| Compare with competitors | Completed |
| Design | |
| Map out design | Completed |
| Launch prototype design | Completed |
| Final design | Completed |
| Implementation | |
| Implement prototype | Completed |
| Implement code | Completed |
| Integration | |
| Integrate codes | Completed |
| Testing | |
| Run acceptance testing | Completed |
| Test analysis | Completed |
| Fix tested components | Completed |
| Maintenance | |
| Updates | Ongoing |
| User feedback | Ongoing |

Table 9 Implementation Checklist

**5.5 Recommendations:**

For future works we are planning to add teams/groups into the game were players will be able to play together as a team to become a threat or eliminate a threat. Also, we are planning to add animations into the application and making it more colorful in general. We are also going to be contacting companies and working with them to make the application fit the companies’ style, for example, their database and so on. Furthermore, we want to make our application available for IOS devices. Moreover, we are looking forward to adding an offline mode were users will be playing against “bots” with different difficulties. Finally, we will want to implement machine learning into our application.

**5.6 Brief Manual:**

**How to install:**

The application will be available for installation on Google Play store for our Android users. Windows users can use the CyberSecTNT through application that enable the usage of Android software like BlueStacks.

**How to use:**

Just like any online game as soon as the application is launched the user is asked to either log in or make an account. After account set up is done, they are free to play the game. The user starts off by scanning possible targets and chooses to attack someone through the different attack options available. They can either pass or fail the attack depending on the defender’s tools levels and the attacker’s tools levels. Tools can be upgraded in the store with coins gained from finishing tasks or transferring funds from another user’s bank account after a cyber-attack.

**5.7 Conclusion**

CyberSecTNT is a game with the aim of helping non-technical users get a general idea of how the security in a digital environment can be easily breached. Since the application is aimed at non-technical users it will not be complicated and will give the users a general idea of how breaches happen from both sides, attacking and defending. With how the internet is getting more integrated with our lives by the day it is crucial for people to get educated on how to keep their data safe and that is the aim of our application.

## 

## **5.8 Task Division:**

***Capstone 1:***

|  |  |  |
| --- | --- | --- |
| Name | Student ID | Task |
| AbdulHameed Salama | 33292 | Methodology/Related literature |
| Abdulaziz Karam | 35621 | Technical background/Related literature |
| Mohamad Masoud | 34706 | Introduction/Methodology |
| Anas El-Ghabra | 42531 | Related literature/Methodology |

Table 10 Task division

***Capstone 2:***

|  |  |  |
| --- | --- | --- |
| Name | Student ID | Task |
| AbdulHameed Salama | 33292 | Web development / Testing |
| Abdulaziz Karam | 35621 | UI Design / Integration / Android development / Database / Testing |
| Mohamad Masoud | 34706 | UI Design / Android Development / Testing |
| Anas El-Ghabra | 42531 | Video editing / Android development / Testing / Database |

Table 10 Task division 2

## **Bibliography**

Accenture/Ponemon Institute: The Cost of Cybercrime. (2019). *Network*

*Security*, *2019*(3), 4. doi: 10.1016/s1353-4858(19)30032-7

Aldawood, H., & Skinner, G. (2018). Educating and Raising Awareness on Cyber Security

Social Engineering: A Literature Review. *2018 IEEE International Conference on*

*Teaching, Assessment, and Learning for Engineering (TALE)*. doi:

10.1109/tale.2018.8615162

Aloul, F. A. (2012). The Need for Effective Information Security Awareness. *Journal of*

*Advances in Information Technology*, *3*(3). doi: 10.4304/jait.3.3.176-183

Arts, T. (n.d.). Hackers. Retrieved from https://hackersthegame.com/.

Guess the Password. (n.d.). Retrieved from <http://www.hackbot.robobotstudio.com/>.

HACK OTHER PLAYERS' DEVICES & UPGRADE YOURS IN THIS HIGHLY

ORIGINAL HACKING GAME. (n.d.). Retrieved from <https://hackex.net/>.

Learn to Code by Playing a Game. (n.d.). Retrieved from https://codecombat.com/about.

Peña-Miguel, & Hoyuelos, S. (2013, November 30). Educational Games for Learning.

Retrieved from

<https://eric.ed.gov/?q=Educational+Games+for+Learning&id=EJ1053979>.

Targeted Attack: The Game – Defend your data. Choose wisely. Succeed or fail. (n.d.).

Retrieved from <http://targetedattacks.trendmicro.com/about-the-game.html>.

The Hacking Game. (n.d.). Retrieved from <http://s0urce.io/>.

i273. (n.d.). Ever wanted to be a hacker. Retrieved from http://i273.com/index.html#hackrun.

WebME - The CyberSecurity Game. (n.d.). Retrieved from

<https://play.google.com/store/apps/details?id=com.thunkable.android.mrigankpawagi.WebME&hl=en>.

10 cyber security facts and statistics for 2018. (n.d.). Retrieved from

<https://us.norton.com/internetsecurity-emerging-threats-10-facts-about-todays-cybersecurity-landscape-that-you-should-know.html>.

# Survey

The reason to why we decided to conduct a survey is because it is the simplest and most effective way of reaching out to the community and better understand it. It will help us better predict what people want to see in our application

Survey questions are as follows:

1. Age?
2. Do you know what cyber security is?
3. Would you be interested in using an educational application to learn more about cyber security?
4. Would you like to get educated about the basic techniques to prevent you from being scammed on the internet?
5. How often do you think cyber-attacks occur?
6. How often do you use a strong password?
7. Would you be interested in understanding how real-life cyber-attacks occur?

|  |
| --- |
| *Table 1 Table of surveys*    *Figure 1 Survey question1: To determine the target age group* |
| *Figure 2 Survey question2: To determine subject knowledge of the group* |
| *Figure 3 To determine the user's level of interest in our application* |
| *Figure 4 To determine the impact of our application* |
| *Figure 5 To determine the users awareness of cyber-attacks* |
| *Figure 6 To understand whether people care about being secure or not* |
| *Figure 7To see if people are interested in an application that mirrors real life attacks* |