A MOBILE GAME FOR LEARNING CYBER-ATTACKS AND THEIR PREVENTION

A Paper
Submitted to the Graduate Faculty
of the
North Dakota State University
of Agriculture and Applied Science

By

Piyush Solanki

In Partial Fulfillment of the Requirements
for the Degree of
MASTER OF SCIENCE

Major Department:
Computer Science

November 2022

Fargo, North Dakota

North Dakota State University
Graduate School

Title

A MOBILE GAME FOR LEARNING CYBER-ATTACKS AND THEIR PREVENTION

By

Piyush Solanki

The Supervisory Committee certifies that this ***disquisition*** complies with North Dakota State University's regulations and meets the accepted standards for the degree of

MASTER OF SCIENCE

SUPERVISORY COMMITTEE:

Dr. Kendall E. Nygard
Chair

Dr. Saeed Salem

Dr. Ronald Degges

Approved:

December 6, 2022	Dr. Simone Ludwig
Date	Department Chair

ABSTRACT

This paper's primary goal is to use Bloom's Revised Taxonomy educational objectives in creating Cyber Air-Attack. It's a game that teaches fundamental concepts about cybersecurity. Because it simplifies and makes learning simple, the course material was designed with Bloom's Revised Taxonomy. This taxonomy divides the course material into increasing levels of complexity, with the basics being the most basic and the advanced being the most complex. We reviewed all literature to understand the area of research and identify any gaps in previous research.

Cyber Air-Attack targets amateur computer users. They will be taught about cybersecurity basics, cyber threats, and countermeasures. This paper will teach you how to identify and prevent cyberattacks.

ACKNOWLEDGEMENTS

My sincere gratitude to Dr. Kendall E. Nygard, my advisor and chairperson of the graduate committee. He believed in me and gave me the chance to complete my North Dakota State University degree. It was a great help to have your support and guidance during the research project as well as for coursework. I want to thank Dr. Saeed Salem and Dr. Ronald Degges from my committee for their invaluable guidance and supportive comments.

My parents are my greatest source of support and encouragement. Finally, I want to thank my friends, particularly Tejas Solapurkar, Jagjot Bhardwaj, and my wife Sudarshna Jadon for their support and love.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1. INTRODUCTION

1.1. Overview

In recent years, ICT (Information Technology and Communications) has made our lives easier and more productive. With a global penetration rate at 62.5%, cybersecurity has seen dramatic changes in the last two years. Cybercriminals have learned to adapt to these changes and can now tailor their strategies to the new realities. (CheckPoint, 2022)

A report (Hunt, 2022) reveals that many companies have failed to prepare for the rapid transition to the cloud. They logged in through unsecured networks, or their home computers, which increased their vulnerability to attacks. Security gaps that are obvious, such as passwords that never expire and folders containing sensitive information accessible to all employees, can increase the risk exponentially.

So, cybersecurity is the biggest challenge facing private companies, government agencies, as well as individuals.

Cybersecurity protects web-connected systems such as data, software, and hardware against cyber-attacks. Ransomware and cookie attacks, as well as denial-of service are all examples of cyber-attacks. Most often, the cyber-attack is used to steal financial information from individuals and businesses.

In the recent past, cyber-attacks continues to grow and are expected to double up by 2025 (Mclean, 2023). There severity and impact on organizations is indicated by the following statistics:

- Surfshark reports that in 2021 there were 212.4 million users affected, compared to 174.4 million in 2020. (Surfshark, 2023)
- Ransomware is the most common form of cyber-attack in healthcare.

- A data threat report published in 2022 stated that almost half (45%) of US companies were affected by a data breach within the last year. (Thales Group, 2022)
- According to KPMG's 2022 outlook on fraud (KPMG, 2022), 62% of American companies experienced a cyber-attack or data breach in 2021.
- The Data Breach Investigations Report (Basset et al., 2020) was based on more than 157,525 security incidents and over 3,950 data breaches.
- Ransomware attacks, which hold files and systems hostage, pose a serious threat to data security. The Symantec Security Summary (Stackpole, 2021) shows that ransomware payments rose 171% between 2020 and 2020. The highest payout was $10 million.
- The Data Breach Report (IBM, 2021) revealed that 2021 was the year with the highest data breach cost in 17 years. It rose from $3.86 million in 2020 to $4.24 million in 2021.

Cyber-attacks often occur because of ignorance or lack of awareness. Hackers will continue to develop new technologies and techniques to conduct different types of cyberattacks. It is essential to be educated and learn about cyber-attacks to protect yourself.

1.2. Background and Problem Statement

Cloud services are increasingly popular in today's digital age where everyone wants to be connected online. Cloud sharing has made it easier for hackers to steal data. Security threats are also faced by small and medium-sized companies when it comes protecting their data. Everyone needs to be aware of the possible cyber-attacks that they could be exposed to, and what preventative steps they can take to avoid being a victim to any type.

To prevent cyber-attacks, it is crucial to be well-informed and familiar with countermeasures. Learning cybersecurity can be difficult for both the learner and teacher. Despite the wealth of information available on the Internet about cyber security and the measures it takes, it is still difficult to grasp the basics of cybersecurity education.

Cybersecurity can be learned in many ways. Each method has its advantages and disadvantages. In this digital age, books seem obsolete. Online and mobile apps offer better learning experiences thanks to the development of technology (Gillis, 2022). The tech-enabled reading process isn't engaging students. Interactive learning is crucial to assist students in their learning. This can be used to help students learn how to use the internet quickly.

1.3. Objectives

The problem statement outlines the issue of cybersecurity teaching methods. Without understanding the basics of cybersecurity, it is difficult to grasp complex concepts. It is necessary to find a better teaching method than traditional classroom methods that can teach fundamental concepts of cybersecurity.

In this paper, we designed an interactive, yet informative game named as Cyber Air-Attack that teaches fundamental cybersecurity concepts using Bloom's Revised Taxonomy. Cyber Air-Attack was designed and developed so that it meets the learning objectives. It incorporates the 'Remember' level and 'Understand" levels of Bloom's Revised Taxonomy. This game's main objective is to teach you the following cybersecurity concepts.

- Firewalls and Antivirus are important
- How to avoid Phishing Email
- Strong Passwords are important
- How to avoid Spyware and Adware attacks

1.4. Structure of Paper

The chapters in the paper are organized as follows:

- Chapter 2 describes the Definition of Games, and their Importance in Learning Cybersecurity.
- Chapter 3 provides an overview of the original Bloom's Taxonomy learning goals and a detailed introduction to the levels in Revised Bloom’s Taxonomy.
- Chapter 4 demonstrates how the Remember level of the revised Bloom’s taxonomy, the first cognitive level can be combined with tutorial learning material.
- Chapter 5 demonstrates how the Understand level of the revised Bloom’s taxonomy, the second cognitive level can be integrated with tutorial learning material.
- The conclusions and limitations of the work are presented in Chapter 6. It also contains a recommendation for future research.

2. IMPORTANCE OF GAMES IN LEARNING CYBERSECURITY

There are many methods for training, including face-to-face exercises and workshops, posters and newsletters on paper, online videos, and computer-based training (Abawajy, 2014). To make learning more engaging, fun, and challenging, it is important to have a variety of activities. Simulations and games have been accepted more widely as powerful teaching tools. They could lead to an "instructional revolution".

Let's first define what a game is before we move on. A game is an interactive voluntary activity in which one or more people follow rules to constrain their behavior. This creates artificial conflict and results in a quantifiable outcome (Esposito, 2005). (Rollings and Adams, 2003) identifies eight types of games: strategy, role-playing, action, sport, vehicle simulation, management, construction, adventure, artificial life, and puzzle games. We will be focusing on strategy games, also known as serious or tactical games.

Serious Games are games that serve a higher purpose than entertainment (Chiniara, 2019).These games are an essential topic in the field of educational technology. It is not a new idea to use serious games in education. Video games were first introduced in the United States of America in the 1960s for military and medical schools as well as the general academic community (Bergeron, 2006). (Annetta, 2008), reports that there has been a growing interest in videogames for educational purposes.

The idea that a game can be used to teach is because it motivates the user and provides immediate feedback. Although there are some creative solutions, traditional teaching methods are still valued in school systems. The games are viewed as entertainment and play, not as tools that can be used to teach.

Gamification is a way to transform content from a lecture or e-learning course into a game-based learning experience. This can be in the form either of a full-fledged educational video, a game that adds game elements to normal tasks, such as running for exercise, or a classroom experience in which learners take part in a story-based challenge to master the content (Zamzami et al., 2020). Gamification allows for a clearer identification of cause and effect. Cyber threats can have devastating effects, such as financial loss and identity theft. They are most often caused by ignorance about cybersecurity. This can be easily explained by a game, as the player will need to make decisions based upon his/her cybersecurity knowledge. Different outcomes could result in different levels of success.

Games can be used to enhance students' social skills and help them solve problems. There is no doubt that games have the potential to teach cybersecurity. Education using games should be encouraged and implemented in current education systems.

3. LEARNING THROUGH TAXONOMY PRINCIPLES

Interactive serious games can be a powerful tool to teach internet users the importance of cybersecurity. To teach users how to be safe in a world full of cyber attackers, it is essential to provide a practice environment. Instructional design learning objectives must be used to encourage and engage users in learning about cyber-attacks and countermeasures. To help define the structure and design of the game, it should include a learning taxonomy.

When designing learning objectives for a course, it is important to consider what kind of work students should do to show that they have achieved the course objective. Educational taxonomies can be used to develop learning objectives and assess student achievement. A taxonomy refers to a system of classification that has been ordered in some manner.

Research has been extensive on various taxonomies. There are many learning taxonomies available, including SOLO (Structure of observed Learning Outcomes), Finks Taxonomy and Bloom's Taxonomy. Bloom's Taxonomy, which was first proposed by educators led by Benjamin Bloom in 1956 (Krathwohl, 2002) is the most widely used learning taxonomy.

3.1. Bloom’s Taxonomy

Bloom's Taxonomy identifies intelligence levels. This includes learning, thinking, and understanding. (Bloom et al., 1956)

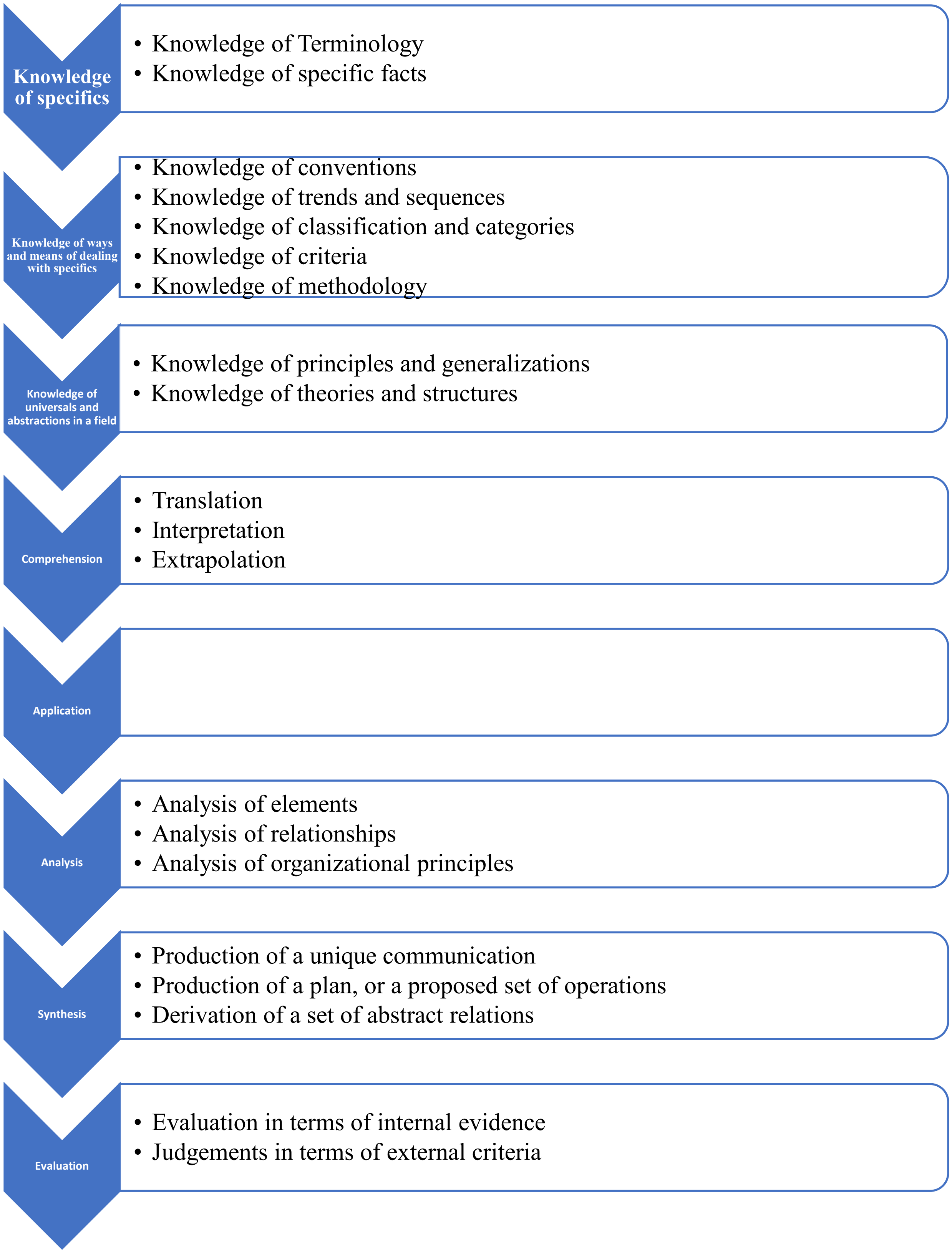
This learning taxonomy was created to help students analyze and evaluate concepts, processes, and principles, rather than memorizing facts. It is most used when creating educational, training, or learning processes. It can also be used in the creation of educational computer games.

The taxonomy is based on the three domains of learning. The committee identified three domains of learning and educational activities (Bloom et al., 1956)

- Cognitive: mental Skills (*Knowledge*).
- Emotional: growth of emotions or feelings (*attitude, or self*).
- Psychometer manual or physical skills *(skills).*

3.1.1. Cognitive Domain

Cognitive domain is knowledge and development of intellectual skills (Bloom et al., 1956). Six levels can be broken down into the cognitive domain, from the most basic to complex. Figure 1 illustrates the entire structure of the cognitive domain.



Knowledge of specifics

- Knowledge of Terminology
- Knowledge of specific facts

Knowledge of ways and means of dealing with specifics

- Knowledge of conventions
- Knowledge of trends and sequences
- Knowledge of classification and categories
- Knowledge of criteria
- Knowledge of methodology

Knowledge of universals and abstractions in a field

- Knowledge of principles and generalizations
- Knowledge of theories and structures

Comprehension

- Translation
- Interpretation
- Extrapolation

Application

Analysis

- Analysis of elements
- Analysis of relationships
- Analysis of organizational principles

Synthesis

- Production of a unique communication
- Production of a plan, or a proposed set of operations
- Derivation of a set of abstract relations

Evaluation

- Evaluation in terms of internal evidence
- Judgements in terms of external criteria

Figure 1: The Original Taxonomy

Sub-categories were created for all levels, except the application. The levels are listed in Table 1.

Table 1: The Original Bloom's Taxonomy

Level	Description
Knowledge	To recall or retrieve material previously learned
Comprehension	To understand and construct meaning from material
Application	To be able either to use learned material or to apply material to new and concrete settings
Analysis	To be able classify and distinguish the parts of material by its structure of organization. This will aid in understanding the material
Synthesis	To be able combine components to create a new, coherent whole
Evaluation	To be able judge, review, and even criticize the material value of a given objective

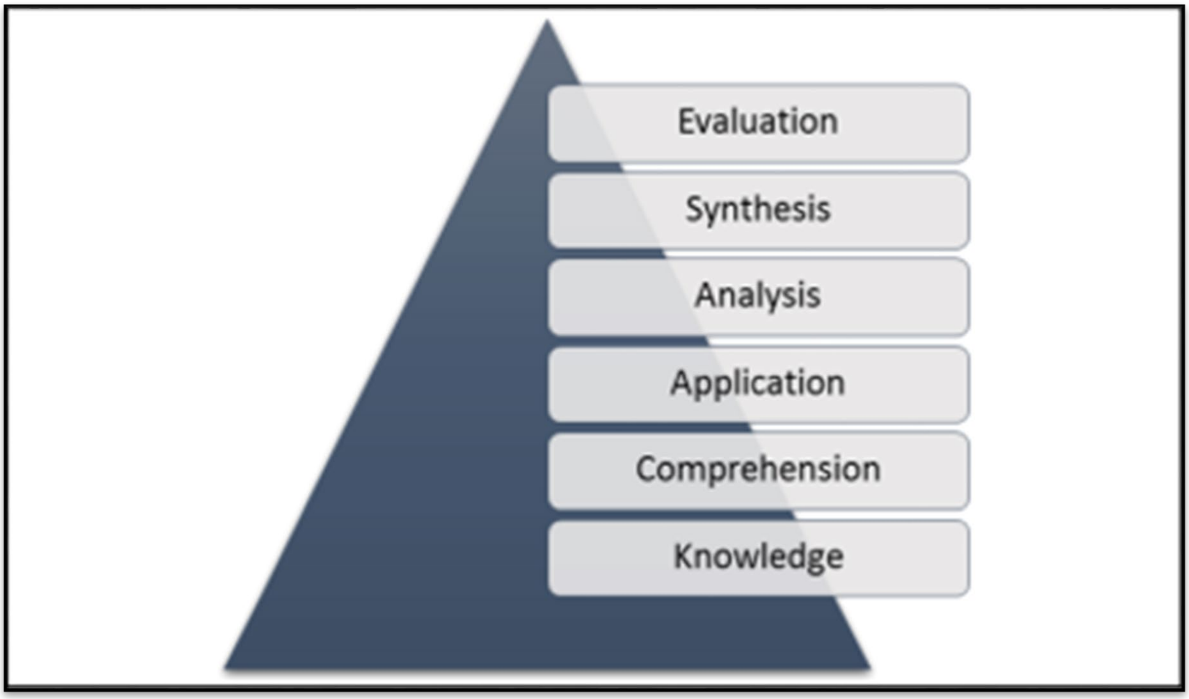


Figure 2: The Original Bloom's Taxonomy

Figure 2 illustrates Bloom's Taxonomy graphically. It is unidimensional in nature. Researchers, teachers, curriculum designers, and assessment writers have all used the original taxonomy. It was subject to significant revision due to criticism. The design of the taxonomy was based on the 1950 classroom environment and educational environment. (Krathwohl, 2002) found that Bloom's Taxonomy was not perfect. One weakness is the assumption that cognitive processes can be arranged in a single dimension, from simple behavior to complex behavior (Furst, 1994). One reason was to include the latest developments in psychological and educational literature. The original taxonomy was primarily based on school curriculum and instruction. These flaws were addressed by Bloom's Original Taxonomy.

3.2. Revised Bloom’s Taxonomy

Lorin Anderson, a former Bloom's student, and David R. Krathwohl, along with a group psychologist, reviewed the Original Bloom’s taxonomy and named as Revised Bloom’s Taxonomy (Krathwohl, 2002). Many changes have been made to the revised taxonomy in terms of structure, terminology, and assumption.

3.2.1. Changes in Terminology

When revised, The Bloom's Original Taxonomy experienced many terminological changes. There were four major terminology changes that took place:

- Six cognitive categories were renamed from nouns to verbs.
- Verbs were used to replace the sub-categories in six of the major categories. (e.g., interpreting, exemplifying, inferring, etc.)
- In terms of thinking, the knowledge dimension was deemed inappropriate. The knowledge domain sub-categories were reframed to categorize knowledge domain in four parts: Factual, conceptual, and procedural knowledge.
- The new title for comprehension was understanding, while synthesis was renamed as creating.

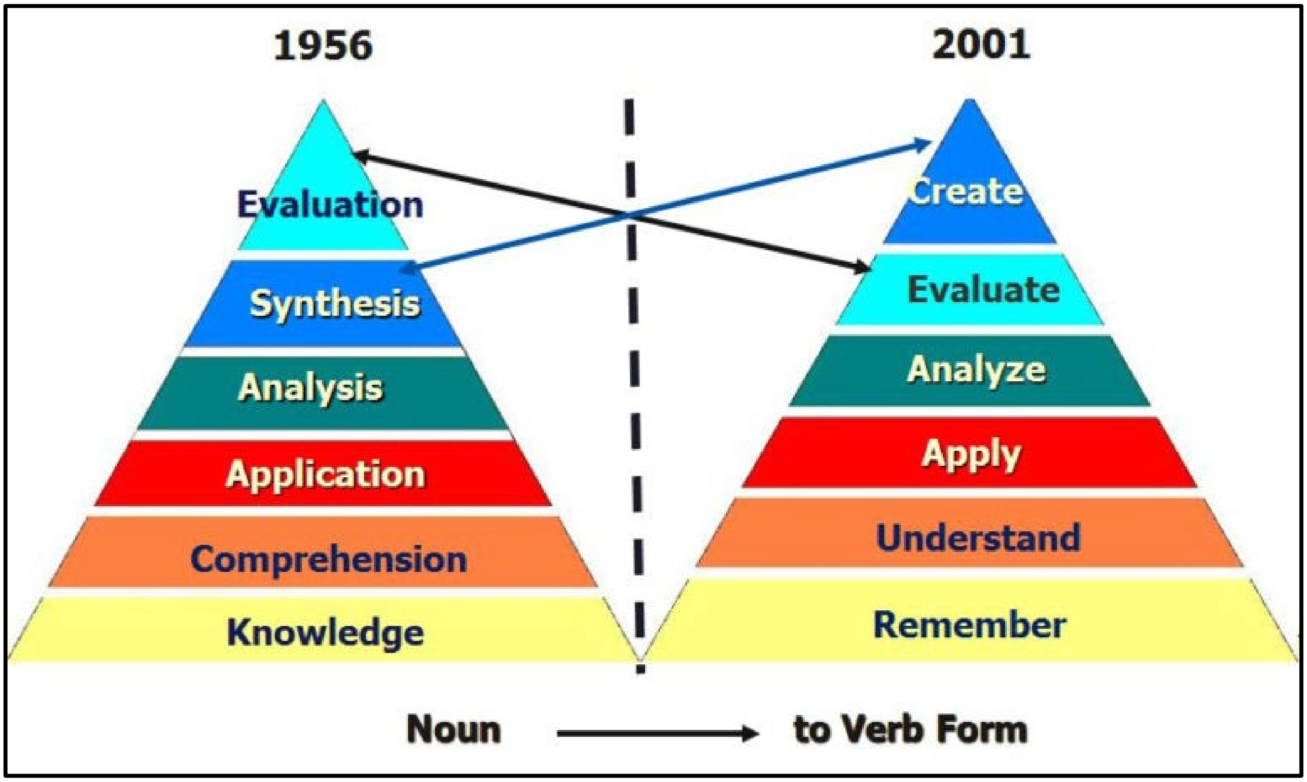


Figure 3: Comparison between Original and Revised Bloom's Taxonomy.

3.2.2. Changes in Structure

The most important change in the revised taxonomy is the structure. Original taxonomy was a one-dimensional structure. Knowledge was described in verb aspect. Sub-categories were the noun aspects. This resulted in an anomaly within the unidimensional framework as the knowledge domain was dual-natured.

From the revised taxonomy, the two-dimensional table was made. The revised taxonomy removed this anomaly. Separate dimensions were permitted for the noun and verb. The cognitive process dimension is based on the noun, while knowledge is provided by the verb (Krathwohl, 2002).

Table 2: Structure of Revised Bloom's Taxonomy

Knowledge Dimension	**Cognitive Process Dimension**					
	Remember	Understand	Apply	Analyze	Evaluate	Create
Factual Knowledge						
Conceptual Knowledge						
Procedural Knowledge						
Meta-Cognitive Knowledge						

The table shows that the knowledge domain, which is a distinct dimension, forms the vertical axis with its four levels. The cognitive process dimension forms the horizontal axis with six levels.

3.2.2.1. The Cognitive Dimension

There are six levels in the cognitive dimension.

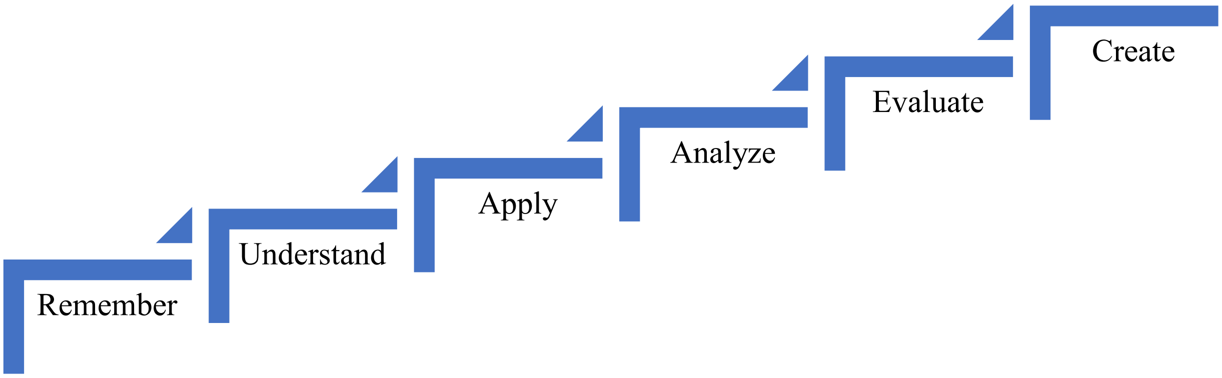


Figure 4: Six Levels of Cognitive Dimension.

3.2.2.2. The Knowledge Dimension

There are four categories in the knowledge dimension which were later sub-categorized.

Factual Knowledge - These are the basic elements that all learners need to know to understand a discipline and solve problems within it.

Conceptual and Procedural Knowledge - It is the interrelationships between basic elements in a larger structure which allows them to work together.

Metacognitive Knowledge - Both knowledge and awareness of cognition can be combined with knowledge and understanding of one's own cognition.

4. COMPRISING THE GAME WITH REMEMBER LEVEL

The 'Remember' level of Bloom's Revised Taxonomy is the highest or, as we prefer, the lowest in the cognitive distribution techniques. This dimension can be subdivided into *Recognizing* or *Remembering*. "Recognizing" refers to the act of locating or identifying knowledge in a long-term memory that is consistent with the present memory. "Recalling" refers to retrieving relevant knowledge from long-term memories.

This level's learning outcome is that the learner should be capable of finding knowledge consistent with the current material in long-term memories and retrieving relevant information from long term memory. (Mayer, 2002). This level of course design can be achieved using the following technologies: flash cards, book marking, flashcards, rote learning based upon repetition and reading. We tried to include both conceptual and factual knowledge to help the 'Remember' level in the paper. Taxonomy matrix of the 'Remember' level is shown in Table 3.

Table 3: Taxonomy Table for Remember Level

Knowledge Dimension	**Cognitive Process Dimension**					
	Remember	Understand	Apply	Analyze	Evaluate	Create
Factual Knowledge	*X*					
Conceptual Knowledge	*X*					
Procedural Knowledge						
Meta-Cognitive Knowledge						

The basic elements of the course are what define fact knowledge. The game design has a start menu page with an info icon. The info icon leads to a document that contains information about all icons used in the game. Different icons can be used to signify different enemies or allies. The information document contains all the definitions of icons and information that learners need to reach the 'Remember" level in the factual knowledge domain. The game requires that players have some basic knowledge about the icons they see. The player will be kicked off the game if they hit the wrong icon. This forces them to learn more about these icons. The icons are taught to the learners and then they can be used in the game. They also use their memories to recall the icons.

Conceptual knowledge can be defined as the interrelationship between the basic elements of the larger structure. This domain is the focus of the game. Through the information page, the player will be able to learn more about the icons used in this game. As the icons are introduced into the real world, the concepts will be tested. This activity will help the player to attain the conceptual knowledge at the 'Remember' level. This game's success depends on the player's knowledge of the icons. To learn about the icons, the player must refer to the Info icon. Then, they will need to memorize this information during the game. The game design can help players reach the Remember Level in the cognitive domain.

5. COMPRISING THE GAME WITH UNDERSTAND LEVEL

The 'Understand level is the second level in Bloom's Revised Taxonomy's cognitive distribution of techniques. This level helps to understand the written and spoken instructions. This level covers activities such as summarizing, explaining, exemplifying, and interpreting.

According to the two-dimensional Bloom model, this game incorporates the level in relation to both the 'Factual and 'Conceptual levels of the knowledge domain, shown in Table 4 below.

Table 4: Taxonomy Table for Understand Level

Knowledge Dimension	**Cognitive Process Dimension**					
	Remember	Understand	Apply	Analyze	Evaluate	Create
Factual Knowledge		*X*				
Conceptual Knowledge		*X*				
Procedural Knowledge						
Meta-Cognitive Knowledge						

Understand + Factual is a summary of the features of the game. **Understand+ Conceptual** describes how to classify the characters of the game, which is the main purpose for designing the game. The info icon contains relevant information that is related to the game scenarios. The 'Understand level provides the player with basic information using graphics, images, and text. The player can use the information to make sense of it and then apply it in real-world situations. The Info icon allows the player to quickly make decisions within the game. The game design can incorporate the "Understand" level.

6. THE SOFTWARE DESIGN AND FUNCTIONALITY

This chapter contains details about the design and tools used for Cyber-Attack game. Cyber Air-Attack covers many cybersecurity concepts but focuses mainly on the most fundamental. This game teaches cybersecurity interactively by using Bloom's Revised Taxonomy. It is intended for a broad range of users. The game plot is built around different cyberattack types. There are 18 types, and 10 countermeasures to combat them. Cookies, DNS tunneling, and eavesdropping are all examples of cyber-attacks. There are also email spam, identity spoofing and malware. Phishing attack, Ransomware, ransomware, spyware as well as zero-day exploit attacks. Cyber-Air Attack lets you control the plane using your touch input. As your power up, you must avoid the attacks and blast the right attack. To counter cyber-attacks, there are 10 power-ups available in the game: anti-virus and two-factor authentication, malware, Trojan antivirus, DNS Firewall (SSL), code encryption, data protection, firewall, SSL, code security, data protection, firewall. A tutorial icon is located on the game menu. It shows the player the various power-ups available and the enemies that can be defeated by them.

The plane is controlled by the player. His/her primary objective is to destroy the counterattack and save the plane. This game has endless levels. Your success can be measured by how many attacks you have successfully destroyed.

6.1. The Software Design

6.1.1. Game Plan Basic Concepts

The steps to play the Game (on Android application on a smart phone) are:

- Start the game
- Power up with a counter measure

- Move the Airplane arrow by touch input to collide with the correct attack to destroy them and avoid incorrect attacks
- Show the score increase live on top of the screen when a correct attack is destroyed
- The game will end if the player is possessing a counter measure power and colloid with the incorrect attack

6.1.2. Description

This Game has a two-Dimensional endless runtime play. The player's character will always be in the same vertical position, but the attacks and the screen scene will move downwards. The player's character should be able to either kill or avoid the attacks depending upon the power up (Counter measure).

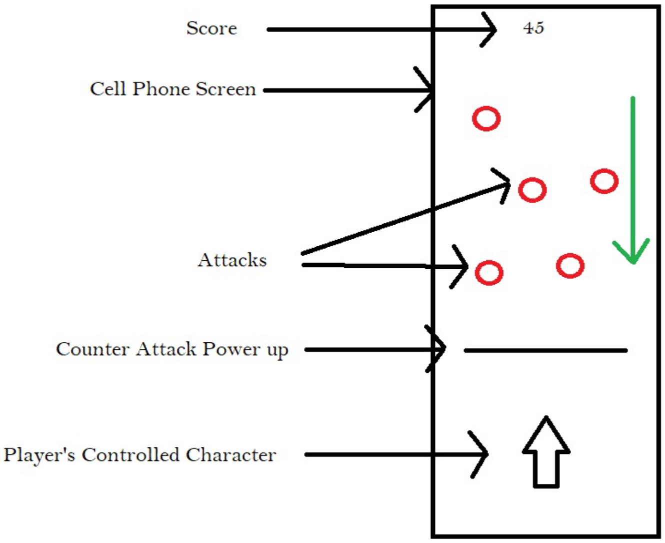


Figure 5: Game Schematic Diagram

6.2. Analysis and Design

6.2.1. Actors

In Software engineering, an actor specifies a role performed by a user or another system that interacts with the system. We have 2 actors in this Software project, the player, and the developer. They are different from each other in just a manner that a developer has ability to debug the game and is allowed to do modifications and extensions to the game.

6.2.2. Use Cases

A Use Case diagram depicts the sequence of interactions between the actors and the system as a response to an event started by the actor. We have divided the Use Case into 3 parts: Interface, Home, and Gameplay

6.2.2.1. Interface

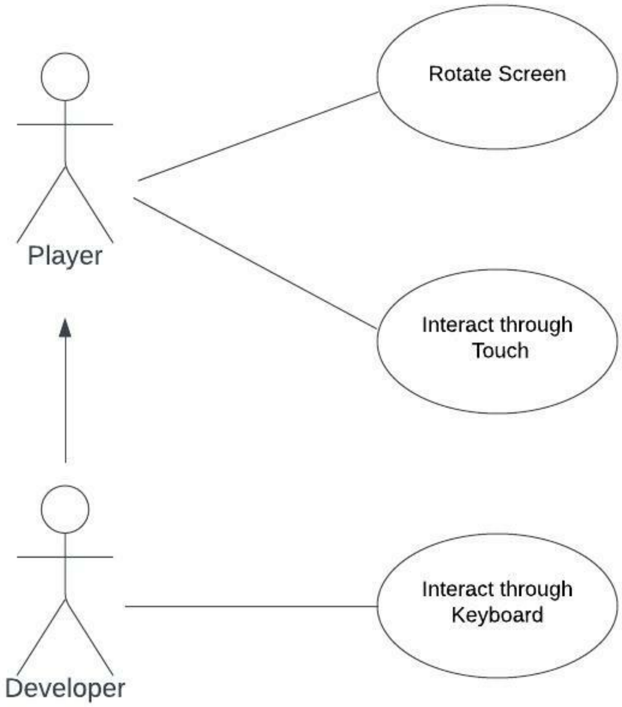


Figure 6: Use Case Diagram 1

6.2.2.2. Home

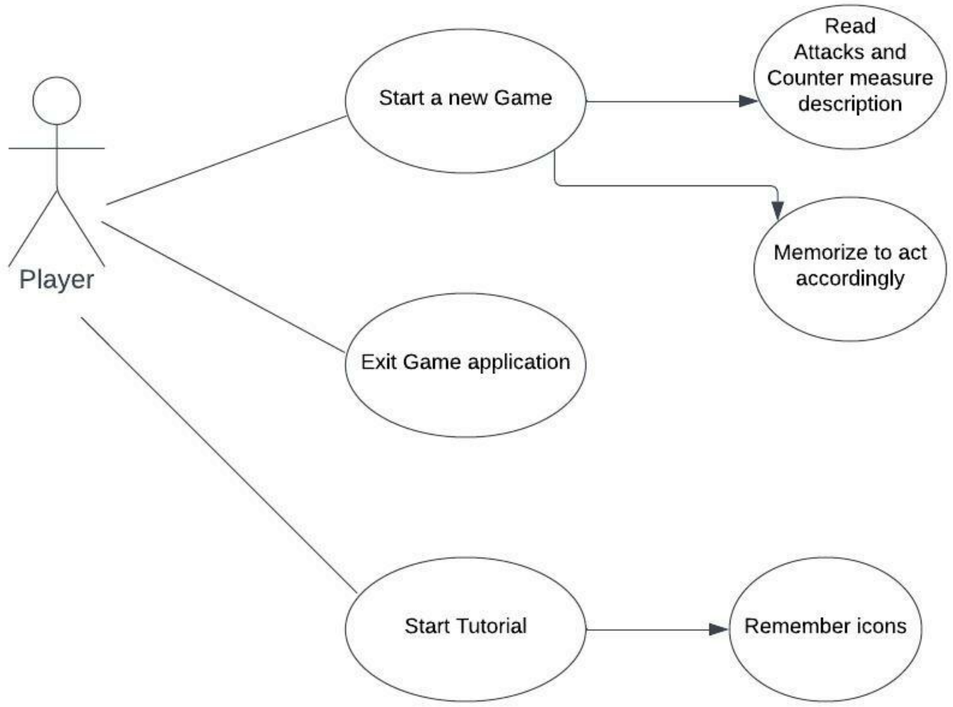

Player
Start a new Game
Read Attacks and Counter measure description
Memorize to act accordingly
Exit Game application
Start Tutorial
Remember icons

Figure 7: Use Case Diagram 2

6.2.2.3. Gameplay

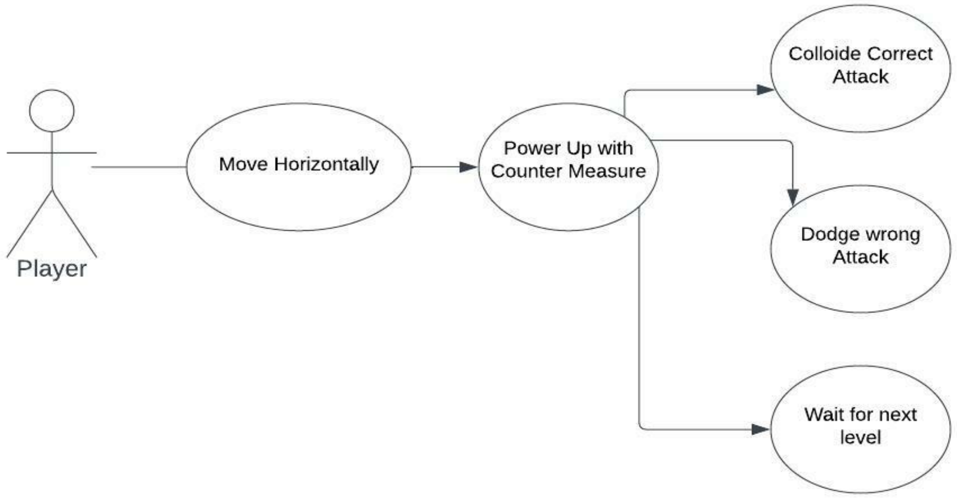


Figure 8: Use Case Diagram 3

6.2.3. Activity Diagram

The Player Starts the application and the main menu screen is loaded. It allows the player to start the game. Then the Player will be given option to either start the game or start the tutorial or Exit the game.

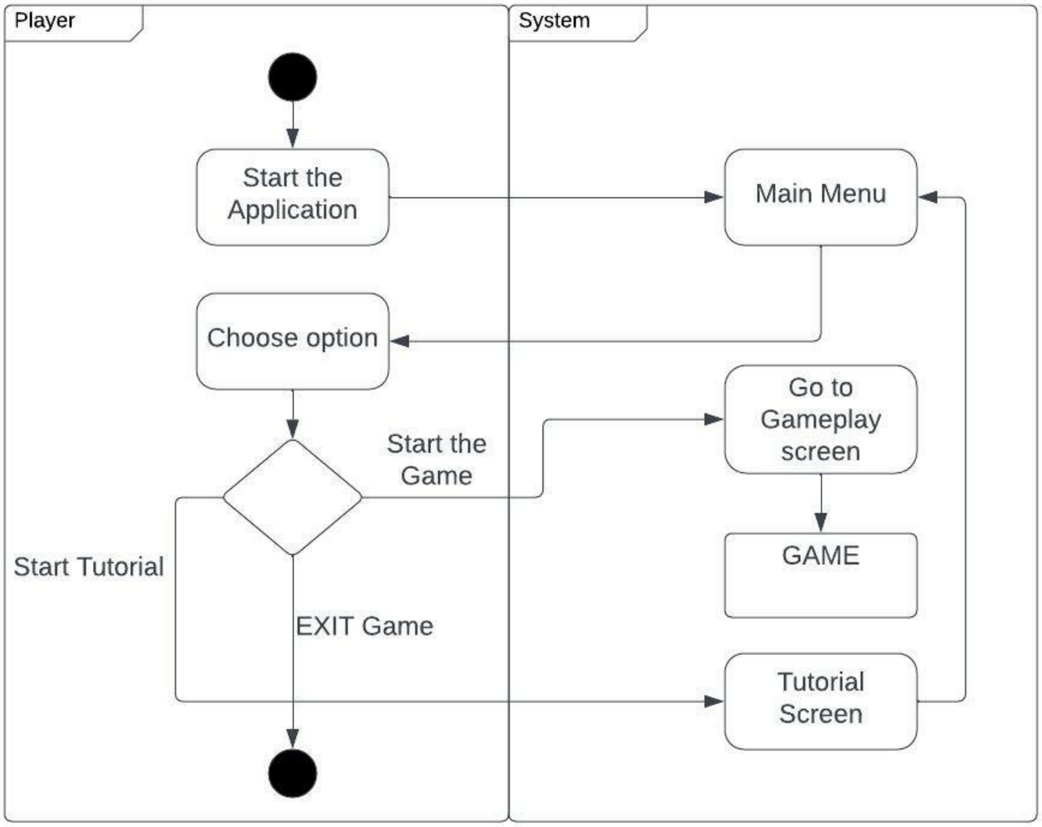


Figure 9: Activity Diagram

6.3. The Game Navigation

Figure 3 below shows the menu editor of Cyber Air-Attack. This diagram represents all the screens in this game and all the possible navigations available.

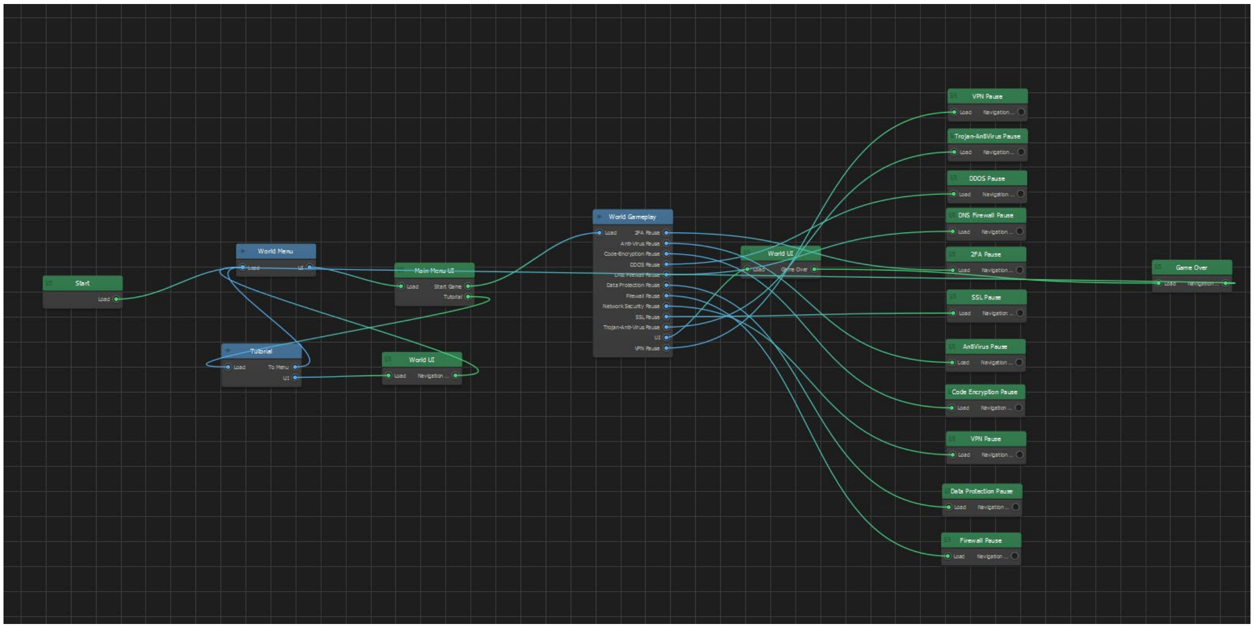


Figure 10: Menu Editor Screen

6.4. The Success Scenarios of Cyber Air-Attack

The menu screen appears after the game has been launched. There are two options on the menu screen. To play the game, the player has two options: Tap to Start or Tap to T. The menu is shown in Figure 4.

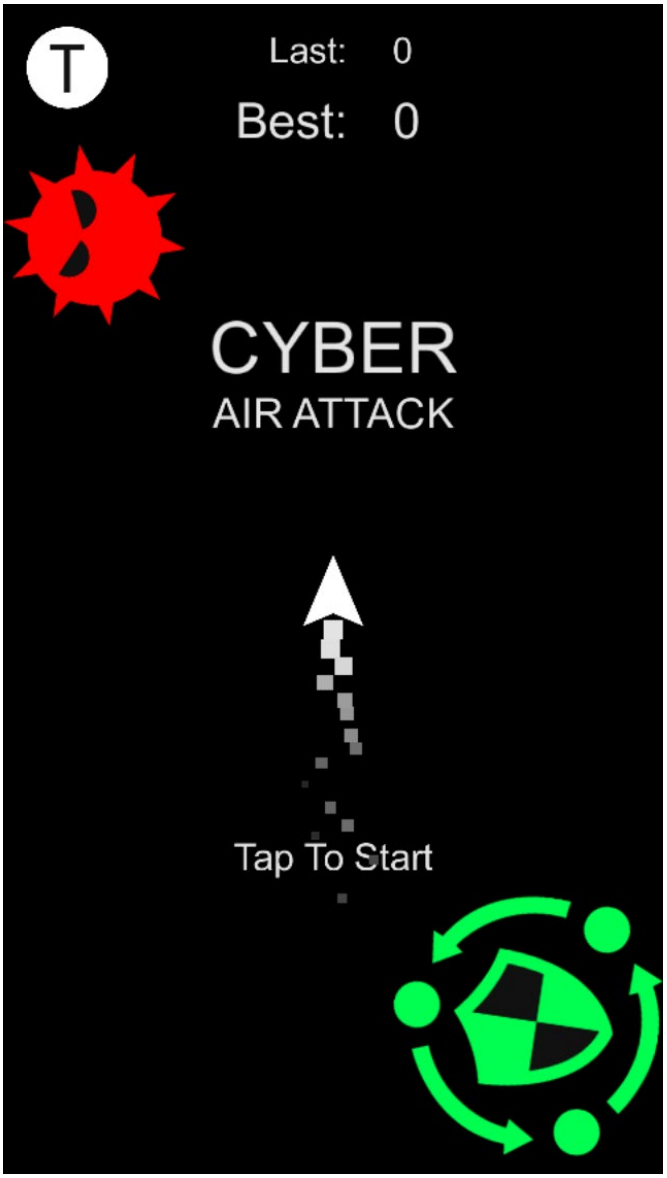
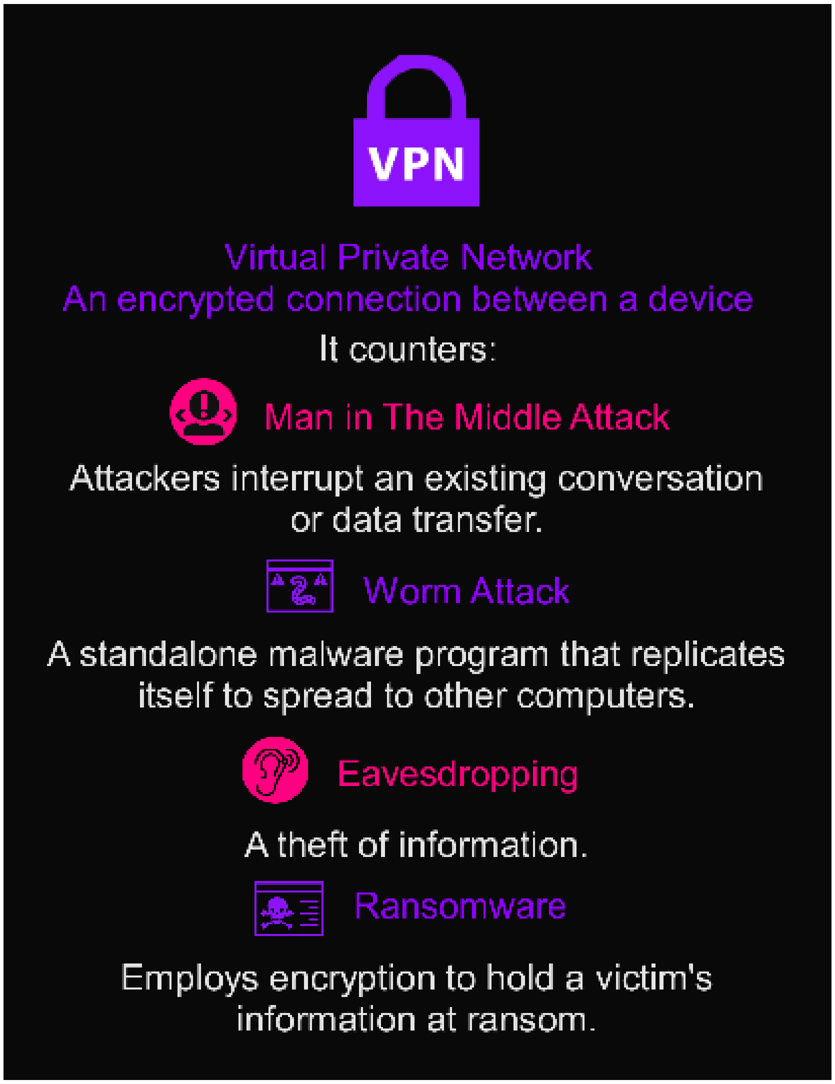


Figure 11. Cyber Air-Attack Menu Screen

The tutorial screen is displayed when the player clicks on the "T" icon. This allows the player to familiarize themselves with power ups, i.e., counter measures, and their descriptions. It also shows the attack counters that each power up can defeat. The "T" screen can be further divided into two sections to show the Cyber-attack icons and countermeasures on one screen.



VPN

Virtual Private Network
An encrypted connection between a device

It counters:

Man in The Middle Attack

Attackers interrupt an existing conversation or data transfer.

Worm Attack

A standalone malware program that replicates itself to spread to other computers.

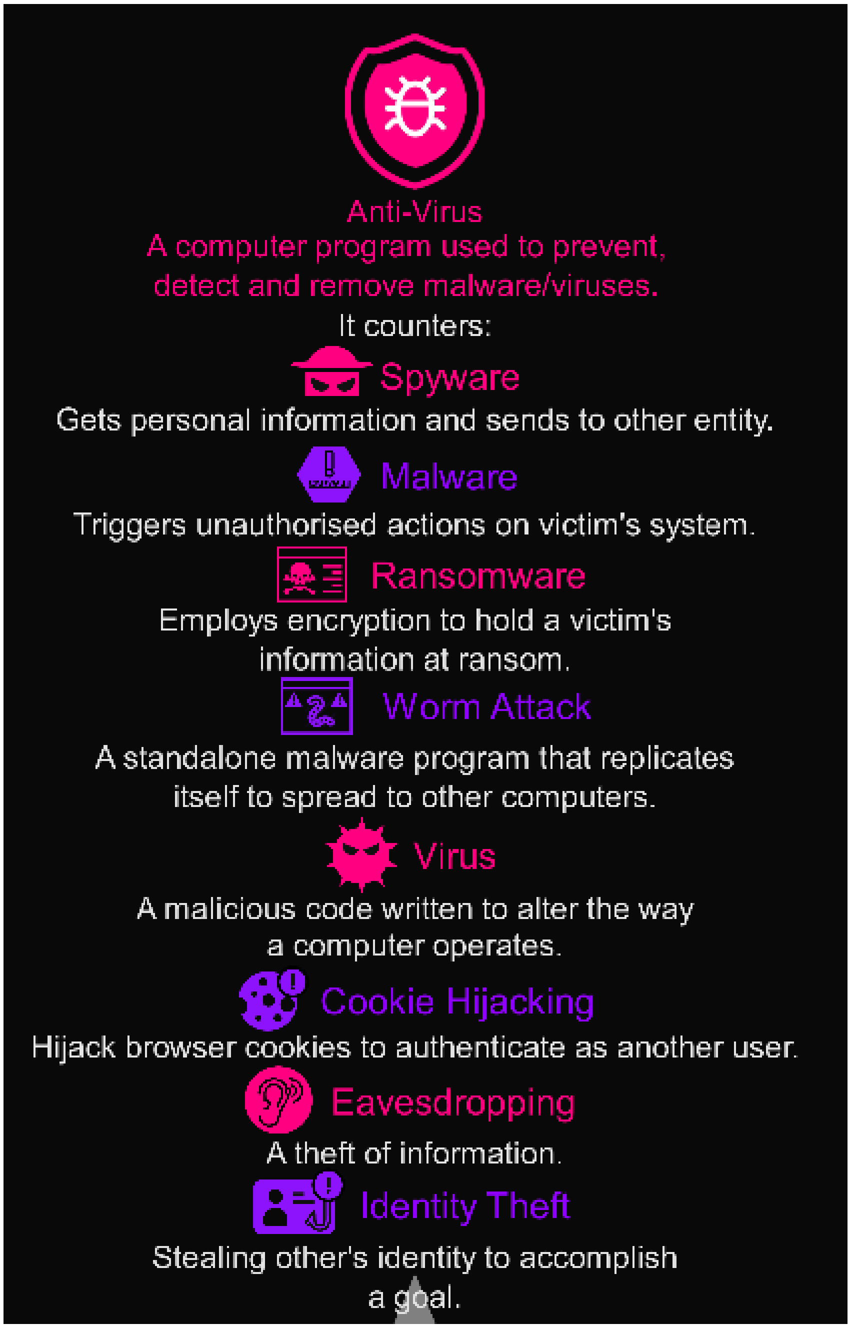
Eavesdropping

A theft of information.

Ransomware

Employs encryption to hold a victim's information at ransom.

Figure 12: Cyber Air-Attack Info Screen 1



Anti-Virus
A computer program used to prevent, detect and remove malware/viruses.
It counters:

Spyware
Gets personal information and sends to other entity.

Malware
Triggers unauthorised actions on victim's system.

Ransomware
Employs encryption to hold a victim's information at ransom.

Worm Attack
A standalone malware program that replicates itself to spread to other computers.

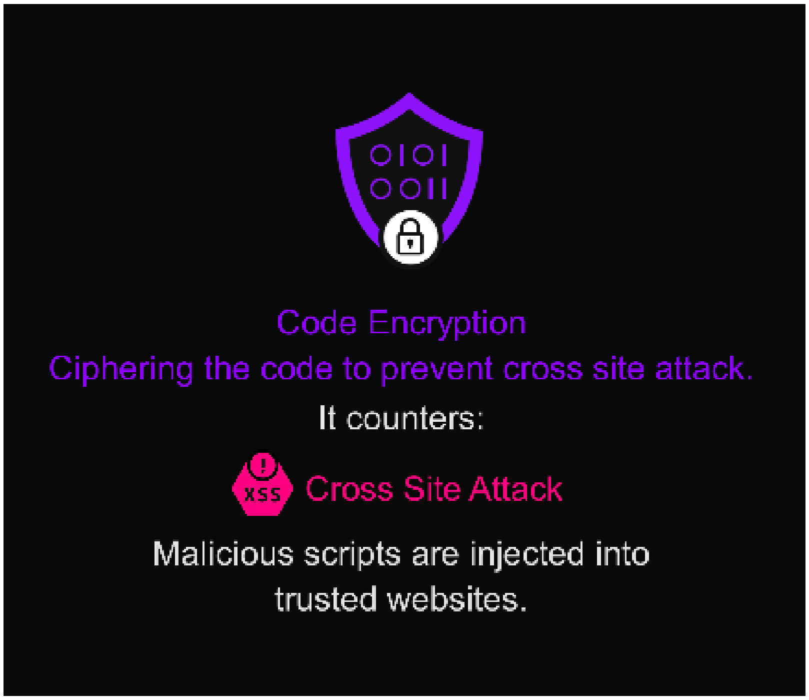
Virus
A malicious code written to alter the way a computer operates.

Cookie Hijacking
Hijack browser cookies to authenticate as another user.

Eavesdropping
A theft of information.

Identity Theft
Stealing other's identity to accomplish a goal.

Figure 13: Cyber Air-Attack Info Screen 2

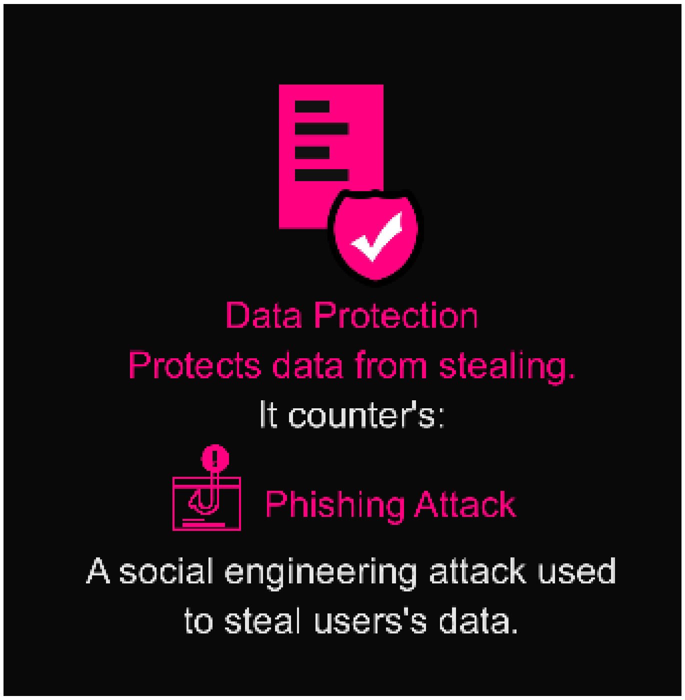


Code Encryption
Ciphering the code to prevent cross site attack.
It counters:

Cross Site Attack

Malicious scripts are injected into trusted websites.

Figure 14: Cyber Air-Attack Info Screen 3

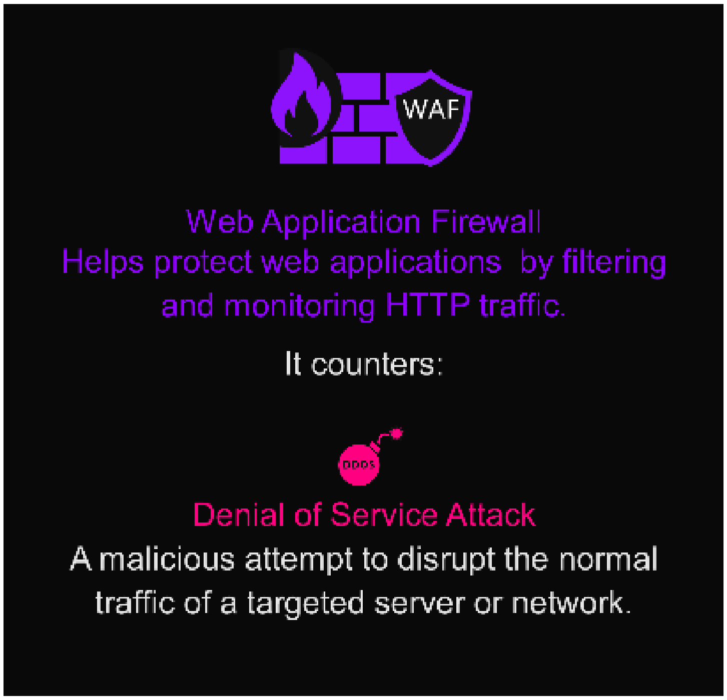


Data Protection
Protects data from stealing.
It counter's:

Phishing Attack

A social engineering attack used to steal users's data.

Figure 15: Cyber Air-Attack Info Screen 4

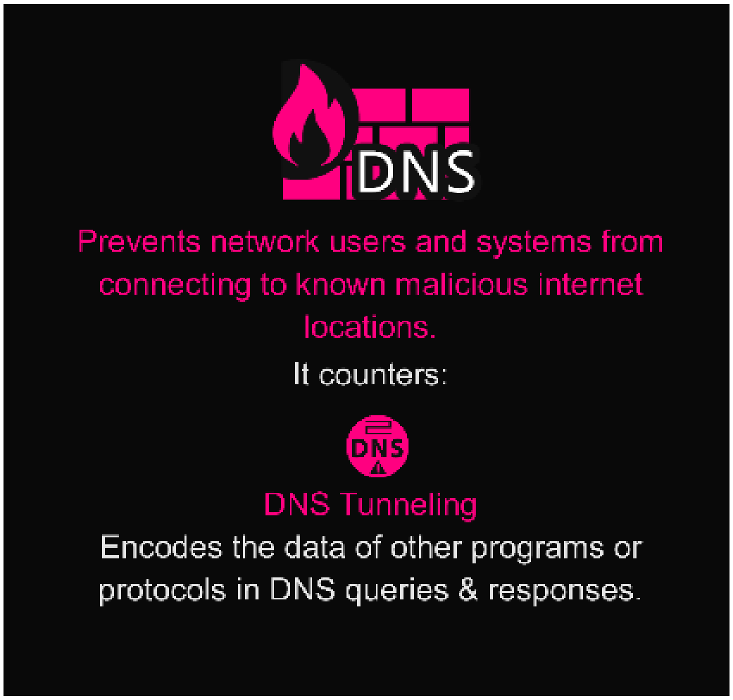


Web Application Firewall
Helps protect web applications by filtering and monitoring HTTP traffic.

It counters:

Denial of Service Attack
A malicious attempt to disrupt the normal traffic of a targeted server or network.

Figure 16: Cyber Air-Attack Info Screen 5

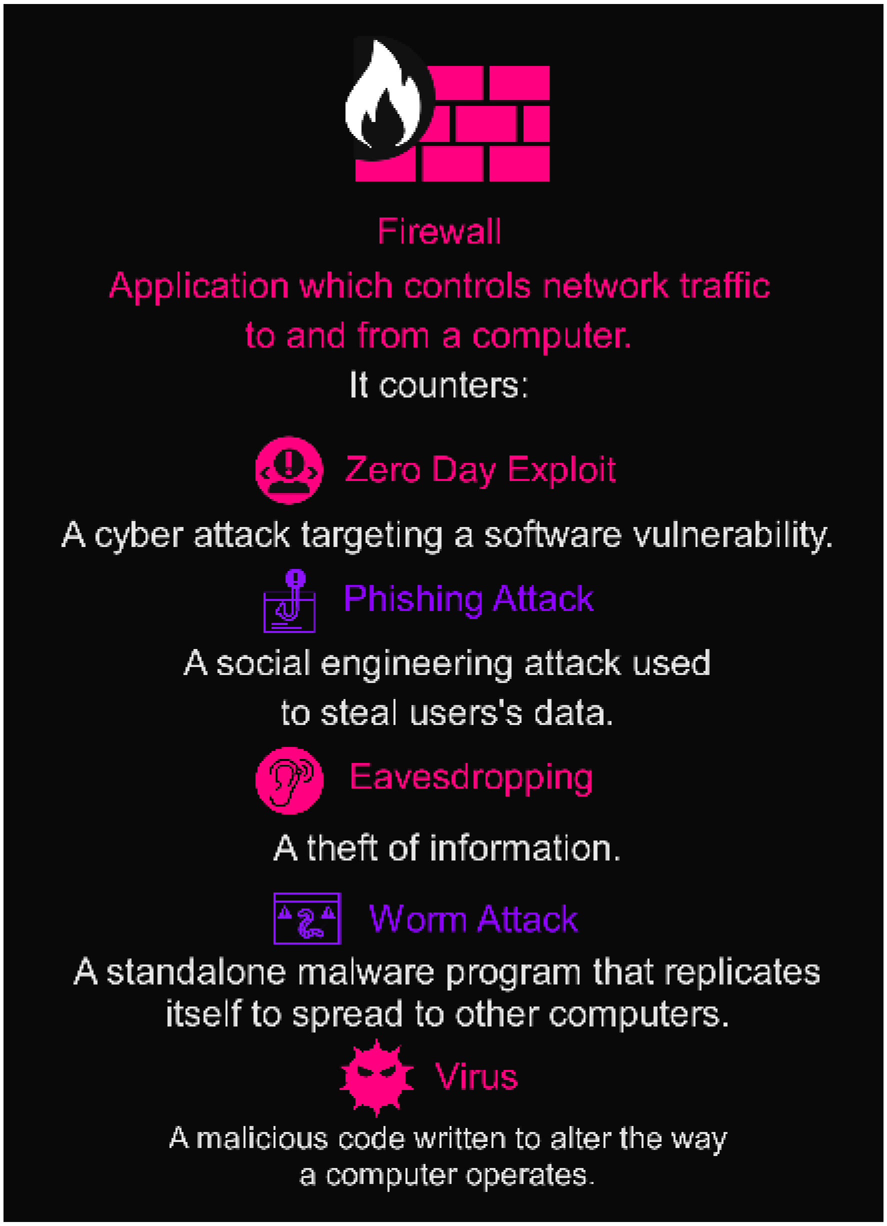


Prevents network users and systems from connecting to known malicious internet locations.

It counters:

DNS Tunneling
Encodes the data of other programs or protocols in DNS queries & responses.

Figure 17: Cyber Air-Attack Info Screen 6



Firewall

Application which controls network traffic
to and from a computer.

It counters:

Zero Day Exploit

A cyber attack targeting a software vulnerability.

Phishing Attack

A social engineering attack used
to steal users's data.

Eavesdropping

A theft of information.

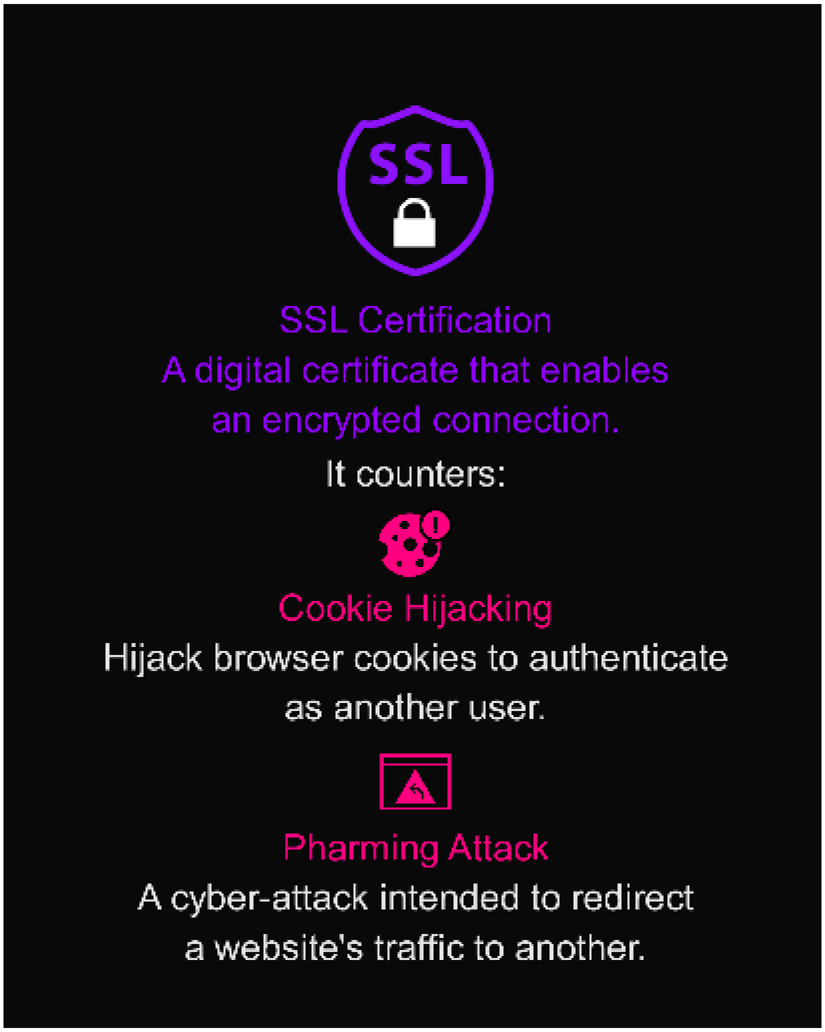
Worm Attack

A standalone malware program that replicates
itself to spread to other computers.

Virus

A malicious code written to alter the way
a computer operates.

Figure 18: Cyber Air-Attack Info Screen 7



SSL Certification

A digital certificate that enables an encrypted connection.

It counters:

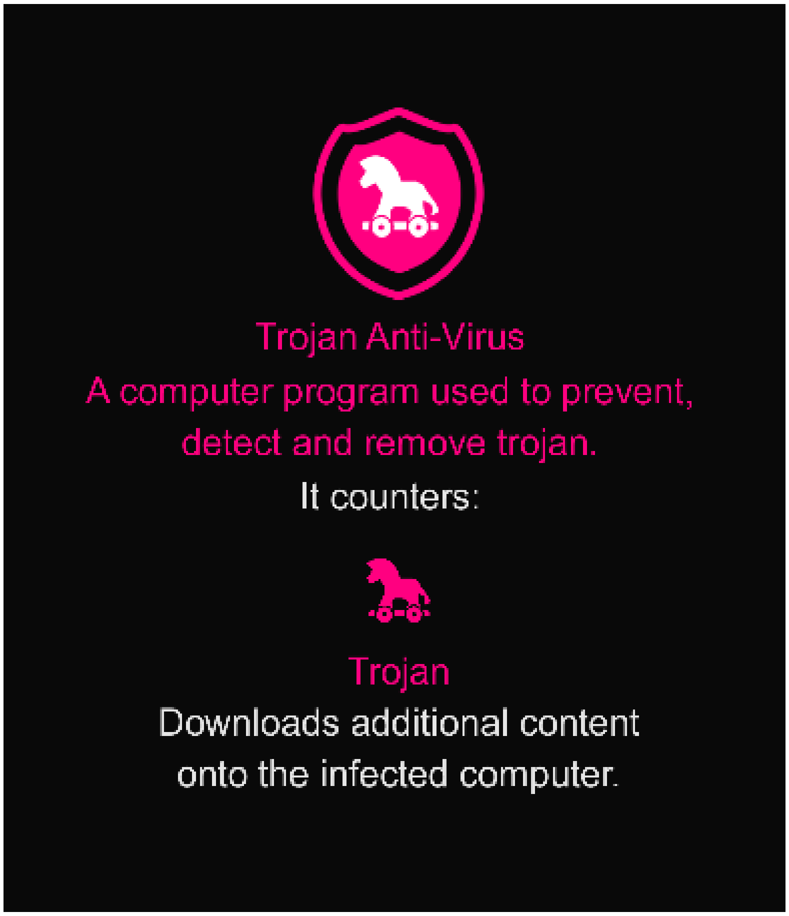
Cookie Hijacking

Hijack browser cookies to authenticate as another user.

Pharming Attack

A cyber-attack intended to redirect a website's traffic to another.

Figure 19: Cyber Air-Attack Info Screen 8



Trojan Anti-Virus

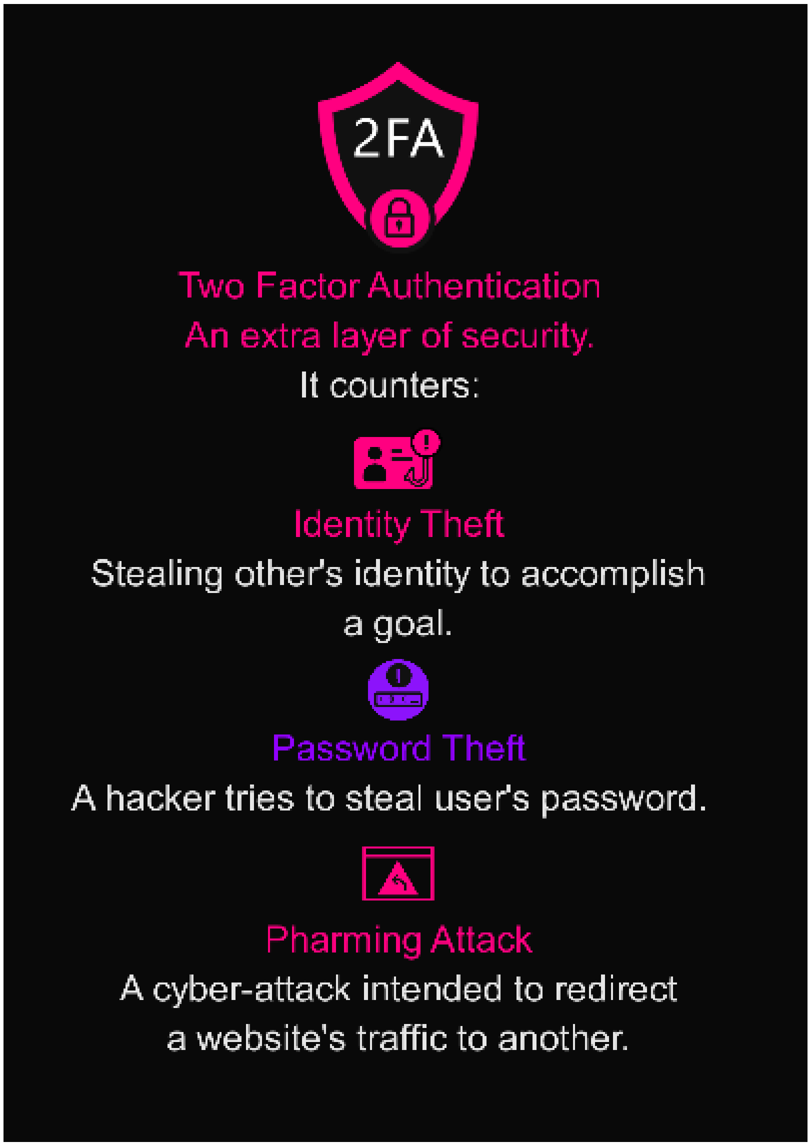
A computer program used to prevent, detect and remove trojan.

It counters:

Trojan

Downloads additional content onto the infected computer.

Figure 20: Cyber Air-Attack Info Screen 9



Two Factor Authentication

An extra layer of security.

It counters:

Identity Theft

Stealing other's identity to accomplish a goal.

Password Theft

A hacker tries to steal user's password.

Pharming Attack

A cyber-attack intended to redirect a website's traffic to another.

Figure 21: Cyber Air-Attack Info Screen 10

6.5. Outcome of the Game

This game's main purpose is to demonstrate itself as a better teaching method. By playing the game, the player recognizes the icons. Knowing the icons and the countermeasures that can be used to combat them, the player will learn more about cybersecurity.

This game requires that the player can understand and overcome all its challenges. It will be easier to play the game and earn more points if the player is more familiar with cybersecurity concepts. Tests are the best way to learn these concepts. Each step of the game tests player's ability to learn. This game can be used as a teaching tool. This game's success is dependent on your cybersecurity knowledge. This is how you can learn and give feedback to players.

6.6. Tools and Software used for Development of Game

This game was developed and designed using Buildbox. Buildbox is a drag-and-drop software for game creation. It can be used on both Windows and OSX platforms (Gust, 2016). Buildbox was released in January 2015. It has been used to create more than 150 games, which have been featured on Apple's app store charts and taken up by major publishers (n.d., 2018).

Buildbox's main features include the image drop wheel, option bar and asset bars, collision editor, scene editors, monetization options and sliders that alter the game's physics. It is easy to deploy a game created through Buildbox. It can easily be exported to Windows Store, Android Store, or iOS Steam as a gaming application.

The icons used for depicting attacks and counter attacks, along with the main Airplane character has been created using Adobe's Photoshop tool. The reason to select Photoshop as the graphics designing tool is the ease of use and the content available online to learn it. Since, Adobe's photoshop is very well-known software, the tutorials offered online to understand it were readily available.

6.7. Why Buildbox

When compared to other tools available in the market such as GameSalad and GameMaker Studio, Buildbox has edge over them in different aspects. The easiest drag and drop game making software is the Buildbox. It requires zero coding knowledge and provides better UI designs options to gamify the educational concepts. While Gamemaker Studio and GameSalad are expensive to use, Buildbox is easy to get started without buying any premium professional version of it.

With Buildbox, you can create the entire game with ease. The features like image drop wheel, collision editor, asset bar, scene editor and over thousands of game assets including animations and various sound effects, Buildbox becomes the first preference among the zero-code development environment for building games. Buildbox allows you to define each aspect of any character or object of your game with utmost detailing.

The comparison between Buildbox, GameSalad and Gamemaker studio is shown in the below table 5.

Table 5: Comparison Between Tools

Parameters	**Buildbox**	**GameSalad**	**GameMaker Studio**
Pricing	Cheap	Expensive	Expensive
Editing Performance	Smooth	Poor	Average
User Interface	Great User Interface	Average User Interface	Good User Interface
Usage	Easy to use	Easy to Use	Easy to use

7. CONCLUSION

Cybersecurity education is popular because it encourages learning by doing. Cybersecurity is becoming a more serious concern due to the increasing number of cybercrimes. This issue must be addressed by educating people at all levels about cybersecurity concepts and the possible cyber-threats. Although many efforts have been made to teach this topic in the past, they seem to be ineffective in reaching large numbers of people and making cybersecurity more accessible.

Our goal for this paper was to raise awareness about cybersecurity through the Bloom's Revised Taxonomy's 'Remember' level and 'Understand" levels. We created a game to help users understand the dangers of malware attacks and how to prevent them. The 'Remember" level of the cognitive domain in Bloom's Revised Taxonomy was incorporated by detailed information about icons used in our game. The game provides the basic concepts of cybersecurity that a player can remember to reach the remember level. The game can also incorporate the 'Understand" level by allowing players to remember the information and apply it while they play the game. This game was made easy to appeal to amateur users. We chose to use games over traditional methods of teaching because they are more engaging, effective, engaging, and fun.

8. LIMITATIONS AND FUTURE WORK

The game was designed and developed, but it has not been tested by actual users. To evaluate users' understanding of concepts, evidence is needed. The game is web-based and therefore only those who have internet access can use it. The game is designed to teach concepts, which cannot be reached by people who are not interested in gaming.

This game features 18 icons that target 18 types cyberattacks and their countermeasures. This game could be expanded to include additional icons that teach complex concepts about cybersecurity. Research can also be extended through the incorporation of all higher order levels Bloom's Revised Taxonomy.

REFERENCES

A. Rollings , & E. Adams, *Andrew Rollings and Ernrest Adams on Game Design* (2003) (pp. 287-288). Indianapolis: New Riders, An Imprint of Pearson Education. Retrieved from https://doi.org/10.1016/B978-0-12-801462-2.00001-1

Abawajy, J. (2014). *User preference of cyber security awareness delivery methods, Behaviour & Information Technology.* doi:10.1080/0144929X.2012.708787

Annetta, L. A. (2008). Video Games in Education: Why They Should Be Used and How They Are Being Used. *JSTOR*, pp. 229–39. Retrieved from https://www.jstor.org/stable/40071547

Basset, G., Hylender, D. C., Langlois, P., Pinto, A., & Widup, S. (2020, January). *Introduction to the 2020 DBIR: Verizon Enterprise Solutions*. Retrieved from Verizon Enterprise: https://www.verizon.com/business/resources/reports/dbir/2020/introduction/

Bergeron, B. (2006). *Developing serious games.* Hingham: Charles River Media.

Bloom, B., Engelhart, M., Furst, E., Hill, W., & Krathwohl, D. (1956). *Taxonomy of Educational Objectives: The Classification of Educational Goals: Handbook 1 Cognitive Domain.* Michigan: David McKay Company.

CheckPoint. (2022, February 16). *Biggest Cybersecurity Challenges in 2022*. Retrieved from Check Point Software: https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cybersecurity/biggest-cybersecurity-challenges-in-2022/

Chiniara, G. (2019). Clinical Simulation (Second Edition). In G. Chiniara, *Clinical Simulation* (pp. 917-940). Canada: Academic Press. doi:https://doi.org/10.1016/C2017-0-01173-4

Esposito, N. (2005). A short and simple definition of what a videogame is. *Digital Games Research Conference 2005, Changing Views: Worlds in Play* (pp. 2-3). Vancouuver: Authors & Digital Games Research Association (DiGRA). Retrieved from http://www.thegamesjournal.com/articles/WhatIsaGame.shtml

Furst, E. (1994). Bloom's Taxonomy: Philosophical and Educational Issues. In L. a. Anderson, *Bloom's Taxonomy: A Forty-Year Retrospective* (pp. 28-40). Chicago: The National Society for the Study of Education.

Gillis, A. (2022). *What is Cybersecurity.* Retrieved from Techtarget: https://www.techtarget.com/searchsecurity/definition/cybersecurity

Gust, J. (2016). *Best Free Game Making Tools*. Retrieved from Gamedeveloper.com: https://www.gamedeveloper.com/design/best-free-game-making-tools

Hunt, R. (2022, October 14). *The 2021 Financial Data Risk Report reveals every employee can access nearly 11 million files*. Retrieved from Varonis: https://www.varonis.com/blog/2021-financial-data-risk-report

IBM. (2021, July). *Cost of a Data Breach Report.* Retrieved from IBM: https://www.ibm.com/downloads/cas/OJDVQGRY

KPMG. (2022, January 1). *A triple threat across the Americas: KPMG 2022 Fraud Outlook*. Retrieved from KPMG: https://home.kpmg/xx/en/home/insights/2022/01/kpmg-fraud-outlook-survey.html

Krathwohl, D. R. (2002). A Revision of Bloom's Taxonomy:An Overview. In D. R. Krathwohl, *Theory into Practice* (pp. 212-218). New york: Routledge.

Mayer, R. E. (2002). Rote Versus Meaningful Learning. In R. D. Krathwohl, *Theory into Practice* (pp. 226-232). New York: Routledge.

Mclean, M. (2023, June 1). *2023 must-know cyber attack statistics and Trends*. Retrieved from Embroker: https://www.embroker.com/blog/cyber-attack-statistics/

n.d. (2018). *Buildbox*. Retrieved from Buildbox: https://www.buildbox.com/apple-features-50-buildbox-games/

Stackpole, B. (2021, April 1). *Symantec Security Summary*. Retrieved from Symantec Enterprise Blogs: https://symantec-enterprise-blogs.security.com/blogs/feature-stories/symantec-security-summary-april-2021

Surfshark. (2023, April 21). *Data Breach Statistics by country: Recap of 2021*. Retrieved from Surfshark: https://surfshark.com/blog/data-breach-statistics-by-country-in-2021

Thales Group. (2022). *Perspectives and Pathways to Sovereignty and Transformation*. Retrieved from Thalesgroup: https://cpl.thalesgroup.com/data-threat-report

Zamzami, Z., Kai Wah Chu, S., Shujahat, M., & Jacqueline Perera, C. (2020). The impact of gamification on learning and instruction: A systematic review of empirical evidence. *Educational Research Review, 30*(100326). doi:https://doi.org/10.1016/j.edurev.2020.100326