BASIC CYBERSECURITY AWARENESS THROUGH GAMING

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

By

Vikas Krishnarao Kulkarni

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

Major Department:
Computer Science

December 2018

Fargo, North Dakota

North Dakota State University
Graduate School

Title

Basic Cybersecurity Awareness Through Gaming

By

Vikas Krishnarao Kulkarni

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. Simone Ludwig

Dr. Ronald Degges

Approved:

12/21/2018 — Date

Dr. Kendall E. Nygard — Department Chair

ABSTRACT

The goal of this paper is to bring the basic awareness of cybersecurity among students so that they do not become a victim of cybercrime. Studies show that cybersecurity serious games support multiple well-established perspectives of learning and have the potential to motivate individuals to learn by keeping them in a state of flow.

Educators use the Bloom's revised taxonomy, as it provides an effective method for the students who are learning a topic. Bloom's revised taxonomy identifies six cognitive levels, starting from basic steps in learning to the more advances steps.

This paper includes developing a game called DodgeTheThreats that provides some useful tips on basic cybersecurity. By making use of a serious game that incorporates Bloom's taxonomy of learning, it is possible to have a very effective learning tool for the students and thereby raise the awareness of cybersecurity.

ACKNOWLEDGMENTS

I would like to express my sincere gratitude and respect to my advisor, Dr. Kendall Nygard for guiding me in this endeavor from the beginning until the end. Without his guidance and persistent help this dissertation would not have been possible.

I would like to thank my committee members, Dr. Simone Ludwig and Dr. Ronald Degges for their valuable guidance and helpful comments. It is also my duty to express my gratitude to my parents for their unconditional support and encouragement. They have been a constant source of inspiration for me all through my life.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Figure Page

1. INTRODUCTION

To raise the awareness of cybersecurity this paper involves developing a game called DodgeTheThreats that provides few useful tips on basic cybersecurity. The game successfully incorporates some aspects of the first level and the second level in the revised bloom's taxonomy. But before getting into the details of the game, this chapter first explains regarding the importance of cybersecurity and the necessary questions to be asked when considering serious games for cybersecurity. Next, the chapter mentions about the objectives of the serious game that is developed and then regarding the organization of the chapter.

1.1. Importance of Cybersecurity

Cybercrime ranks second most common type of economic crime experienced in the world (PWC, 2016). In 2016 alone, the loss due to cybercrime according to the report from Norton was $125.9 billion globally (Norton, 2016) . The global cost of cybercrime has reached about 0.8 percent of global GDP. Companies and Organizations have a major responsibility of recruiting new cybersecurity professionals and training their workforce to protect themselves from the ever-growing threat of cybercrime. However, there are estimations that there would be a shortage in the cyber security workforce of 1.8 million workers by the year 2022 (Frost and Sullivan, 2017). There is a strong necessity to investigate the existing methods of training and awareness to prevent attacks and potentially draw individuals to the field of cybersecurity. Along those lines, this paper also examines and evaluates the relationship between serious gaming and improved cybersecurity awareness and training.

The important questions to be asked when discussing about training and awareness methods are as follows.

1. Why should serious games be considered for cybersecurity training?

2. What advantages can the application of serious gaming for training provides which the contemporary cybersecurity training could not?
3. If a serious game is to be developed, how can it be designed to be an effective learning tool?

The ability of training and awareness programs to be effective relies heavily on how they are communicated to users (Ghazvini & Shukur, 2017). The existing methods of training include face-to-face exercise and workshops, paper-based posters and newsletters, and online videos and computer-based training (Abawajy, 2014). To maintain a person's attention while trying to communicate information using the current methods of training is a challenging task (Cone, Irvine, Thompson, & Nguyen, 2007). To address the perceived problems with current methods of cybersecurity training and awareness (and potentially the workforce shortage) serious games have been purposed to make training more efficient and engaging.

1.2. Serious Games for Cybersecurity Education

The academic and gaming communities have come together and expended considerable amount of effort to merge their interests into what is now known as "educational gaming/serious gaming". Serious games have already proven to be effective in and out of the classroom. Additionally, the United States military is one of the major adopters of serious games. Tactical Iraqi has proven effective in teaching the military Arabic (Lewis, 2010). While America's Army has been successful as a recruiting and pre-training tool (Zyda et al., 2003). A study conducted on the effectiveness of the serious game. CyberCIEGE against the Department of Defense's information security awareness videos revealed game players had a higher level of improvement (Jones, Yuan, Carr, & Yu, 2010). Another study found that users were better able to detect

phishing after playing the game Anti-Phishing Phil versus those who just used existing training material (Sheng et al., 2007).

1.3. Objectives

The main objective of this paper is to bring the basic cybersecurity awareness with the help of a serious game called DodgeTheThreats. The game includes the following cybersecurity tips.

- Avoiding spam emails
- Understanding the difference between safe and unsafe websites
- Being careful of what to and what not to click while browsing the internet
- Avoiding Phishing scams- Identifying suspicious emails and phone calls
- Importance of having an antivirus
- Importance of backing up the data
- Importance of checking the trust of software
- Protecting from infected flash drives/other storage devices
- Importance of firewall
- Importance of having updated software

This paper associates a serious cybersecurity game called DodgeTheThreats with the classical classifications of the cognitive domain developed by Bloom.

1.4. Chapter Organization

The chapters in the paper are organized as follows.

- Chapter 2 presents the literature review and the main motivation for using serious games for Cyber security awareness

- Chapter 3 presents an overview of original Bloom's Taxonomy learning objectives and a detail explanation of the Revised Bloom's Taxonomy.
- Chapter 4 presents the tool used to build the game and the game design of DodgeTheThreats
- Chapter 5 explains how the Remember level and Understand level of the revised Bloom's taxonomy can be incorporated with the game that is developed.
- Chapter 6 presents a set of conclusions and the limitations related to the work. It also provides the recommendation for future work.

2. LITERATURE REVIEW

Before the use of serious games for cybersecurity training, it is necessary to investigate the major aspects. It is important to know why serious games are suitable for cybersecurity games. Along those lines, this chapter covers the following topics regarding video games.

- The popularity of video games.
- The learning principles that are incorporated in serious video games.
- The motivation that serious video games provide for learning.
- Existing successful serious game on CyberSecurity – Anti-phishing Phil.
- Game design for creating effective cybersecurity training games.

2.1. The Popularity of Video Games

There are several benefits of using video games as a medium to teach individuals cybersecurity concepts. The first of these benefits is the increasing popularity of video games in modern era. A survey of Entertainment Software Association (2017) revealed that 65% of US households are home to at least one person who plays 3 or more hours of video games a week. The video game industry made a total of $30.4 billion just in 2016 (Entertainment Software Association, 2017). Although this does not mean that average video game players would play serious games (and specifically those for cybersecurity training) but it does reflect the increased interest in gaming. Students and workers targeted by training and awareness programs are more likely to be familiar with video games or play video games than ever before. Video games have a great potential of reaching individuals to a global level very easily.

The distribution of players across age groups is important when looking to use serious games for cybersecurity training and awareness. In contradiction to the belief that the average person who plays video games is a young male in his teens or twenties, the average video game

player is thirty-five years old (Herr & Allen, 2015). Distributions of the average gamers by age group are relatively equal, meaning there are gamers young, old, and middle-aged (Entertainment Software Association, 2017). It is necessary to educate the children regarding cybersecurity so that they don't become victim of cybercrime and also to make them prepared to meet the demand of the cybersecurity workforce. People who are middle-aged are already working in jobs and need to learn how to avoid threats to not only their personal computers, but also their role in protecting their employer from a cyber-attack. Lastly, older people (age 50+) are typically targeted by online scams and fake technical support calls that could be prevented through learning about cybersecurity using a serious game (Carlson, 2006). Serious games for cybersecurity training and awareness have the greatest potential for educating and introducing cybersecurity to females (Herr & Allen, 2015). In addition to the capability of reaching wide range of individuals, serious games are designed in a manner that makes learning more efficient and effective. It is important to mention that there are many perspectives of learning that are supported by games, each of which complements one another by supporting different learning goals and outcomes (Hense & Mandl, 2014).

2.2. The Main Learning Principle of Serious Video Games

Video game teaches the player with the help of positive reinforcement of the desired behavior by punishing the player for performing undesired actions. Payoffs in video games include awarding players with virtual currency, achievements, high scores on leaderboards, and completion of tasks or levels. Conversely, video games punish players by losing to AI or other humans, losing life in the game, having to replay a level after failure, or falling behind on the leaderboard. Players, therefore, learn throughout the play session what they should and should not do to avoid punishment (Hense & Mandl, 2014). Hense and Mandl (2014) pointed out the

behaviorist principles of positive reinforcement and punishment work best in action, sports, and racing games, as players are regularly being provided immediate feedback regarding their actions. Due to the continuous feedback, it is expected that these principles would work best when continually practicing and repeating an activity (Hense & Mandl, 2014). To be an effective learning tool, it is important that serious games should have objectives and user interfaces that are straightforward and easy for inexperienced players to understand. For instance, players of CyberCIEGE reported difficulty knowing what they had to do next to complete the objectives of the game (Hagen, Irvine, & Thompson, 2009). Furthermore, players of Anti-Phishing Phil preferred the easy to follow unambiguous information presented to them in text and video-based training methods (Abawajy, 2014). Easing users into the game, while allowing experienced players to skip basic levels, should help address the problem of users with varying degrees of skill.

2.3. The Motivation for Gaming

In addition to the teaching and learning theories that serious games support, the motivational aspects of video games must also be examined. The flow theory is considered as one of the most popular theory while considering the motivation for video games. Grund (2015) conducted a literature review of the theoretical foundations of using games and game elements for learning and motivation and found thirty-four separate publications. Of those thirty-four publications on theory, flow theory was mentioned the most (seventeen times).

2.3.1. Flow Theory

The concept of flow, proposed by Mihály Csíkszentmihály, is a positive psychology theory that describes the human experience of being fully immersed in a state of focused

motivation (Csikszentmihalyi, Abuhamdeh, & Nakamura, 2014). In this theory, there are three conditions necessary to achieve flow state as stated below.

1. One must be involved in an activity with a clear set of goals. This adds direction and structure to the task.
2. One must have a good balance between the perceived challenges of the task at hand and his or her own perceived skills. One must have confidence that he or she is capable to do the task at hand.
3. The task at hand must have clear and immediate feedback. This helps the person negotiate any changing demands and allows him or her to adjust his or her performance to maintain the flow state (Csikszentmihalyi et al., 2014).

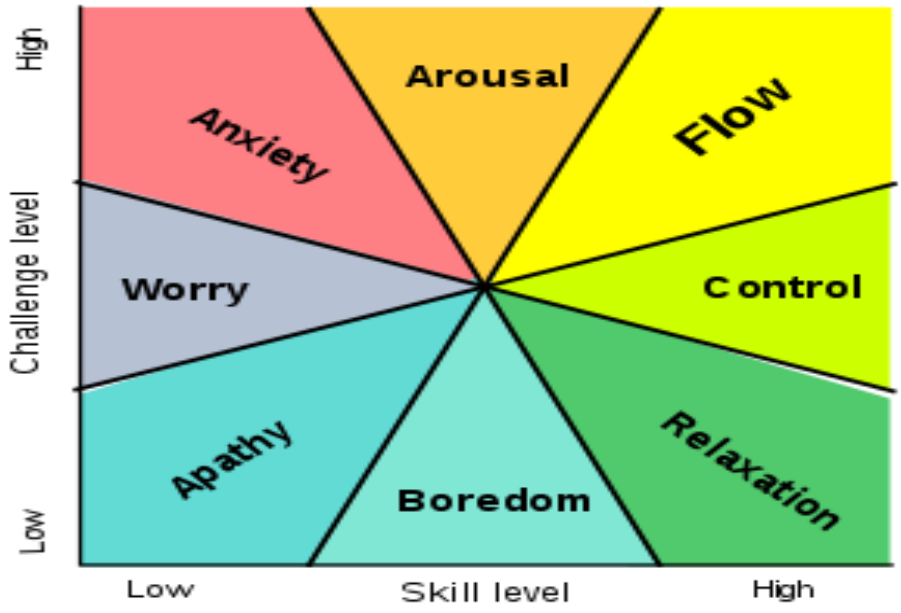

Fig 1. Mental State in Terms of Challenge Level and Skill Level

As shown in above figure 1, each mental state is explained as follows.

- **Apathy** indicates low skill, low challenge. This is usually experienced when we are alone doing nothing.

- **Boredom** indicates medium skill, low challenge. This is usually felt while doing chores.
- **Relaxation** indicates high skill, low challenge. This is usually experienced when we are eating, reading, or talking to a friend.
- **Worry** indicates low skill, medium challenge. This is usually experienced when contemplating work struggles.
- **Anxiety** indicates low skill, high challenge. This is usually experienced when one is under stress at work or a sudden threat arises. Anxiety is uncomfortable, obviously, so people often try to reduce the challenges in front of them by giving up responsibility, setting our sights lower, or going into denial.
- **Arousal** indicates medium skill, high challenge. This is usually experienced when a person is performing a new task or is learning something. Csikszentmihalyi considers arousal a positive state, even though the challenge is eclipsing our skills. It's a neighbor to flow, and it can turn into flow if the person boosts his/her skills a bit.
- **Control** indicates high skill, medium challenge. This is usually experienced while driving a car. This is another positive state and this state can lead us to flow if the person can increase the challenge.
- **Flow** indicates high skill, high challenge. This is experienced when doing tasks that a person loves to do like a hobby, favorite work.

Furthermore, Csíkszentmihály represents flow as harnessing of emotions in the service of performance and learning. Some of the effects of flow are feelings of spontaneous joy, rapture and elation while performing tasks (Goleman, 1996).

Flow concepts describes about the ideal states of the player while playing the game and when they are highly receptive for learning. It is because of these observations that game

designers have started to pay great attention to the meaning behind individual game mechanics and their systematic impact on gameplay.

In this flow state, individuals lost sense of time and concentrated intently on the activity they were involved in, feeling that they could react appropriately to whatever was presented to them (Nakamura & Csikszentmihalyi, 2014). The researchers, Chen and Johnson (2004), believed that a video game would intrinsically motivate players and put them in a state of flow (Chen & Johnson, 2004).

2.4. Existing Serious Game for CyberSecurity: Anti-Phishing Phil

Anti-Phishing Phil is an engaging training game originally developed at Carnegie Mellon University and now commercialized by Wombat Security Technologies. In the Anti-Phishing Phil training game, players helps a fun fish character called Phil to identify food and to avoid fish traps. The food are in the form of good websites/genuine email whereas the fish traps include fake links, malicious attachments, cash prizes, "respond-to" emails asking for sensitive information and other similar traps. Users are given a limited amount of time to analyze each email and spot traps. Users learn to verify the information presented to them, rather than trust easily forged email features such as logos or URLs to decide if the message is fraudulent or not. The game comes with an extensive collection of randomized legitimate and fraudulent emails, so users can play the game multiple times without seeing the same messages. In just a little over 10 minutes, users proceed through a succession of three rounds, with each round introducing new tips and teaching them how to fend off dangerous email attacks. Figure 2 and figure 3 are the screenshots of the game Anti-Phishing Phil

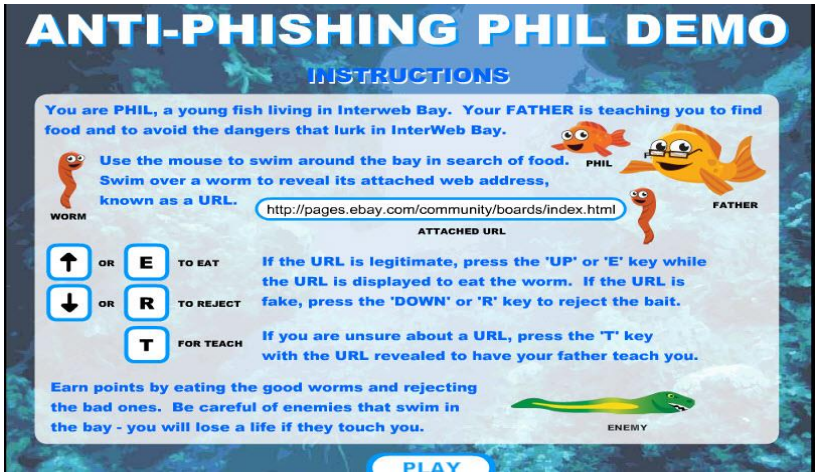

Fig 2. Screenshot-1 for Anti-Phishing Phil

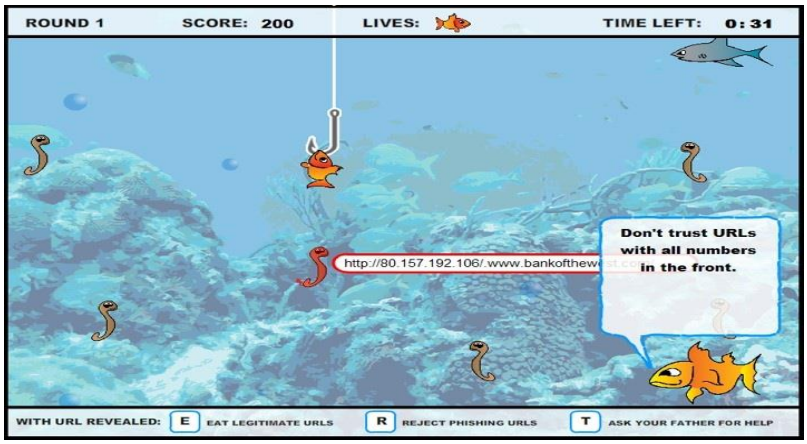

Fig 3. Screenshot-2 for Anti-Phishing Phil

After improving the game using a pilot study, the effectiveness of Anti-Phishing Phil was evaluated using a two-phase study. Individuals were divided into three groups of fourteen. One group was asked to read existing training material, another had to read the Anti-Phishing Phil tutorial messages, and the final group played the game for fifteen minutes. People who played the game performed better than both the other two training conditions, with significantly lower false positives rates. The improvement in performance was shown to be caused by individuals learning how to correctly determine what websites were phishing and those that were not (Sheng

et al., 2007). Game players were more confident in their choices, believed that they had learned critical information, and had fun playing Anti-Phishing Phil. Conversely, traditional methods did not improve confidence and were found less fun (29% versus 50%) (Sheng et al., 2007).

2.5. The Game Design for DodgeTheThreats

Endless runner games provide a nearly ideal setting to put the player into a flow state. The task in the game is challenging, but not impossible. Player choices create results quickly (immediate feedback). It feels like the player is being skillful. There is no time for the player to have other thoughts other than being engaged in the game. Such games include tight little circles of activities that pass through small anxiety, arousal, quick reaction, a small sense of control and a moment of relaxation, before the next challenge. In such games the player character continuously runs while preventing the obstacles. In the recent past the Android apps like Temple Run, Subway surfers were very popular smart phone Endless runner games. In 2017, the smartphone game "*Subway Surfers*" was the most downloaded game across the globe (Live, 2017). The game DodgeTheThreats is also an endless runner game which is developed with a similar design in mind. The game design is explained in detail in separate chapters.

3. BLOOM'S TAXONOMY

After having discussed why serious games are such an effective tool for cybersecurity training. The next question that is relevant is that how we can design a game that best facilitates the learning process. Bloom's taxonomy is an effective method that is employed by teachers, instructors, professional trainers, and curriculum planners (Bloom, Engelhart, Furst, Hill, & Krathwohl, 1956). Educators often use Bloom's Taxonomy to create learning outcomes that target not only subject matter but also the depth of learning they want students to achieve, and to then create assessments that accurately report on students' progress towards these outcomes (Anderson et al., 2001).

The committee identified the following three domains of educational activities or learning (Bloom, 1956).

- Cognitive - mental skills (knowledge)
- Affective - growth in feelings or emotional areas (attitude or self)
- Psychomotor - manual or physical skills (skills)

3.1. Original Bloom's Taxonomy

In our study we consider the Cognitive domain. The Bloom's Taxonomy of the Cognitive Domain provides a hierarchical arrangement of learning processes. A brief summary of the six levels is given in the table 1 below.

Table 1. The Original Bloom's Taxonomy

LEVEL	EXPLANATION
Knowledge	The learner remembers and recognizes information, ideas, and principles in the basic form in which they were learned.
Comprehension	The learner translates, explains, and interprets information based on prior learning.
Application	The learner selects, transfers, and uses information, ideas, and principles in an abstract sense to complete a problem or task with a minimum of direction.
Analysis	The learner distinguishes, classifies and interrelates the constituent parts of a larger and integrated knowledge structure.
Synthesis	The learner originates, integrates, and combines multiple ideas and principles into a larger assembly that is new to him or her.
Evaluation	The learner makes judgments, appraises, assesses, or critiques the merits and validity of ideas.

3.2. Revised Bloom's Taxonomy

To add relevance for students and teachers, Lorin Anderson and David R. Krathwohl along with a group of psychologists came up with revised bloom's taxonomy (Krathwohl, 2002). In revised bloom's taxonomy writers changed the nouns listed in original taxonomy into verbs (Fuller et al., 2007). Though the changes in revised Bloom's taxonomy are minor, they are quite important and occurred in three categories: terminology, structure and emphasis (Forehand,

2010). Figure 4 shows the 6 levels of the cognitive domain in the revised Bloom's taxonomy and a brief summary of each levels is explained in table 2.

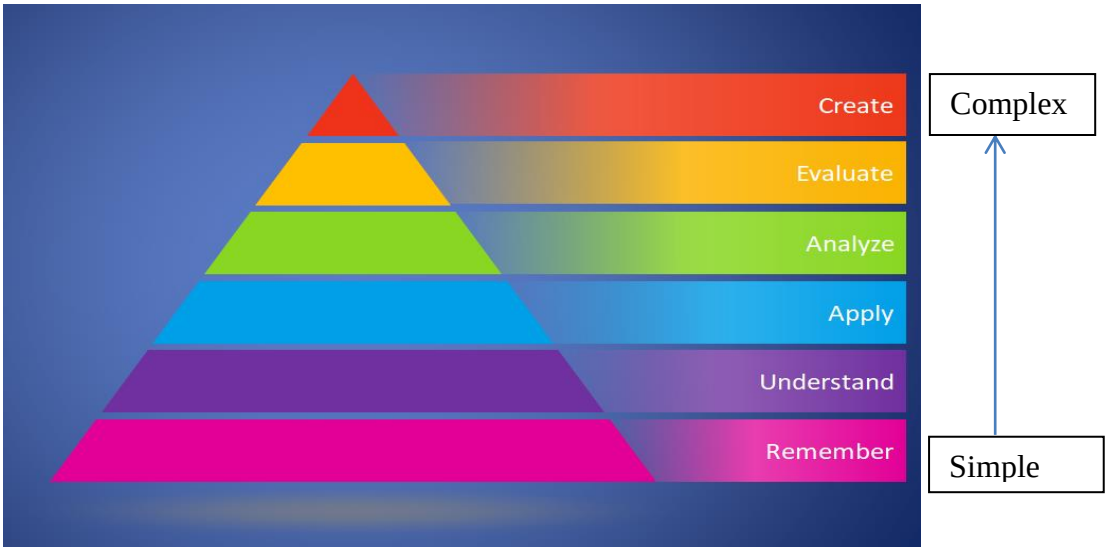

Fig 4. Revised Bloom's Taxonomy

Table 2. The Revised Bloom's Taxonomy

CATEGORY	EXAMPLES, KEY WORDS (VERBS), AND TECHNOLOGIES FOR LEARNING
Remembering: Recall or retrieve previous learned information.	**Examples**: Recite the name of a computer virus. Quote the definition of computer attacks. Recite the list of trusted software. **Key Words**: defines, describes, identifies, knows, labels, lists, matches, names, outlines, recalls, recognizes, reproduces, selects, states **Technologies**: book marking, flash cards, rote learning based on repetition, reading, memory games

Table 2. The Revised Bloom's Taxonomy (continued)

CATEGORY	EXAMPLES, KEY WORDS, AND TECHNOLOGIES FOR LEARNING
Understanding: Comprehending the meaning, translation, interpolation, and interpretation of instructions and problems. State a problem in one's own words.	**Examples**: Rewrite the principles of test writing. Explain in one's own words the steps that happen in a phishing attack. Translate an equation into a computer spreadsheet. **Key Words**: comprehends, converts, defends, distinguishes, estimates, explains, extends, generalizes, gives an example, infers, interprets, paraphrases, predicts, rewrites, summarizes, translates **Technologies**: create an analogy, participating in cooperative learning, taking notes, storytelling, Internet search
Applying: Use a concept in a new situation or unprompted use of an abstraction. Applies what was learned in the classroom into novel situations in the work place.	**Examples**: Using a technique to remove a virus from an infected flash drive. Apply the techniques learnt and identifying an insecure website **Key Words**: applies, changes, computes, constructs, demonstrates, discovers, manipulates, modifies, operates, predicts, prepares, produces, relates, shows, solves, uses **Technologies**: collaborative learning, create a process, practice

Table 2. The Revised Bloom's Taxonomy (continued)

CATEGORY	EXAMPLES, KEY WORDS AND TECHNOLOGIES FOR LEARNING
Analyzing: Separates material or concepts into component parts so that its organizational structure may be understood. Distinguishes between facts and inferences.	**Examples**: Troubleshoot a piece of equipment by using logical deduction. Recognize logical fallacies in reasoning. Gathers information from a department and selects the required tasks for training. **Key Words**: analyzes, breaks down, compares, contrasts, diagrams, deconstructs, differentiates, discriminates, distinguishes, identifies, illustrates, infers, outlines, relates, selects, separates **Technologies**: Fishbowls, debating, questioning what happened, run a test on to how a particular technique solves the problem
Evaluating: Make judgments about the value of ideas or materials.	**Examples**: Select the most effective solution to protect the sensitive data. Hire the most qualified candidate. Explain and justify a new budget. **Key Words**: appraises, compares, concludes, contrasts, criticizes, critiques, defends, describes, discriminates, evaluates, explains, interprets, justifies, relates, summarizes, supports **Technologies**: survey, blogging

Table 2. The Revised Bloom's Taxonomy (continued)

CATEGORY	EXAMPLES, KEY WORDS AND TECHNOLOGIES FOR LEARNING
Creating: Builds a structure or pattern from diverse elements. Put parts together to form a whole, with emphasis on creating a new meaning or structure.	**Examples**: Write a manual for having the best cybersecurity practices for an IT industry. Design a machine to perform a specific task. Integrates training from several sources to solve a problem. Revises and process to improve the outcome. **Key Words**: categorizes, combines, compiles, composes, creates, devises, designs, explains, generates, modifies, organizes, plans, rearranges, reconstructs, relates, reorganizes, revises, rewrites, summarizes, tells, writes **Technologies**: Create a new security model, write an essay, network with others

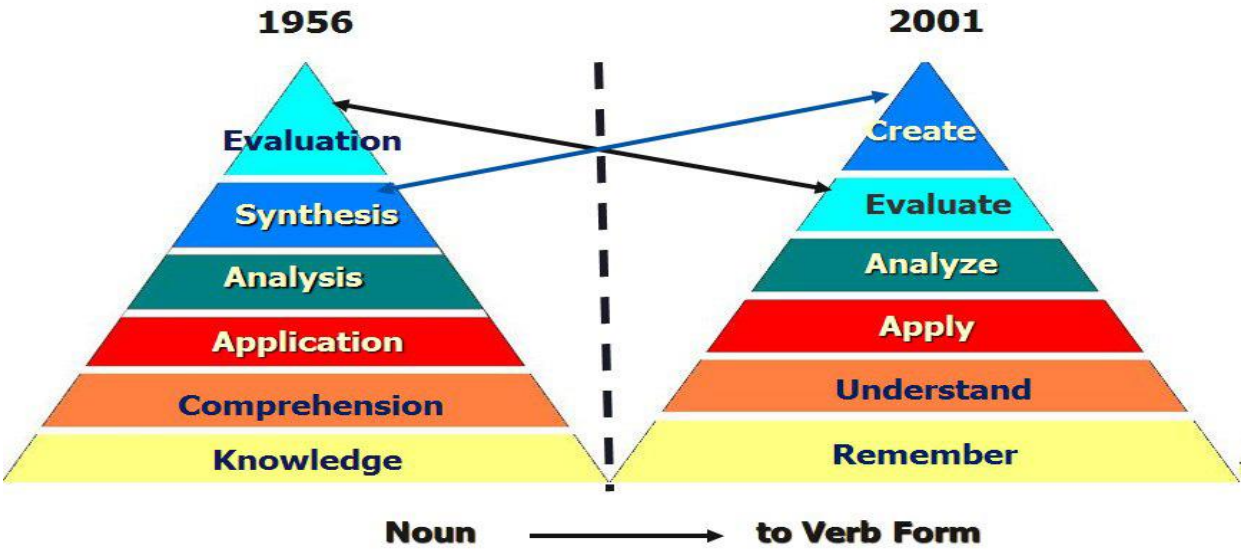

Fig 5. Comparison Between Original and Revised Bloom's Taxonomy

3.2.1. Cognitive Processes and Levels of Knowledge Matrix

Bloom's Revised Taxonomy not only improved the usability of it by using action words, but added a cognitive and knowledge matrix. While Bloom's original cognitive taxonomy did mention three levels of knowledge or products that could be processed, they were not discussed very much and remained one-dimensional.

- **Factual** - The basic elements students must know to be acquainted with a discipline or solve problems.
- **Conceptual** – The interrelationships among the basic elements within a larger structure that enable them to function together.
- **Procedural** - How to do something, methods of inquiry, and criteria for using skills, algorithms, techniques, and methods.
- **Metacognitive** – Knowledge of cognition in general, as well as awareness and knowledge of one's own cognition.

When the cognitive and knowledge dimensions are arranged in a matrix, as shown below, it makes a nice performance aid for creating performance objectives.

Table 3. The Structure of Cognitive Domain 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						

4. GAME DESIGN

This chapter is for explaining the detailed design of the game DodgeTheThreats and also about Buildbox which is the tool used to build DodgeTheThreats. Before explaining the game design it is necessary to understand the fundamental elements of a video game.

4.1. Typical Game Architecture

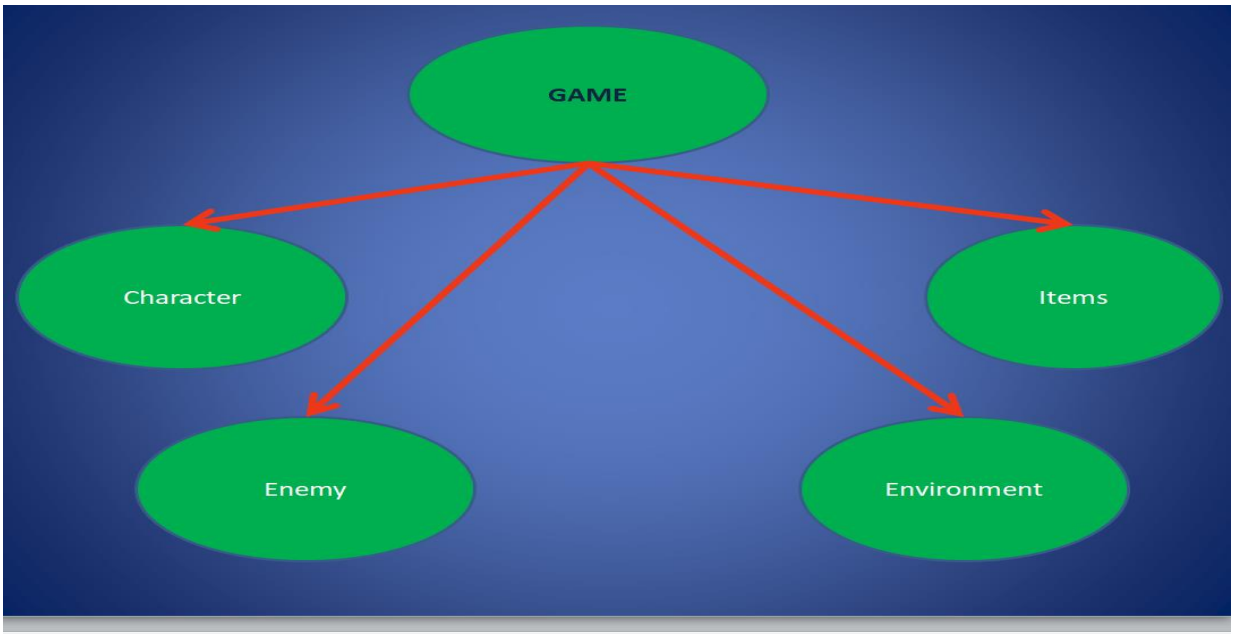

Fig 6. Architecture of a Typical Game

An archetype of a video game as shown in figure 6 consists of a character, a set of enemies, the environment and some items that can be collected by the character.

- Character is the entity that a user playing the game has control over.
- An enemy is the entity that tries to destroy the character.
- Environment is the scene where the fight between the character and the enemy takes place.
- Items are those entities that either help the character or create problems

4.2. Buildbox

Buildbox software allows the game development by focusing on the archetypical elements of a game. Buildbox was founded by Trey Smith in August 2014. It is a drag-and-drop game building software and focused on game creation. The main features of Buildbox are the image drop wheel, asset bar, option bar, collision editor, scene editor, monetization options and sliders that change the physics within the game. The user can change or edit the character or multiple characters from the character settings, edit or change environmental settings (gravity, friction) create multiple worlds and levels, create a coin system, power ups, checkpoints, change the user interface and buttons with Node Editor Menu, animate objects, create banner and video ads, export for different platforms with one click, store the source code, edit character and object components and do many other things.

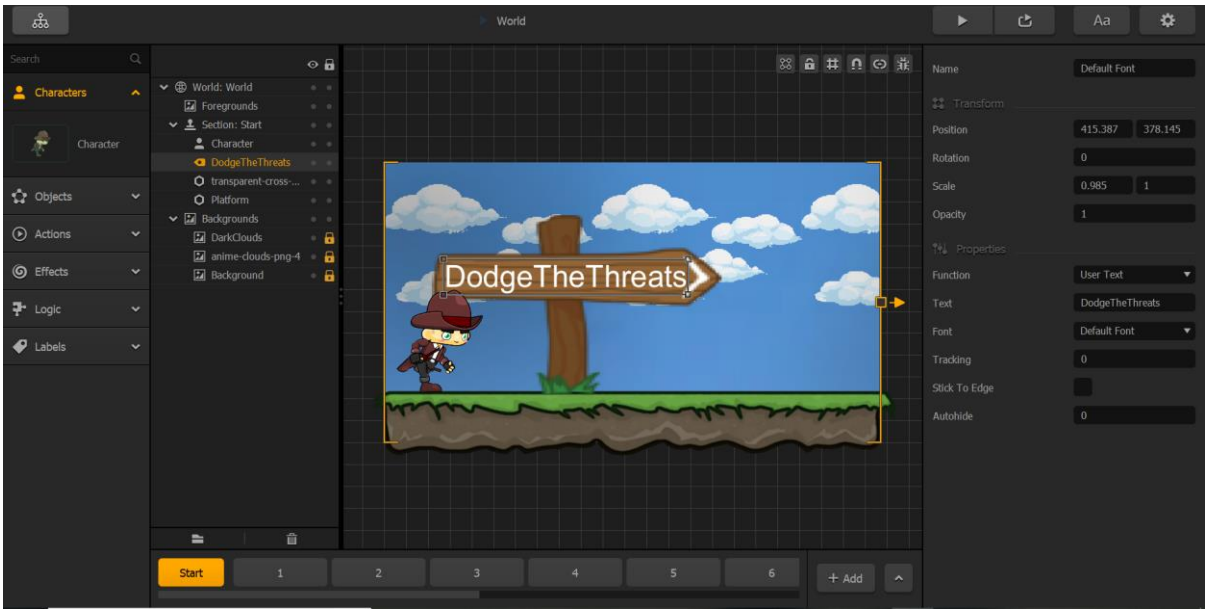

Fig 7. Buildbox Scene Editor Screen

The major UI in Buildbox consists of

- Scene Editor - This is the main screen of the build box. It is the place where scenes of a game are edited. It is possible to drag and drop any object and set it either as a character, enemy, or some item.
- Node Menu Editor - The node menu editor allows complete customization of the game layout. It allows adjusting the settings to choose all of the menu screens that are necessary.

The environment can have a background set and can have multiple layers of images. When a character entity is added to the game, following main properties can be set.

1. Name - Used to refer the object
2. Collision Shape - This is necessary for setting the boundary of the object which decides as to when it collides with other objects so that necessary impact happens.

For animations Buildbox allows uploading a single png file or a set of png files as frames that constitute the particular animation. The animations for the character include -

3. Default Animation - This decides how the character appears when he is doing nothing.
4. Shooting Animation - The animation of the character when he fires a weapon
5. Bullet Animation - This is the animation to run for the bullet after the character fires a weapon.
6. Jump Animation - This is the animation to run when Character is jumping.
7. Move Animation - This is the animation to run when Character is moving. This is useful if the player has a game with a bipedal character can stand still, or run. In which case the default animation will be the character standing still, and this animation will show the character running.
8. Defeated Animation - This is the animation to run when Character dies.

9. Jump Sound - Accepts MP3 file and is the sound played when the character is jumping.
10. Shoot Sound - Accepts MP3 file and is the sound played when the character is shooting.
11. Defeated Sound - Accepts MP3 file and it is the sound played when the character dies
12. Ground Collision - MP3 file - played when character collides with the ground.

Other entities including enemies, platforms, physics object etc. have similar properties like the character depending on their purpose in the game.

- Actions - They are a set of items that has a particular effect on the character, enemy or the environment. The list of action items include -

1. Coin - do nothing but add Reward number of coins to the player's coin collection.
2. Kill All Enemies - Kill all objects of type Enemy, that have Destroy set to "Destroy Character" and are active (i.e. objects are not asleep).
3. Invincibility - make player invincible for a time, and will kill enemies on contact.
4. Powerup Magnet - suck Powerup Actions (such as coins and abilities, but excluding Checkpoints) toward the character while active.
5. Strike - when collected, a button when pressed will kill enemies in contact with the player.
6. Set Checkpoint - set a checkpoint that will be used for Restart from Checkpoint button.
7. Next Checkpoint - move player character to next checkpoint.
8. Restart Checkpoint - give ability to restart at last checkpoint.
9. Effects - To make more dynamic animations. Buildbox has the following game effects.
10. Trail - Trail can be used to show creepy enemy tentacles, waving grass, smoke, etc.
11. Flag - A flag is just what it sounds - an image that appears to be rippling in a breeze. But the effect can be used to animate jellyfish or similar.

12. Particle - can produce destroy animation like smoke, fire, falling debris etc.

Game created in Buildbox can be exported as a gaming application in Windows store, iOS, Steam, Android Store, Samsung Store and Amazon Store (with support for the Amazon Fire HD, Fire Phone and Fire TV) or as a Windows exe/OSX. There is a Buildbox forum for the community of game developers using Buildbox that discuss and share solutions to problems that arises during development.

4.3. The Game – DodgeTheThreats

Figure 8 shows the node menu editor of DodgeTheThreats. It shows all the available screens in the game and how the player can navigate by clicking the navigation buttons.

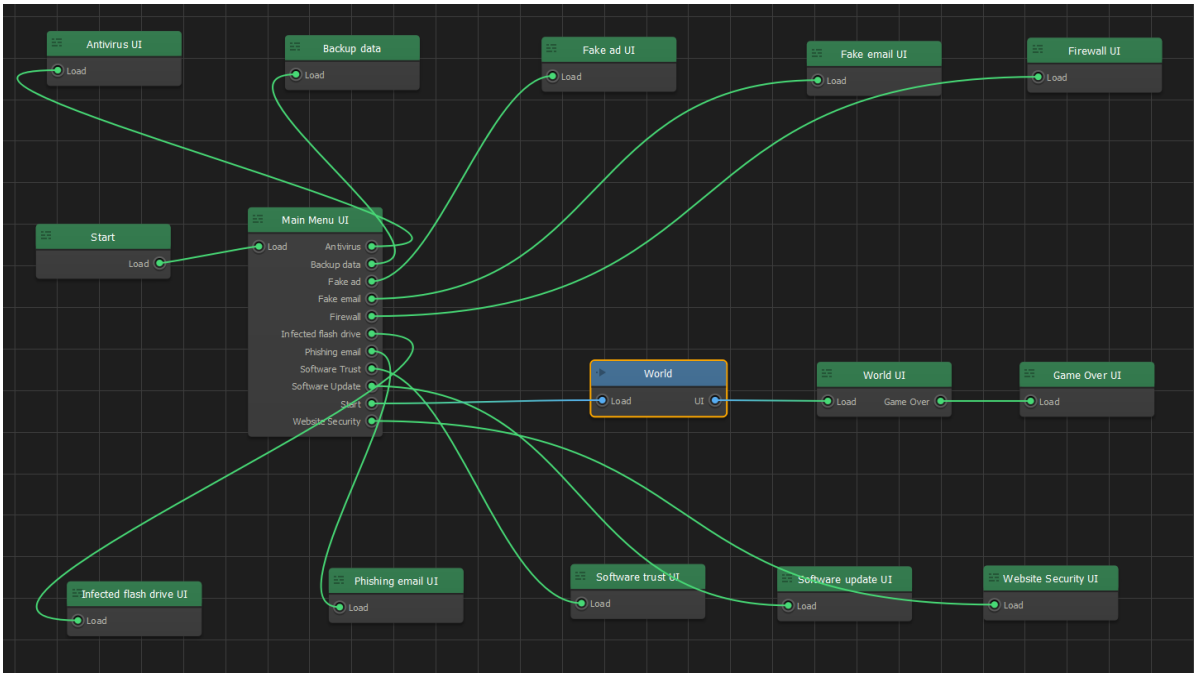

Fig 8. DodgeTheThreats Game Flow Diagram

The game flow is as follows.

1. When the player launches the game he can either click on the icons or on start button as shown in figure 9.

Fig 9. DodgeTheThreats Start Screen

2. If he clicks on any of the icons he is taken to a page that explains him about the icon that he clicked as shown in figure 10.

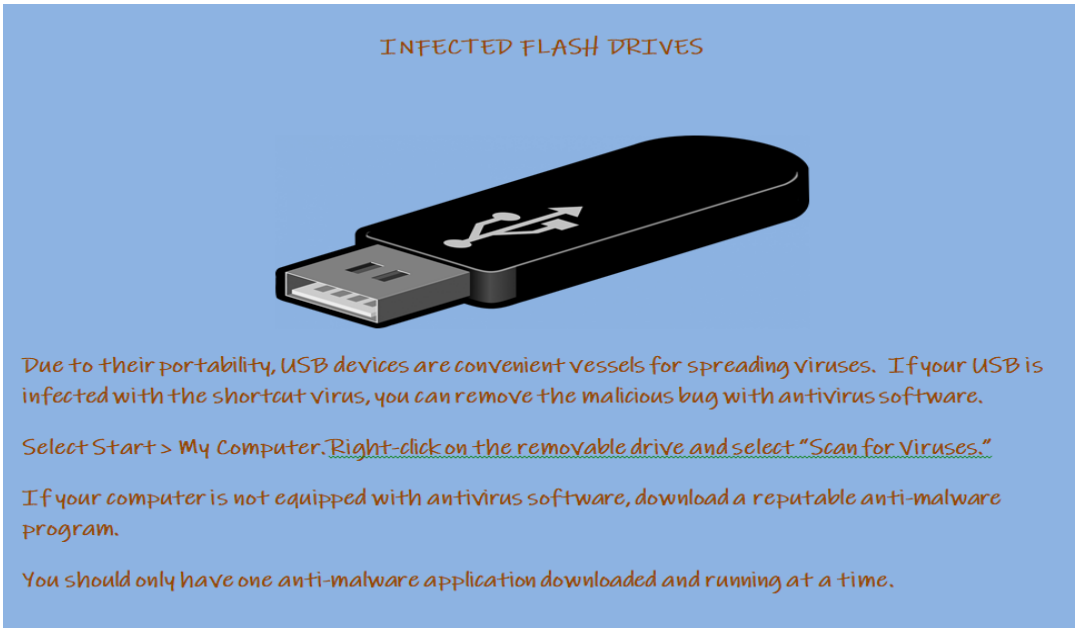

Fig 10. DodgeTheThreats Icon Information Screen

3. If the player clicks on the start button the game starts. Figure 11 shows start scene of the game.

Fig 11. DodgeTheThreats Game Start Screen

4. When the game is over. He is presented with restart and the main menu navigation button. Figure 12 shows game over screen.

Fig 12. DodgeTheThreats Game-Over Screen

5. The restart button restarts the game and mainmenu button takes him to the opening page again.

The player playing the game initially plays to familiarize himself with all the icons. Once that happens, he will play the game to score more points. To score more points he will have to

understand what the icons mean. In order to understand the properties of the icons he has to read what the icons stand for. The information regarding the icons is very precise and very practical that the user faces. Once they understand what icons are threats and what icons are friendly to them. It will help the player with two purposes. Firstly it helps him to score more points and secondly and more importantly, learn a new concept in cybersecurity.

The player keeps on playing with an aim to score more points which will happen only if he understands the meaning of the icons. Understanding the meaning of an icon implies understanding a concept in cybersecurity.

After the end of the game the player can successfully recognize an icon and understand what it stands for. With this knowledge there is a hope that he applies the gained knowledge from the game to the real life scenarios. Below are some of the explanations of the scenes in the game.

1. The scene contains two icons on two platforms that represent http and https. If the player jumps on https icon he survives but if he jumps on http icon he dies.

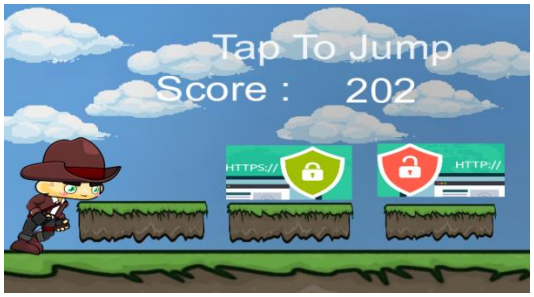

Fig 13. Encountering Websecurity Icon in DodgeTheThreats

2. In another scene the player has to grab an antivirus icon in order to kill a Trojan virus which tries to approach him and kill him

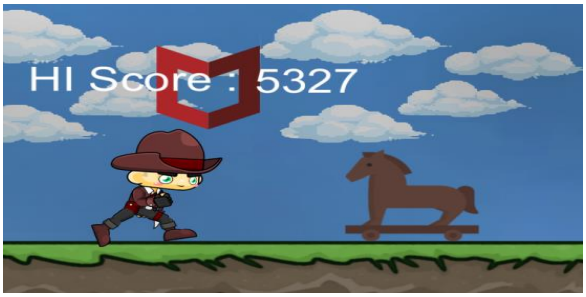

Fig 14. Encountering Antivirus Icon in DodgeTheThreats

3. The player is presented with a fake ad that tells him that he has won an award and which attracts him to grab. But when he picks it he dies.

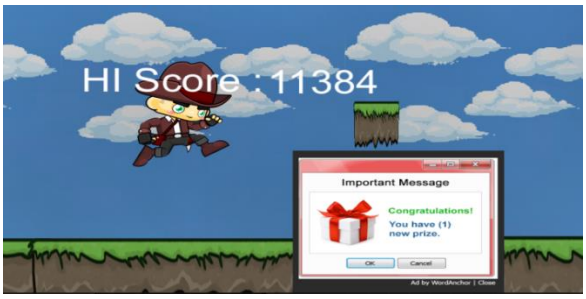

Fig 15. Encountering Fake Ad Icon in DodgeTheThreats

4. The player sees a series of icons that act as a bridge between 2 platforms. The player should step on only those icons that are friendly to him. If he steps on phishing email icon he dies.

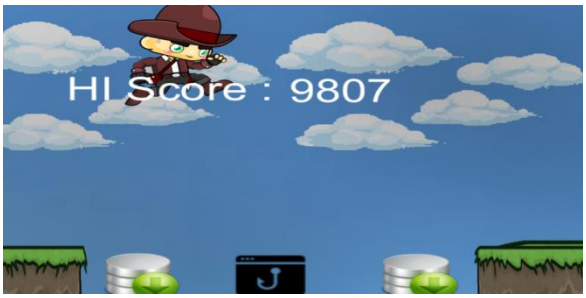

Fig 16. Encountering Phishing Email Icon in DodgeTheThreats

5. The player encounters a hovering flash drive which contains a virus which he has to jump or else he dies.

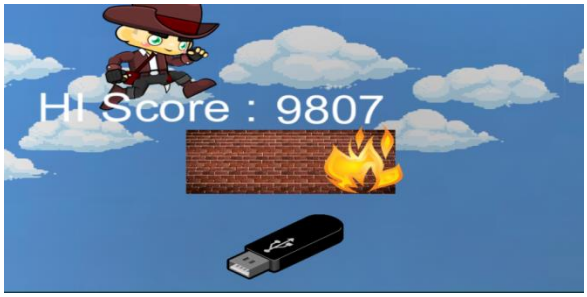

Fig 17. Encountering Flash Drive Icon in DodgeTheThreats

6. The player has to jump on Backup data icon which acts as a bridge between two platforms

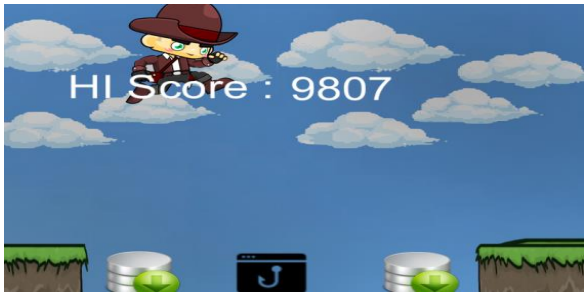

Fig 18. Encountering Backup Data Icon in DodgeTheThreats

7. A firewall should help the player to kill a swarm of unauthorized data that tries to kill the player.

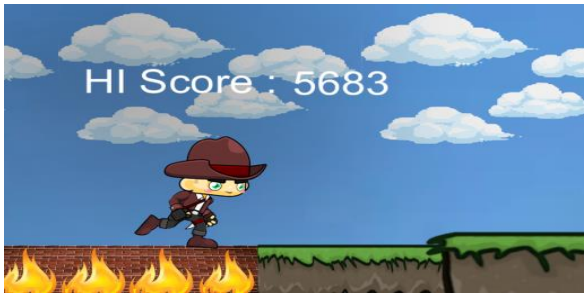

Fig 19. Encountering Firewall Icon in DodgeTheThreats

8. A software update is necessary to prevent the player from getting killed by an attacker.

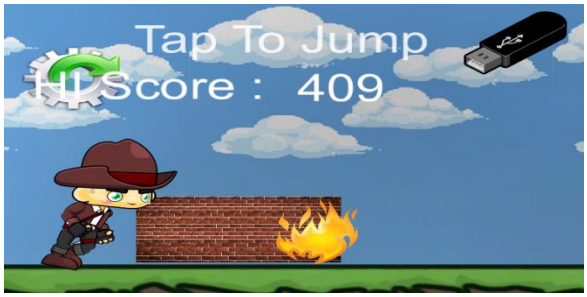

Fig 20. Encountering Software Update Icon in DodgeTheThreats

9. The player encounters another person holding a fake message. If he grabs it he is killed.

Fig 21. Encountering Fake Email Icon in DodgeTheThreats

10. A swarm of icons shows up and the player survives only if he collides with trusted software icon.

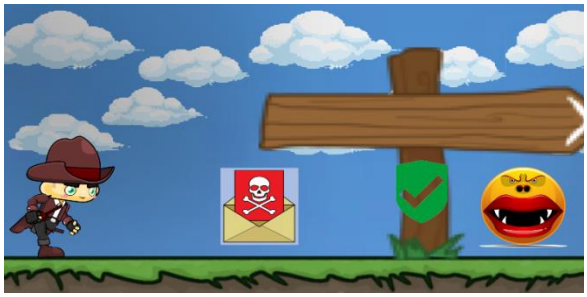

Fig 22. Encountering Trusted Software Icon in DodgeTheThreats

4.3.1. Achieving the Flow State in DodgeTheThreats

As discussed in the earlier section there are three conditions for achieving the flow state.

1. Goal
2. Balance

3. Feedback

- Goal - Since scoring is introduced in the game the goal in DodgeTheThreats is to set the highest score. This provides a goal for the player to aim.
- Balance - As the player proceeds in the game, the difficulty level of the game is increased. This provides a balance between the challenges faced and the player's skill.
- Feedback - Each time the player makes a correct decision by selecting the right icon he survives and each time dies he makes a bad decision he dies and this happens immediately. This is how the game provides the feedback.

Since all the three conditions are met, the player can achieve the flow state which is expected to enhance his/her learning.

5. INCORPORATING THE REMEMBER LEVEL AND UNDERSTAND LEVEL

Bloom taxonomy provides useful guidelines for developing effective online course materials for computer science topics (Ray, Denton, Beseman, & Nygard, 2004). In a similar manner, the game DodgeTheThreats also tries to follow the guidelines of Bloom's taxonomy.

5.1. Lower Order Thinking and Higher Order Thinking

Higher-order thinking skills are reflected by the top three levels in Bloom's Taxonomy i.e. Analyzing, Evaluating, and Creating. Lower-order thinking skills are reflected by the lower three levels in Bloom's Taxonomy i.e. Remembering, Understanding, and Applying. These levels are called so as they help learner in developing their fundamental knowledge of the subject being taught. On the other hand, Analyze, Evaluate, and Create combine to form the higher order thinking skills as they represent categories that goes beyond recalling and understanding the fundamentals of the concept. The higher order thinking skill helps learner to move toward an abstract knowledge of the subject. The game developed only accommodates for the first two levels of lower order thinking as incorporating higher order thinking is difficult.

5.2. Incorporating Remember Level

Remembering is when memory is used to produce or retrieve definitions, facts, or lists, or to recite previously learned information. The verbs associated with this level includes define, duplicate, list, memorize, recall, repeat, reproduce, state etc.

Initially the player plays the game and becomes familiar with the icons. Since the game makes the player play it again and again, he becomes familiar with the icons. The scenes in the game are set up in a way that requires some knowledge of the icons that the player sees. For example - In a particular scene the player is deceived by a fake email that says win 1000$ points but when he grabs it he is killed. In another scene the player has to jump between 2 platforms by using the available icons as a bridge between the platforms. But not all icons are safe. If he steps

on the wrong icon he dies. Each time he dies the player gets a purpose to understand what icons kill him and what will help him to survive in the game. This information can be obtained by clicking the icons in the main menu. By repeatedly playing the game he will be able to recall the icons.

When the player clicks on the icons and reads the information regarding the icons, that knowledge would help the player navigate to greater distance in the game and thereby allows him to score higher points. The score in the game is decided by the distance travelled by the player in the game from the starting point. Only when the player has certain knowledge regarding the icons he will be able to score higher points. As the saying goes "A picture is worth a thousand words" the game developed makes use of icons which the player becomes familiar by repeatedly playing the game.

The major objective of Remember level in the framework of current work is that the learner must first be informed with the knowledge of terminology associated with basic cybersecurity, i.e. the factual knowledge associated with basic cyber security which the game does it by repeatedly presenting the icons each time he plays. Once the player understands the icons information, the game also helps in retaining the information about its working since the player has to make use of the concept that he has learnt in the icon information screen during the game play. On the knowledge dimension of the taxonomy table remember level falls on the factual and conceptual category as shown in table 4 as the game successfully makes the player to remember the facts and concepts of the icons that he sees.

Table 4. Taxonomy Table for Remember Level

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

5.3. Incorporating Understand Level

Understanding level constitutes constructing meaning from different types of functions be they written or graphic messages or activities like interpreting, exemplifying, classifying, summarizing, inferring, comparing, or explaining. The verbs associated with this level include Classify describe, discuss, explain, identify, locate recognize, report, select, translate, paraphrase etc. When the user clicks on an icon in the main menu the player sees information about the icon. The information presented is something that the user commonly experiences. For example the information about phishing email is as below-

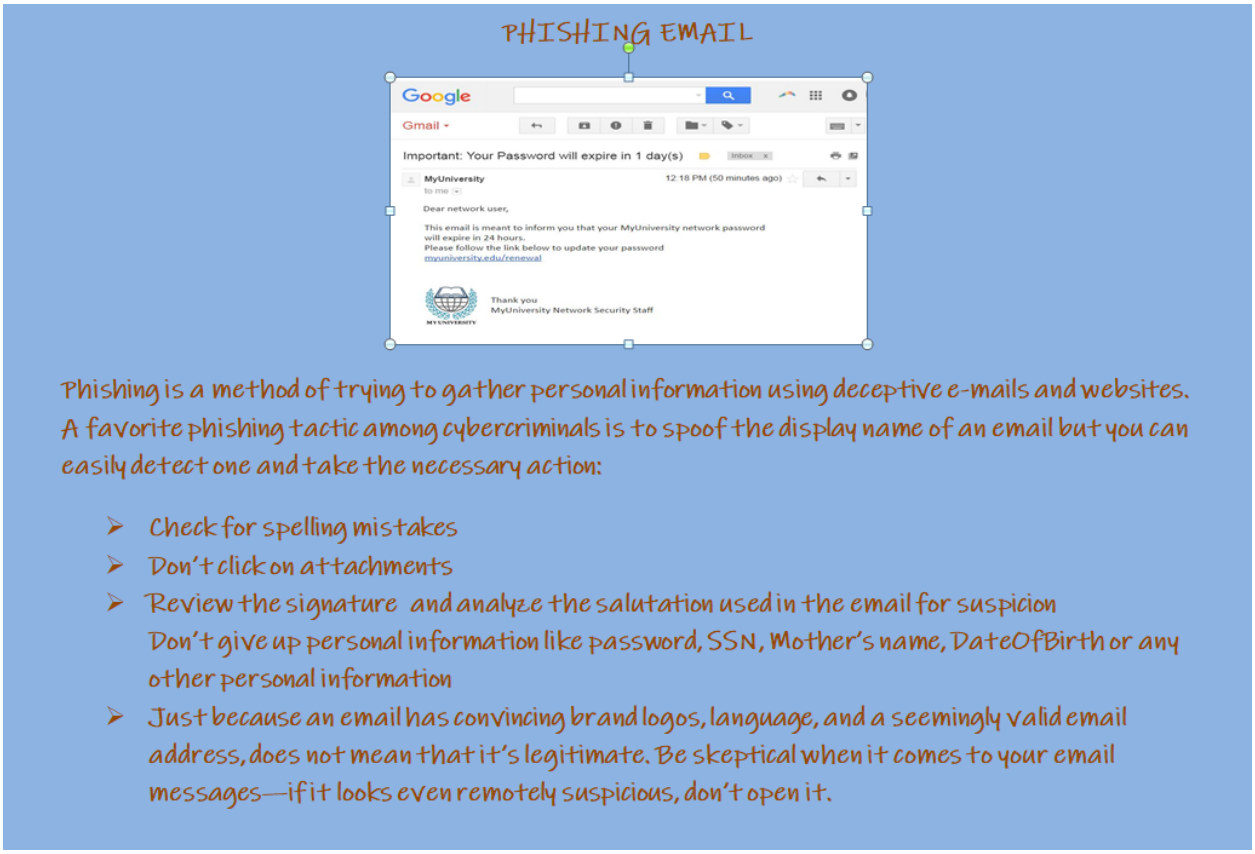

Fig 23. Encountering Phishing Email Icon Info Screen

By reading the above information he understands those phishing icons is a threat in the game and take his decision accordingly.

The Understand level involves explanation of the key concepts and theories related to the basic cybersecurity which the game achieves by providing the information in the icon info screen using various examples, diagrams or graphics etc. Thus, on the knowledge dimension of the Taxonomy table Understand level falls under the category of factual knowledge and conceptual knowledge as shown in table 5.

Table 5. Taxonomy Table for Understand Level

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

6. CONCLUSION

Billions of dollars have already been lost, and there is a massive gap in the cybersecurity workforce. Traditional methods often lack user input, cannot be updated, and are easily overlooked by users. As cybersecurity is a highly technical topic, it requires an engaging form of training that motivates users to learn about abstract concepts. Research results shows that video games are popular and flow theory explains the motivation for the video games. Initial research into serious games for cybersecurity training and awareness has shown increases in player motivation and learning. The next challenge at hand is how the cybersecurity serious game should be designed? Bloom's revised taxonomy divides the educational material in increasing levels of complexity.

The game DodgeTheThreats incorporates the educational objectives of the first two levels of the revised Bloom's taxonomy for teaching the concepts of basic cybersecurity. Since the game is addictive in nature it motivates the player to play it again and again. The player becomes familiar with the icons and that is how the game incorporates the remember level by making the player remember the facts and concepts of cybersecurity. The Understand level involves explanation of the key concepts and theories related to the basic cybersecurity which the game achieves by providing the information in the icon info screen using various examples, diagrams or graphics. The current version of DodgeTheThreats there is usage of just ten icons. But if the count of the icons is increased to a hundred icons then the novelty of the game also increases and the player can have the opportunity to learn many more topics of cybersecurity. One of the major design challenges in the game is setting up the scenes in a way that it has something to teach. There is a huge scope for innovation of combining the complex learning concepts but still protecting the entertaining aspect of the game.

7. REFERENCES

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, *33*(3), (pp. 237–248).

Anderson, L. W., Krathwohl, D. R., Airasian, P. W., Cruikshank, K. A., Mayer, R. E., Pintrich, P. R., … Wittrock, M. C. (2001). A taxonomy for learning, teaching, and assessing: A revision of Bloom's taxonomy of educational objectives, abridged edition. *White Plains, NY: Longman*.

Bloom, B. S. (1956). *Taxonomy of Educational Objectives Book 1: Cognitive Domain*. New York: David McKay Co Inc.

Bloom, B. S., Engelhart, M. D., Furst, E. J., Hill, W. H., & Krathwohl, D. R. (1956). *Taxonomy of educational objetives: the classification of educational goals: handbook I: cognitive domain*. New York, US: D. Mckay.

Carlson, E. L. (2006). Phishing for elderly victims: as the elderly migrate to the Internet fraudulent schemes targeting them follow. *Elder LJ*, *14*, (p. 423).

Chen, M., & Johnson, S. (2004). Measuring Flow in a computer game simulating a foreign language environment. Unpublished Article. Retrieved from http://markdangerchen.net/pubs/flow_in_game_simulating_fle.pdf

Cone, B. D., Irvine, C. E., Thompson, M. F., & Nguyen, T. D. (2007). A video game for cyber security training and awareness. *Computers & Security*, *26*(1), (pp. 63–72).

Csikszentmihalyi, M., Abuhamdeh, S., & Nakamura, J. (2014). Flow. In *Flow and the foundations of positive psychology* (pp. 227–238). Springer.

Entertainment Software Association. (2017). *ESSENTIAL FACTS About the computer and video game industry*. Retrieved from http://www.theesa.com/wpcontent/%0Auploads/2017/04/EF2017_FinalDigital.pdf

Forehand, M. (2010). Bloom's taxonomy. *Emerging Perspectives on Learning, Teaching, and Technology*, *41*, (p. 47).

Frost, L. ; D. L. S. (2017). *2017 Global Information Security Workforce Study*. Retrieved from https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS-Report.pdf

Fuller, U., Johnson, C. G., Ahoniemi, T., Cukierman, D., Hernán-Losada, I., Jackova, J., … Riedesel, C. (2007). Developing a computer science-specific learning taxonomy. *ACM SIGCSE Bulletin*, *39*(4), (pp. 152–170).

Ghazvini, A., & Shukur, Z. (2017). A Framework for an Effective Information Security Awareness Program in Healthcare. *International Journal of Advanced Computer Science and Applications (IJACSA)*, *8*(2), (pp. 193–205).

Goleman, D. (1996). Emotional Intelligence. Why It Can Matter More than IQ. *Learning*, *24*(6), (pp. 49–50).

Hagen, J., Irvine, C. E., & Thompson, M. F. (2009). *A Preliminary Study of Barriers to Engagement in CyberCIEGE*. Naval Postgraduate School Monterey CA Center for Information Systems Security Studies and Research.

Hense, J., & Mandl, H. (2014). Learning in or with Games? In *Digital systems for open access to formal and informal learning* (pp. 181–193). Springer.

Herr, C., & Allen, D. (2015). Video games as a training tool to prepare the next generation of cyber warriors. In *Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research* (pp. 23–29). ACM.

Jones, J., Yuan, X., Carr, E., & Yu, H. (2010). A comparative study of CyberCIEGE game and Department of Defense Information Assurance Awareness video. In *IEEE SoutheastCon 2010 (SoutheastCon), Proceedings of the IEEE SoutheastCon 2010 (SoutheastCon)* (pp. 176–180). IEEE.

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

Lewis, W. (2010). Serious use of a serious game for language learning. *International Journal of Artificial Intelligence in Education*, *20*(2), (pp. 175–195).

Live, M. W. (2017). *Mobile World Rankings*. Retrieved from https://www.mobileworldlive.com/featured-content/apps-home-banner/netflix-app-tops-revenue-ranking/

Nakamura, J., & Csikszentmihalyi, M. (2014). The concept of flow. In *Flow and the foundations of positive psychology* (pp. 239–263). Springer.

Norton. (2016). *Norton Cyber Security Insights Report*. *Norton Cyber Security Insights Report 2016*. https://doi.org/10.1038/ncomms4240

PWC. (2016). *PWC*. Retrieved from https://www.pwc.com/gx/en/economiccrimesurvey/%0Apdf/GlobalEconomicCrimeSurvey-2016.pdf

Ray, S., Denton, A., Beseman, C., & Nygard, K. (2004). Learning Theory and Styles in Online Computer Science Courses. In *2004 WSEAS Workshop: Engineering Education*.

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007). Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish. In *Proceedings of the 3rd symposium on Usable privacy and security* (pp. 88–99). ACM.

Zyda, M., Hiles, J., Mayberry, A., Wardynski, C., Capps, M., Osborn, B., … Davis, M. (2003). Entertainment R&D for defense. *IEEE Computer Graphics and Applications, 23*(1), (pp. 28–36).