CREU 2016-2017 Final Report: Using a Game to Teach About Phishing

CREU Team Mentor: Jingua Zhang, Winston-Salem State University
CREU Team Member: Patrickson Weanquoi, **Winston-Salem State University**
CREU Team Member: Jaris Johnson, **Winston-Salem State University**

I) Goals and Purpose

Cyber security education has become increasingly critical as we spend more of our everyday lives online. Research shows that college students are mostly unaware of many online dangers. It may be better to teach students about cyber security using their preferred medium, gaming. For this reason, we developed an educational 2D game called Bird's Life that aims to teach high school and college students, as well as general interest individuals, about phishing. Players will come to understand phishing attacks and how to avoid them in real world scenarios through a fun gaming context. The game can be deployed to multiple platforms such as PC, web and mobile devices. To measure the effect of this game on learning the concepts of cyber security, a pre-test, post-test and online survey were developed and used in the evaluation process. Initial evaluation shows that the game has positive impact on student learning.

II) Related Work

Securing ourselves online has been a focal point since the invention of Internet. A virtual attack on an individual through the use of computer has grown directly and also indirectly. There have been many scholarly works done to increase the awareness of cyber security [8, 10]. Many of our ideas originated from work done by scholars. One of those works involved the concept of attack and defense [8]. The intriguing aspect of their research was the incorporation of probability. The probability of the attacker executing their plans is unknown which makes the entire situation equally promising for both the attacker and the defender. Another scholarly work introduced a game based on strategy [10]. The game is in an environment where the leader (guard) has to protect its materials from the follower (robber). The leader has to make the first moves which is observed by the follower. What makes the concept of the game appealing is their use of predictability. The guard, whose patrol route is sometimes predictable by the robber route, can be changed by the player. This attack-defend game teaches the player a critical component of cyber security. Other related works we reviewed for guidance can be found at the end of this report under Related Works References.

III) Process

To begin, we had to game proficiency in Unity3d Game Engine. After a few weeks of getting acquainted with the software, we dived into the game's design. This was a very crucial part of our research because there were many ideas created for the game's design after viewing many scholarly works. Initially, our first design of the game was a 2D based game where the background of the scenes scrolls bottom-up. Due to complications of scaling and looping the background images at the same time, it was difficult to bring the ideas into fruition. We finalized the decision of making the game using the same previous idea, but instead of an upward background scroll, we decided on right-left background scrolling.

Furthermore, after deciding on the scrolling appearance of the game's background, we began development on the structure of the game. There are three main levels: Level 1: introduction of the game, Level 2: tips to protect against phishing, and Level 3: quiz questions.

a) Introduction of the Game

We have come to understand the importance of getting the player interested in the game. This section of the game gives us the opportunity to intrigue the player and encourages them to delve into the game. The purpose of this section is creating a dialogue between two birds. The conversation of the birds foreshadows the general ideas the player will learn throughout the game. In order to accomplish the dialogue between the birds, we hard coded the conversation in a C# class. The screenshot of this level is shown in the following Figure.

Figure 1. Gameplay Level #1

b) Tips to protect against phishing

This level is designed to have the player collect useful tips on how to avoid phishing attacks. The player will be prompted to collect five "gray worms" to obtain a tip. The player can use the rewards to purchase more health if it is low. Once all five tips have been collected, the player will enter the next level to test his/her knowledge of phishing. Screenshots for this level can be found in the following Figure.

Figure 2. Gameplay Level #2

This section of the game required significant amounts of programming because of things such as: freezing time, data structures, menus, animations, and physics:

- Freezing the time when needed was very essential to the game developing process. As a developer, giving and taking control from the player helps the game to flow smoothly. The idea of freezing the game helped solve many problems such as pausing the game to display certain objects, which is essential. The statement to pause the game had to be placed in a single Update() method of Unity. It was a bit frustrating because whenever a class wants to pause the game, it has to verify from the method that has the freeze statement.

- Data Structures was an essential concept to the game development process. We used ADT array bag to store the player's information. It was a new concept and difficult to implement, but its use was efficient and essential. The tips are stored in a bag and are drawn from highest index down when the player completes a task.

- There are many menus created in the game. Many of these menu include How to Play instructions, Tips, Fail and Win menus. There were some difficulties in detecting which menu to disable or enable based on the current context of the game. Since the update method in Unity calculates 60 frames per second, it was difficult to ensure the correct statements were not to be skipped or not reached.

- The animated objects in the game were created through Unity animations. We used a set of assets from the Unity Asset store and combined similar images to simulate a moving object.

- Since the game is a 2D based game, implementing the use of collision was bit simpler than in a 3D game. Nonetheless, we used a built-in component of Unity called "Box Collider2D" to accomplish our goal. Since there were a lot of objects moving within certain scenes, it could be difficult to identify which object is which. To allow Unity to detect the right object, we assigned tags to objects to separate them from each other.

- The main gameplay section contains five "stages" for the player. Each stage reveals a tip. At tip three and above the player gets a limited amount of time to complete each stage. We also included features such as a store where the player can go to replenish their health or time if needed.

c) Quiz Questions

The question scene is designed to test the player's knowledge of previous levels/sections concepts. Questions are randomly selected from the question pool. The player needs to get 80 percent correct to win the game. The screenshots for this level is shown in the following Figure.

Figure 3. Gameplay Level #3

This stage of the game has many similar implementations as the tips scene, but differs on the subject of data structures. Like the tips, the questions in the question scene were placed in an ADT array bag. However, in this setup, a question is randomly drawn out when the sequence is triggered.

Lastly, there are some classes in the game that are worth mentioning. One of those classes is the PlayerPrefsManager.cs. This class manages the saved data of the game. Such saved data includes the volume value, the unlock levels, and the name of the user playing the game. The class uses a built-in Unity HashMap found in the class PlayerPrefs.

IV) Results and Discussion

Throughout our time spent in research and development for our game, the primary goal we kept in mind was our learning objective of successfully teaching people basic cyber security concepts. The measure of our work success was centered on how well individuals unfamiliar with cyber security could grasp the information we presented in the game. Additionally, it centered on individuals' ability to answer questions intertwined within the gameplay solely based on the knowledge they just gained by playing. In order to collect and analyze information on the effectiveness of the game as

both a playing experience and a teaching tool, we decided to keep a data log. This log contained all of the information we deemed most relevant to assess the overall experience and usefulness of our game.

As previously stated, one main area of focus for us was assessing our game as a teaching tool. In order to accomplish this, we gathered two groups of students from Winston-Salem State University with no prior introduction to cyber security concepts. One group was from CSC1310 Computer Programming I class. The other group was from a fundamentals class, CSC3332 Fundamentals of Internet Systems. These two groups consisted of students whose classification ranged from Freshman to Junior. Once these groups were assembled, the assessment of our game could begin.

One of the first methods we decided could give an accurate representation of growth was a pre vs. post-test result examination. To accomplish this, we had both groups answer 5 questions about phishing. Then, students played the game from start to finish. After the gameplay, students will take a post-test that is identical to the pre-test. We then compared both scores to see if there were any improvements in overall performance. For the CSC1310 group, 8 out of 11 students showed improvement in their scores. The improvements ranged from 2 points to 8 points, with an average increase of 3.75 points for these individuals. The other 3 students' scores were still somewhat reassuring because they remained unchanged, with one student scoring 8 both times and the other two scoring 6 both times. The following figure shows the pre-test and post-test comparison.

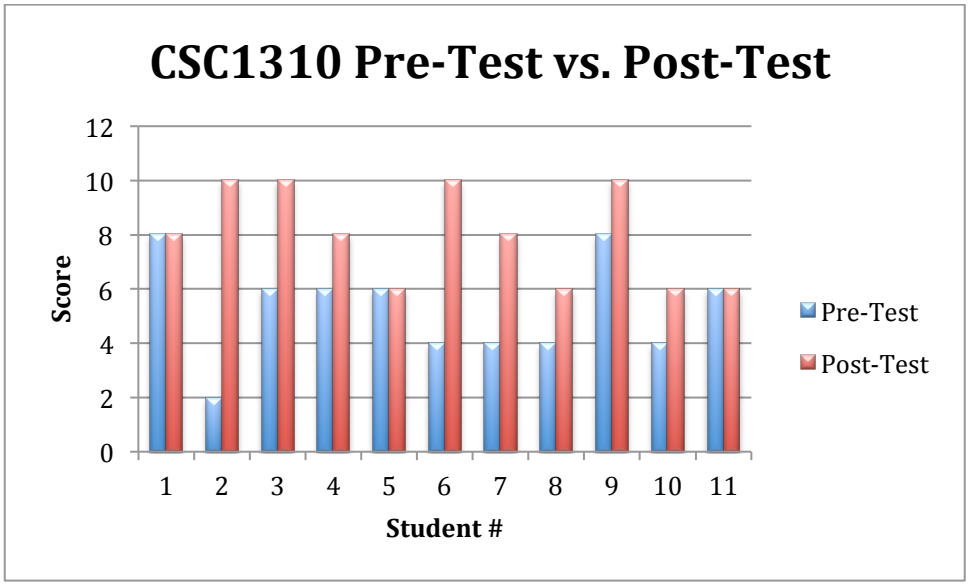

Figure 4. CSC1310 Pre-Test vs. Post-Test

Next, for the CSC3332 group we collected the same information. In this group, 10 out of 19 students showed improvement in their scores. The improvements ranged from 2 points to 6 points, with an average increase of 2.6 points for these individuals. 6 out of 19 students scores remained unchanged, with one scoring 6 both times, one scoring 8 both times, and four scoring a perfect 10 both times. Unfortunately, 3 students' scores decreased by 2 points. The main conclusion we gained from these

results is that the tips provided in the game do have a positive effect on players' understanding about phishing. Also, at the very least, the tips seem to reinforce the player's previous idea of what phishing could be to allow their answers to remain consistent. One thing we will be taking into consideration moving forward is how to refine the tips given to further decrease the possibility of confusing players and lowering their score. We will also look into what information could have made the tips more helpful in understanding phishing. The pre-test and post-test comparison for this group is shown in the following Figure.

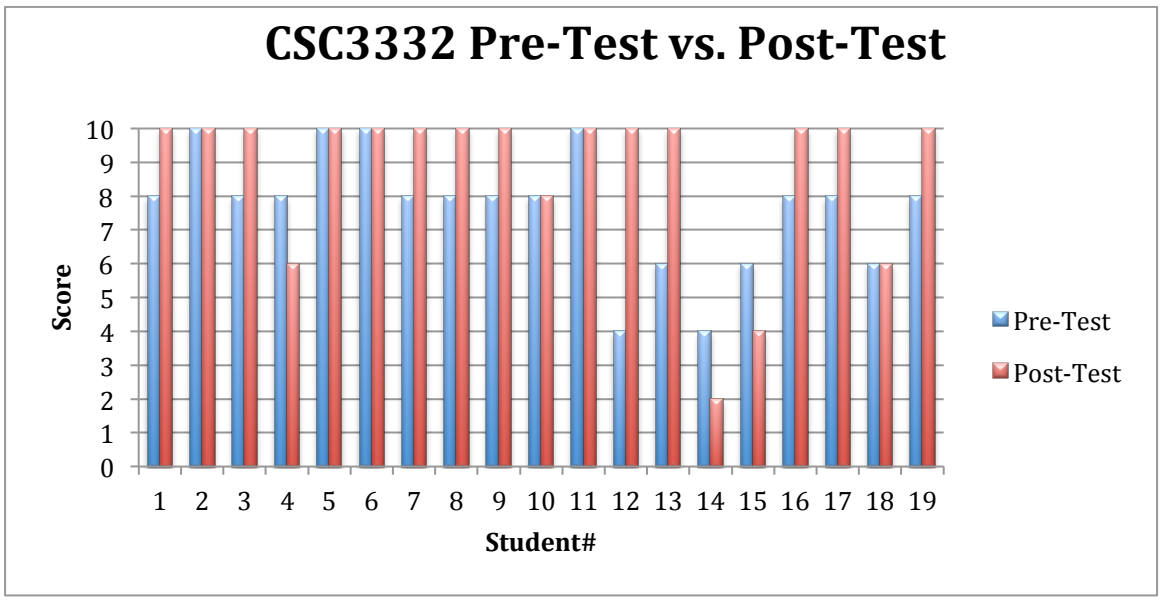

Figure 5. CSC3332 Pre-Test vs. Post-Test

In continuation, we also gave both groups the opportunity to anonymously give comments and feedback on the game as an overall playing experience. This was extremely helpful in directing us towards delivering a higher quality gameplay experience. One of the most consistent comments we received was to make the how-to-play instructions clearer. The second level contains a bomb launch mechanic that many people found difficult or confusing to use. To fix this, we rewrote the instructions on how to move the bomb forward and changed the cursor when over the bomb to make clear that launching is a scrolling action on PC, not clicking. There was also a suggestion for a boss level that we are currently taking into consideration. Outside of those suggestions, most of the feedback simply congratulated us on a well-made game for first time developers and stated that the tips were helpful in learning methods of protection against phishing. The survey results can be found in the following table:

Table I. Survey Results

Survey Questions	Percentage Agree
The game was enjoyable to play.	96%
The game was easy to play.	92%
I had a better understanding of Phishing attacks after playing the game.	90%
The game had a good balance between "play" and "learning" time.	95%
I was motivated to try hard to obtain Phishing Tips.	86%
I tried my best to answer quiz questions correctly in the game.	96%
The game provided immediate feedback when a mistake was made.	90%
I would like to learn more security concepts using games like this.	83%
I would recommend this learning game to other students.	97%

V) Future Work

Moving forward, we plan to continue exploring the realm of cyber security and providing methods and practices that can help people protect themselves online. Before moving on to our next project, we want to take time to refine and evaluate our current game to determine how to maximize its teaching ability. We want to do this because, if done correctly, our game can be introduced during the Fall 2017 semester as a teaching tool at WSSU. For incoming IT/CS students, or students who just want basic knowledge on protection against phishing, this game could become an enjoyable form of education. Afterwards, one of our upcoming research options we have discussed is DOS attacks. We plan to develop a game that is different from the type created to teach about phishing. This new game will be more of a simulation style experience that puts the player in the position of facing a DOS attack. We want to provide them with tips and guidance in real time as they face their "attack" to help them choose the best route towards protection.

VI) Web Links

Project website: http://compsci.wssu.edu/tip/creu
Patrickson Weanquoi Blog: http://patricksonweanquoi.wordpress.com
Jaris Johnson Blog: http://jjohnson514.wixsite.com/techtalk

VII) Presentations and Publications

- Poster presentation at Winston-Salem State University's Scholarship Day
- Plan to submit a poster for 2017 Grace Hopper Conference
- Plan to submit a paper to 2017 Special Interest Group for Information Technology Education Conference (SIGITE)

VIII) References

[1] Catuogno, L., and Alfredo D. S. "An Internet Role-game for the Laboratory of a Network Security Course" Proceedings of the 13th annual conference on Innovation and technology in computer science education (ITiCSE'08)

[2] Chapman, M., Tyson, G., Mcburney, P., Luck, M., and Parsons, S. "Playing Hide-and-seek: an abstract game for cyber security." *Proceedings of the 1st International Workshop on Agents and CyberSecurity - ACySE '14* (2014): 1-8.

[3] Compte, Alexis Le, David Elizondo, and Tim Watson. "A Renewed Approach to Serious Games for Cyber Security." *7th International Conference on Cyber Conflict: Architectures in Cyberspace*: *203-16, 2015*

[4] Cone, B.D., Irvine, C. E., Thompson, M. F., Nguyen, T. D. "A video game for cyber security training and awareness" *Computers & Security, Vol. 26, Issue 1, pg 63-72, 2007.*

[5] Guimaraes, M., Said, H. and Austin, R. "Using Video Games to Teach Security." Proceedings of the 16th Annual Joint Conference on Innovation and Technology in Computer Science Education - ITiCSE '11(2011): 346.

[6] Herr, C. and Dennis, A. "Video Games as a Training Tool to Prepare the Next Generation of Cyber Warriors." *Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research - SIGMIS-CPR '15* (2015).

[7] Jordan, C., Knapp, M., Mitchell, D., Claypool, M. and Fisler. K. "CounterMeasures: A Game for Teaching Computer Security." *2011 10th Annual Workshop on Network and Systems Support for Games*.

[8] Letchford, Joshua., Vorobeychik, Yevgeniy. (2013, May). *Optimal Interdiction of Attack Plans*. http://dl.acm.org/citation.cfm?id=2484955&CFID=665904379&CFTOKEN=22510146

[9] Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., Hong, J. " Teaching Johnny not to fall for phish", *ACM Transactions on Internet Techology, Vol. 10, Issue 2, 2010.*

[10] Mink, M., Freiling, F. C. "Is attack better than defense?: teaching information security the right way." *Proceedings of the 3rd annual conference on Information security curriculum development (InfoSecCD'06).*

[11] Paruchuri, P., Pearce, J.P., Marecki, J., Tambe, M., Ordonez, F., Kraus, S. "Playing games for security: an efficient exact algorithm for solving Bayesian Stackelberg games" *Proceedings of the 7th international joint conference on Autonomous agents and multiagent systems (AAMAS'08).*