



CREU Summer 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. We also created a 28 slide PowerPoint presentation and research paper for the SIGTE conference which breaks down our purpose in greater technical detail. Testing and analysis throughout our summer research shows that the game continues to have a positive impact on student learning, as well as shows promise from technology conferences.

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) must 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.

We also reviewed other scholarly works that focused on cybersecurity, particularly phishing. According to Patel and Luo, about 86% of home computer users are consistently targeted by hackers because of how unaware they are regarding the methods and seriousness of hacking. This information was very important to us because we realized these kind of users are mainly on the front line of attacks by hackers [5]. This was our solid reasoning behind ensuring our game could be played and understood by a general audience of a broad age range. Another work we reviewed that contributed to improving users understanding of phishing was a game called "What.Hack" (pronounced



What dot hack). The game shows a real-world representation of how phishing occurs. The game is simple in its concepts. The player is a new employee whose duty is to recognize any incoming emails as a phish or not. Some of the emails come from relative co-workers while others come from viral company [13]. The work that we found very intriguing was a project described in a journal from PhishingGuru [10]. The concept of their project was to actually send a phish email to users to see if they would click the links in the email and follow the instructions contained within. This was a clever idea because the user is unaware that the email is fake, making their reaction authentic, and providing the user a visual representation of what phishing is. The scholarly works mentioned above are some of the interesting related works we reviewed to help strengthen our understanding of phishing and, simultaneously, how to help players understand the dangers of cybersecurity attacks. Other related works we reviewed for guidance can be found at the end of this report under Related Works References.

III) Process

To begin, one main focus we had this summer was publishing the work we have done. We worked week after week to get our paper written, reviewed, revised, and published. After many weeks of alteration, our paper was accepted as a lightning talk paper.

Also, since forming our developmental process this past Fall, we have largely stuck to the same method for our summer research session. We continued to make improvements to the game's appearance and mechanics, such as revising the how to play instructions to be more clear and precise, creating and reformatting the pre and post-test menus, and creating a log-in system for players to track their progress. This was an important addition because it allows players to have records of their time of completion for the game and comprehension level for the questions. Additionally, we used our previous knowledge gained from the first player test to analyze the effectiveness of our current tips.

Otherwise, the overall structure of the game remained the same. There are still three main levels: Level 1: introduction of the game, Level 2: tips to protect against phishing, and Level 3: quiz questions.

Below we provide a detailed explanation of how we incorporated the pre and post test questions in the game.

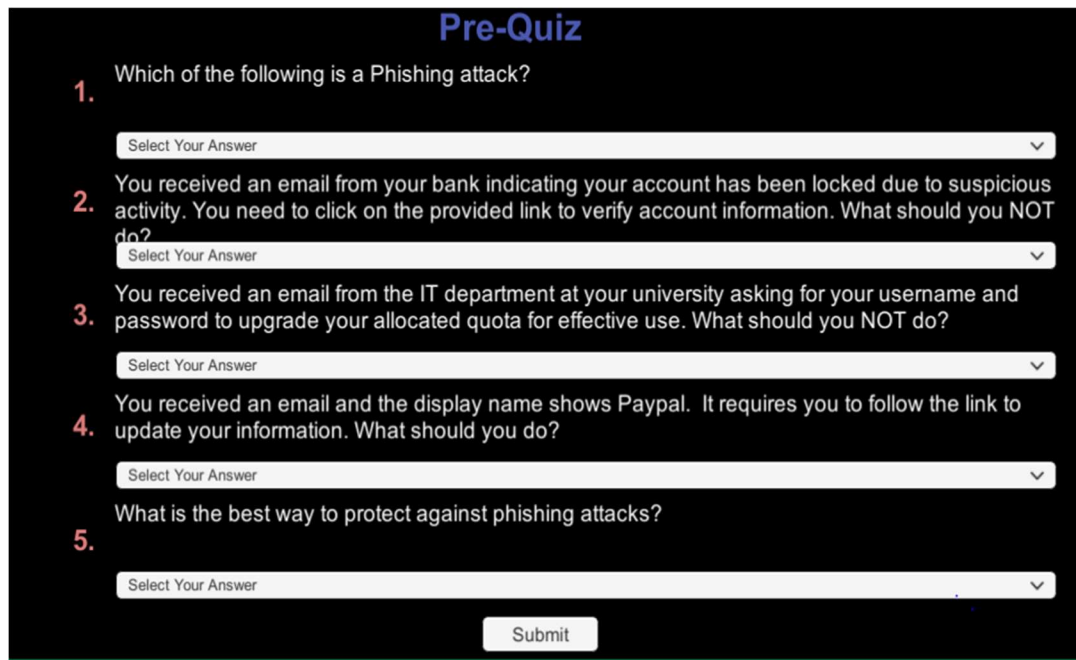
a. Pre-Test and Post-Test Design

There was a lot of work put into implementing the pre-test and post-test into the game. It required some intensive programming to correctly incorporate this idea. First, the design and placement of these tests had to be decided upon. We found the best location to place the pre-test was before the player officially starts the first level gameplay. Initially, we decided there was to be a button that the player had to click voluntarily to access the pre-test, but there were issues with that idea. Some players may choose not to click the button to take the test, therefore negating comparisons of their previous knowledge and their new knowledge. Therefore, we decided to display the pre-test automatically once the game begins. The post-test placement, on the other hand, was much simpler. We chose to place it after the questions scene is completed. The question



scene is the last level in the game, as well as the level where the player test their understanding of the game concepts. Having the post-test after this scene allowed for the player's new gained knowledge to remain fresh in their mind. There was no other alternate placement decided upon for this post-test.

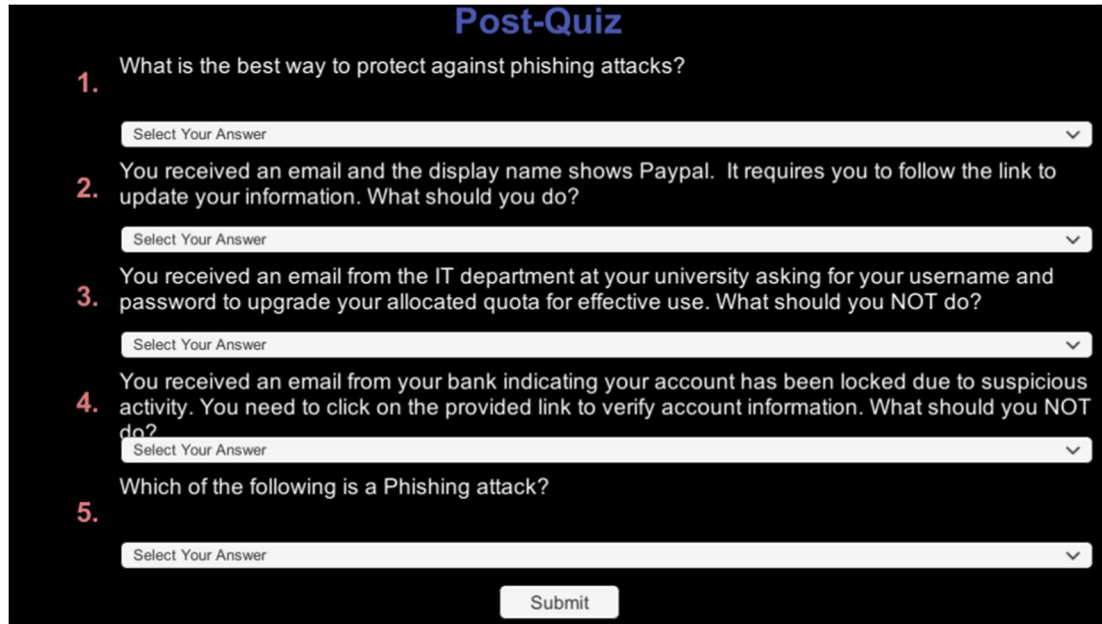
The structure of the tests is not the same as the questions scene. The design of the pre and post-test has a simpler formatted UI. The questions are all placed on the same panel. Each question has its answer choices beneath it in a dropdown format. Our initial idea was to develop a multiple-choice answer UI, but due to limited space, it made more sense to approach the problem this way from a visual aspect.



Pre-Quiz

1. Which of the following is a Phishing attack?
2. You received an email from your bank indicating your account has been locked due to suspicious activity. You need to click on the provided link to verify account information. What should you NOT do?
3. You received an email from the IT department at your university asking for your username and password to upgrade your allocated quota for effective use. What should you NOT do?
4. You received an email and the display name shows Paypal. It requires you to follow the link to update your information. What should you do?
5. What is the best way to protect against phishing attacks?

Figure 1: Pre-Test Design



Post-Quiz

1. What is the best way to protect against phishing attacks?
2. You received an email and the display name shows Paypal. It requires you to follow the link to update your information. What should you do?
3. You received an email from the IT department at your university asking for your username and password to upgrade your allocated quota for effective use. What should you NOT do?
4. You received an email from your bank indicating your account has been locked due to suspicious activity. You need to click on the provided link to verify account information. What should you NOT do?
5. Which of the following is a Phishing attack?

Figure 2: Post-Test Design

b. Pre-Test and Post-Test Programming

The programming aspects of the game required a lot of work and time as well. First, we had to hard code the test questions and answers into a C sharp (C#) class called "QuestionImplementing.cs" When the game starts, each question and answer that is hard coded in "QuestionImplementing.cs" is placed in its individual "QuestionArray.cs" class by using a "for loop." By using this technique, we created many opportunities to use many different style of data structures. Other options we could have used included link list, bag, queue, and or stocking. We decided to first display the questions on the screen by creating an array of gameobject. After placing each question in the gameobject, which has a text component, our next goal was to add the answer choices in a dropdown panel. Since each "QuestionArray.cs" has a question and a list of answers, we copied the list answers to the dropdown panel. What made this entire process promising is that each dropdown panel takes in a list of string items or sprites.

```
//1
phishingQuestions[0] = "Which of the following is a Phishing attack?";
phishingAnswer1[0, 0] = "Select Your Answer";
phishingAnswer1[0, 1] = "e";

phishingAnswer1[1, 0] = "An email that asks you to purchase something that you don't want";
phishingAnswer1[1, 1] = "0";

phishingAnswer1[2, 0] = "A website that contains a malware";
phishingAnswer1[2, 1] = "0";

phishingAnswer1[3, 0] = "An email that tricks someone into providing sensitive information";
phishingAnswer1[3, 1] = "1";
```

Figure 3: A question and its Answer choice hard coded in C# QuestionImplementing Class



```
public QuestionArray(string q,string[,] array)
{
    question = q;
    answers = array;
    for (int i = 0; i < 4; i++)
    {
        singleAnswers.Add(array[i, 0]);
    }
}
```

Figure 4: Copying each question and answer choice to it QuestionArray class

```
questionText[0].text = questionArray[0].getQuestion();
questionText[1].text = questionArray[1].getQuestion();
questionText[2].text = questionArray[2].getQuestion();
questionText[3].text = questionArray[3].getQuestion();
questionText[4].text = questionArray[4].getQuestion();
```

Figure 5: Displaying questions and answer choices to screen

```
for (int eachDropDown = 0; eachDropDown < 5; eachDropDown++)
{
    dropDown[eachDropDown].AddOptions(questionArray[eachDropDown].getSingleAnswer());
}
```

Figure 6: Adding each question and answer choice in DropDown Panel

Once all questions and answer choices have been displayed on the screen, the next step was to document the player's response to each question answered. This step was simpler than we anticipated. When the player is done answering all the questions, a "submit" button is at the bottom of the screen. When this button is clicked, a method is called which creates a text file and places the player's responses in it.

```
bool notanswer = false;
for(int i=0; i<5;i++)
{
    if (dropDown[i].captionText.GetComponent<Text>().text.Equals("Select Your Answer"))
    { notanswer = true; }
    userAnswers1.Add(dropDown[i].captionText.GetComponent<Text>().text);
}
if(notanswer)
{
    return;
}
else
{
    getCorrectAnswers();
    completeScreen();
}
```

Figure 7: Copying copy of player response to Text file

The same process was used for the post-test. But this time, before each question and answer choice is displayed, we decided to alter the order. Therefore, the same classes, methods, and gameobjects were used.



IV) PowerPoint Presentation and Game previews video

In October, a presentation is to be given during a conference in New York. We began preparing a ten (10) minute presentation that covers the research we have done during up until this summer.

We also created a video preview for the conference which will illustrate the many different features of the game.

V) 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. 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 the information we deemed most relevant to assess the overall experience and usefulness of our game. This result is a text file recording of the player's response to the pre and post test questions.

One main area of focus for us was assessing our game as a teaching tool. To accomplish this, we used the game in CSC1310 Computer Programming I class and CSC3332 Fundamentals of Internet Systems class in our department. These two groups consisted of students whose classification ranged from freshman to junior.

We started the impact study with the pre-test and post-test comparison. To accomplish this, we had both groups answer five questions about phishing. Then, students played the game from start to finish. After the gameplay, students took a post-test that was 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 20% to 80% increases, with an average increase of 37.5% for these individuals. The other 3 students' scores were still somewhat reassuring because they remained unchanged, with one student scoring 80% both times and the other two scoring a perfect 100% both times. The Fig. 8 shows CSC1310 pre-test and post-test score comparison.

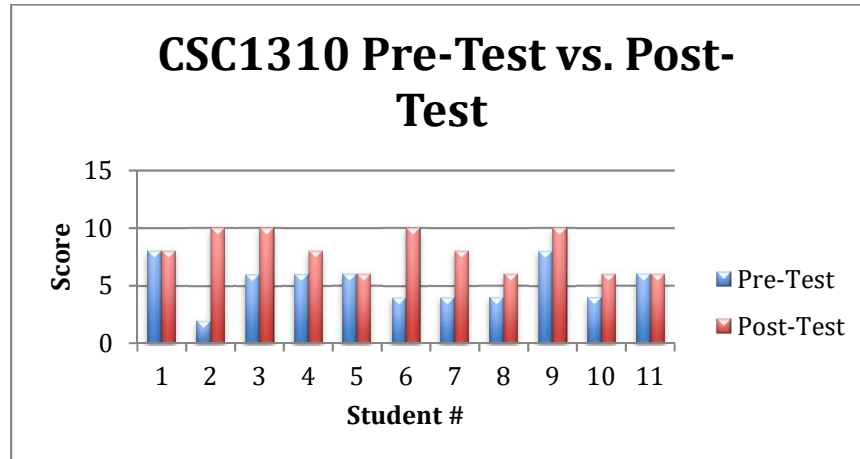


Figure 8. CSC1310 Pre-Test vs. Post-Test

In addition to the pre-test and post-test comparison, we examined the log files in detail. The Fig. 9 shows the summary of evaluation data obtained from the log files. We can see that there were many players who required more than three play troughs to receive a passing score. Of these players, 4 out of 5 required 3-5 attempts. There was one outlier that required 9 attempts in order to receive a passing score. However, the majority still required 2 or less attempts, showing positive reinforcement for the game's use as a teaching tool. Also, the 10% difference between players with a score of 80% and those with a score of 100% is much closer to a 50/50 split shown in Fig. 10, considering the sample size was small with an actual ratio of 5:6.



| CSC1310 | | | | | |
|-----------|-----------------------|---------------|-------------------------------------|--|--------------------|
| Student # | Number of Time Played | Passing Score | Attempt Scores | | |
| 1 | 1 | 0.80 | 0.80 | Average Score of Students: | 0.91 |
| 2 | 3 | 0.80 | .20, .60, .80 | Mean of Students' Score: | 1.00 |
| 3 | 2 | 0.80 | .60, .80 | Standard Deviation of Students' Score: | 0.10 |
| 4 | 2 | 0.80 | .60, .80 | | |
| 5 | 2 | 1.00 | .60, 1 | | |
| | | | | Passing of Attempts | Number of Students |
| 6 | 5 | 1.00 | .20, 0.00, 0.00, .60, 1.00 | 1 | 3 |
| 7 | 4 | 1.00 | 0.00, .40, .60, .80 | 2 | 4 |
| 8 | 1 | 1.00 | 1.00 | 3+ | 5 |
| 9 | 1 | 1.00 | 1.00 | | |
| | | | .20, .20, .20, .20, .40, .40, 0.00, | | |
| 10 | 9 | 0.80 | .60, .80 | | |
| 11 | 5 | 1.00 | 0.00, .40, .40, .20, 1.00 | Player with .80 score | 5 |
| | | | | Player with 1.00 score | 6 |

Figure 9. CSC1310 Data Summary from log files



Figure 10. CSC1310 Score Pie Chart

Next, for the CSC3332 group we collected the same information. In this group, 12 out of 19 students showed improvement in their scores. The improvements ranged from 20% to 80% increases, with an average increase of 20% for these individuals. 5 out of 19 students scores remained unchanged, with one scoring 80% both times and four scoring a perfect 100% both times. Unfortunately, 3 students' scores decreased by 20% during some attempts. 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 performance for this group is shown in the following figure.

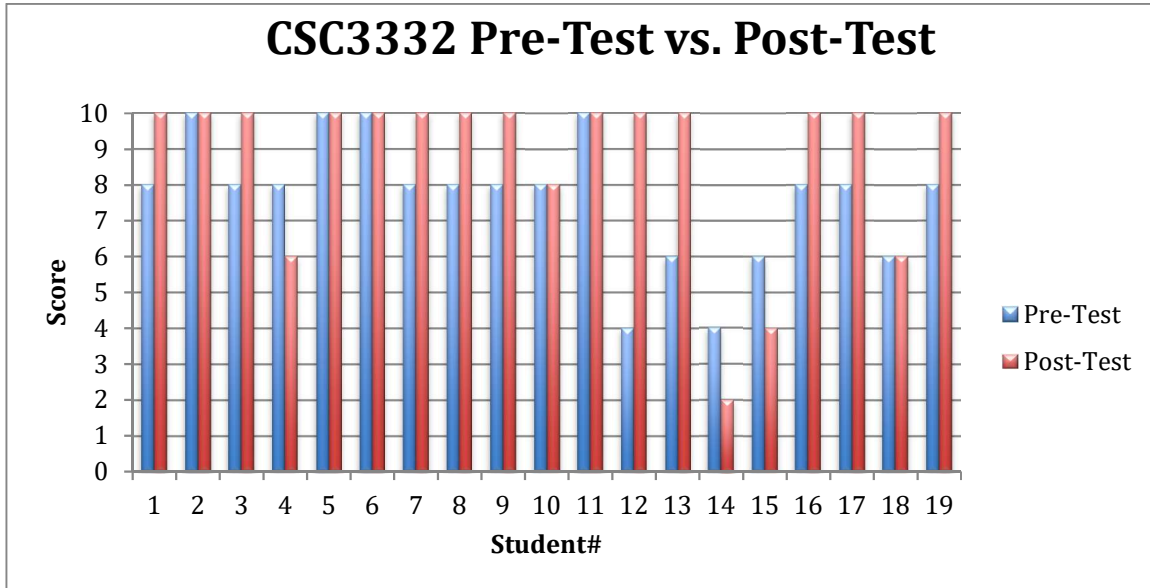


Figure 11. CSC3332 Pre-Test vs. Post-Test

Additionally, as shown by the following statistics in Fig. 12, no player required more than three playthroughs before they received a passing score. This reveals that there is a quick effectiveness and learning curve for individuals that play the game with little to no previous experience with its concepts. Furthermore, 15 of the 19 players only required 2 playthroughs to receive a passing score. Additionally, the 6% difference of players with 80% scores and 100% scores is much closer to a 50/50 split shown in Fig. 13, considering it was ten players to nine.



| CSC 3332 | | | | | |
|-----------|-----------------------|---------------|----------------|--|--------------------|
| Student # | Number of Time Played | Passing Score | Attempt Scores | | |
| 1 | 2 | 0.80 | 0.00, .80 | | |
| 2 | 1 | 1.00 | 1.00 | | |
| 3 | 1 | 1.00 | 1.00 | | |
| 4 | 1 | 0.80 | 0.80 | | |
| 5 | 2 | 0.80 | .20, .80 | Average Score of Students: | 0.89 |
| 6 | 3 | 0.80 | 0.00, .40, .80 | Mean of Students' Score: | 0.80 |
| 7 | 2 | 0.80 | 0.00, .80 | Standard Deviation of Students' Score: | 0.10 |
| 8 | 2 | 0.80 | 0.00, .80 | | |
| 9 | 1 | 0.80 | 0.80 | | |
| 10 | 1 | 1.00 | 1.00 | | |
| 11 | 3 | 1.00 | .20, .20, 1.00 | | |
| 12 | 3 | 0.80 | .20, 0.00, .80 | | |
| 13 | 2 | 1.00 | .40, 1.00 | | |
| | | | | Pass Attempts | Number of Students |
| 14 | 3 | 1.00 | .20, .40, 1.00 | | |
| 15 | 2 | 1.00 | .40, 1.00 | 1 | 6 |
| 16 | 1 | 1.00 | 1.00 | 2 | 9 |
| 17 | 2 | 0.80 | .20, .80 | 3+ | 4 |
| 18 | 2 | 0.80 | .60, .80 | | |
| 19 | 2 | 1.00 | .60, 1.00 | Player with .80 score | 10 |
| | | | | Player with 1.00 score | 9 |

Figure 12. CSC3332 Data Summary from log files



Figure 13. CSC3332 Score Pie Chart

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 currently decided did not fit the scheme we desired for our game as of now. 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 1. 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% |

VI) Future Work

In summary, we introduced a 2D game “Birds’ Life” that aims to help students learn about phishing. We did the initial evaluation in two classes. The results are promising. We will refine the game based on student feedback and further improve our assessment method to more accurately show the impact of game. We plan to use the updated mobile version in several computer introductory courses in fall 2017. We will post the game online to benefit more students in other institutions or anyone who wants to gain basic knowledge on how to protect against phishing. This game could become an enjoyable form of education. Additionally, our current and future research option, currently in the literary review phase, is DDoS attacks and defense. 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 DDoS 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. Additionally, this simulation is being explored in the realm of VR as to make use of modern technology for a more immersive experience.

VII) 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>



VIII) Presentations and Publications

- Our paper has been accepted as lighting talk and we will present it at SIGITE 2017 in October.

IX) References

- [1] Anthony Y. Fu, Wan Zhang, Xiaotie Deng, and Liu Wenyin. 2006. Safeguard against *unicode attacks*: generation and applications of UC-simlist. In *Proceedings of the 15th international conference on World Wide Web (WWW '06)*. ACM, New York, NY, USA, 917-918. DOI=<http://dx.doi.org/courseinfo.wssu.edu:2048/10.1145/1135777.1135943>
- [2] 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)*
- [3] 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.
- [4] 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*
- [5] 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*.
- [6] Dipti Patel and Xin Luo. 2007. Take a close look at phishing. In *Proceedings of the 4th annual conference on Information security curriculum development (InfoSecCD '07)*. ACM, New York, NY, USA, Article 32, 4 pages. DOI: <https://doi-org.courseinfo.wssu.edu/10.1145/1409908.1409943>
- [7] Greg Aaron, Katharine A. Bostik, Rod Rasmussen, and Edmon Chung. 2008. Protecting the web: phishing, malware, and other security threats. In *Proceedings of the 17th international conference on World Wide Web (WWW '08)*. ACM, New York, NY, USA, 1253-1254. DOI: <https://doi-org.courseinfo.wssu.edu/10.1145/1367497.1367753>
- [8] 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.
- [9] 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).
- [10] Jordan, C., Knapp, M., Mitchell, D., Claypool, M. and Fislser, K. "CounterMeasures: A Game for Teaching Computer Security." *2011 10th Annual Workshop on Network and Systems Support for Games*.
- [11] Letchford, Joshua., Vorobeychik, Yevgeniy. (2013, May). *Optimal Interdiction of Attack Plans*.
<http://dl.acm.org/citation.cfm?id=2484955&CFID=665904379&CFTOKEN=22510146>
- [12] Julie S. Downs, Mandy Holbrook, and Lorrie Faith Cranor. 2007. Behavioral response to phishing risk. In *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit*(eCrime '07). ACM, New York, NY, USA, 37-44.
DOI=<http://dx.doi.org/courseinfo.wssu.edu:2048/10.1145/1299015.1299019>
- [13] 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*.



- [14] 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)*.
- [15] 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)*.
- [16] Rachna Dhamija, J. D. Tygar, and Marti Hearst. 2006. Why phishing works. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '06)*, Rebecca Grinter, Thomas Rodden, Paul Aoki, Ed Cutrell, Robin Jeffries, and Gary Olson (Eds.). ACM, New York, NY, USA, 581-590.
DOI=<http://dx.doi.org/courseinfo.wssu.edu:2048/10.1145/1124772.1124861>
- [17] Zikai Alex Wen, Yiming Li, Reid Wade, Jeffrey Huang, and Amy Wang. 2017. What.Hack: Learn Phishing Email Defence the Fun Way. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems (CHI EA '17)*. ACM, New York, NY, USA, 234-237. DOI: <https://doi-org.courseinfo.wssu.edu/10.1145/3027063.3048412>