Journal of Cybersecurity Education, Research and Practice

Volume 2018 | Number 2 Article 2

December 2018

# Using a Game to Improve Phishing Awareness

Patrickson Weanquoi
*Winston-Salem State University*, pweanquoi115@rams.wssu.edu

Jaris Johnson
*Winston-Salem State University*, jjohnson514@rams.wssu.edu

Jinghua Zhang
*Winston-Salem State University*, zhangji@wssu.edu

Follow this and additional works at: https://digitalcommons.kennesaw.edu/jcerp

Part of the Information Security Commons, and the Technology and Innovation Commons

## Recommended Citation

Weanquoi, Patrickson; Johnson, Jaris; and Zhang, Jinghua (2018) "Using a Game to Improve Phishing Awareness," *Journal of Cybersecurity Education, Research and Practice*: Vol. 2018 : No. 2 , Article 2.
Available at: https://digitalcommons.kennesaw.edu/jcerp/vol2018/iss2/2

This Article is brought to you for free and open access by DigitalCommons@Kennesaw State University. It has been accepted for inclusion in Journal of Cybersecurity Education, Research and Practice by an authorized editor of DigitalCommons@Kennesaw State University. For more information, please contact digitalcommons@kennesaw.edu.

# Using a Game to Improve Phishing Awareness

**Abstract**

*Cybersecurity education has become increasingly critical as we spend more of our everyday lives online. Research shows that college students are mostly unaware of the many online dangers. To teach students about cybersecurity using their preferred medium, gaming, we developed an educational 2D game called "Bird's Life" that aims to teach 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 cybersecurity, a pre-test, post-test, and online survey were developed and used in the evaluation process. In Spring 2017, the Windows version of the game was used in two courses in our department (CSC1310 Computer Programming I and CSC3332 Fundamentals of Internet Systems). In Spring 2018, it was used in five sections of one general education course (CSC1306 Computer and Its Use I).*

**Keywords**

Cybersecurity, Phishing, Game-Based Learning

**Cover Page Footnote**

This project was supported by Collaborative Research Experiences for Undergraduates (CREU) via iAAMCS AYUR program. Game Assets: Worms are from https://opengameart.org/content/skyll-floating-skull-worm# 2D Games Asset Pack is from https://www.assetstore.unity3d.com/en/#!/content/24039 Birds Pack is from https://www.assetstore.unity3d.com/en/#!/content/27774 Particle Ribbon is from https://www.assetstore.unity3d.com/en/#!/content/42866

This article is available in Journal of Cybersecurity Education, Research and Practice: https://digitalcommons.kennesaw.edu/jcerp/vol2018/iss2/2

# INTRODUCTION

Securing ourselves online has been very important for many years. The frequency of virtual attacks on an individual through the use of a computer has grown both directly and indirectly. Students need to be prepared for the network security challenges they encounter so that the workforce of the future has the additional cybersecurity skills to best protect the interests of the nation.

Games have been successfully used in many areas of education, including computer science, to engage students in learning. Research shows multiple benefits of cybersecurity games (Pusey, Tobey and Soule, 2014; Tobey, Pusey and Burley 2014). They can inspire students to explore more in the security field and help students test their knowledge in authentic settings. The cybersecurity educational community needs these tools to keep students motivated and engaged in learning security concepts.

Many games have been used to teach cyber security concepts (Catuogno & Alfredo, 2008; Chapman, Tyson, Mcburney, Luck, and Parsons, 2014; Compte, Elizondo, and Watson, 2015; Guimaraes, Said, and Austin, 2011; Herr & Dennis, 2015; Irvine, Thompson, and Allen, 2005; Jordan, Knapp, Mitchell, Claypool, and Fisler, 2011; Kumaraguru, Sheng, Acquisti, Cranor, and Hong, 2010; Patel & Luo, 2007; Sheng, Magnien, Kumaraguru, Acquisti, Cranor, Hong, and Nunge, 2007; Shostack & Denning, 2013; Williams, Meneely, and Shipley, 2010). "Control-Alt-Hack" is a tabletop card game that was designed to raise people's awareness of computer security (Shostack & Denning, 2013). "Protection Poker" is a software security game that lets software development teams to assess the risks and deploy fortifications to prevent most damaging attacks (Williams et al., 2010). CyberCIEGE provides a virtual world interface that simulates the role of a network manager in protecting the network with a limited budget (Irvine et al., 2005). "Anti-Phishing Phil" is an online game developed to teach how to not fall for phishing attacks (Sheng et al., 2007). The What.Hack game challenges players to identify real-life phishing emails in an active and entertaining way (Wen, Li, Wade, Huang, and Wang, 2017). The authors (Klopfer, Osterweil, and Salen, 2009) did a comprehensive study on educational games and argued that games could engage students in learning without disrupting the dichotomy of school or play. In addition, they presented 13 principles of designing learning games, which can serve as a useful guide for educational game developers.

We found that college students prefer computer games to tabletop games. Some tabletop games have too many rules to memorize which makes it difficult to engage students effectively. Some high-quality cybersecurity games require the players to have substantial knowledge of the field to enjoy. Therefore, they have almost no value for students (Werther, Zhivich, Leek, and Zeldovich, 2011). On the other hand, some educational computer games are targeted to high school students. However, very few games were developed to enhance security education for college students. Furthermore, many creators of the educational games have focused primarily on the research and development process. They have not put sufficient emphasis on the evaluation and assessment of the games.

According to Patel and Luo (Patel & Luo 2007), about 86% of most attacks targeted home computers because their users are unaware of the dangers of phishing. To help students understand the concepts of phishing and scientifically assess it on student learning, we developed a 2D game called *Bird's Life*. The objective of the game is to provide students with a fun environment to learn about phishing. Two undergraduate students developed the game using the Unity3D game engine in about six months. The game was not designed only for gamers. Students without prior gaming experience can complete the game within 20 minutes. There are three main levels in the game:

- Level One: Introduce the game story
- Level Two: Collect phishing prevention tips
- Level Three: Identify phishing emails

According to Nagarajan et al. (Nagarajan, Allbeck, Sood, and Janssen, 2012), measuring the students' skills before and after gameplay is very important to determine the game's effectiveness; however, few security games have implemented this. To evaluate the potential impact of the game on student learning, we implemented in-game assessments (pre-test and post-test) in *Bird's Life*. To collect the feedback from the students, we created an online survey. In addition, we used a different log file for each player to record his/her behavior during gameplay. This portable and self-contained game makes it easy to share with other faculty engaged in STEM teaching and research. The Windows version of the game was used in two courses (CSC1310 and CSC3332) in Spring 2017 and five sections of the CSC1306 course in Spring 2018. The classroom evaluation shows promising results.

The following section describes the design and implementation details of the game. The classroom evaluation section shares our experience using it in the classroom. The last section presents the conclusion and future work.

## GAME DESIGN AND DEVELOPMENT

*Bird's Life* is a decision-making game. The player controls the main character using arrow keys or motion controls on PCs and mobile devices respectively. The player needs to understand the directions of each level in order to accomplish the tasks. The game starts with “How to Play”. The “Start” and “How to Play” screens are shown in Fig. 1 and Fig. 2.

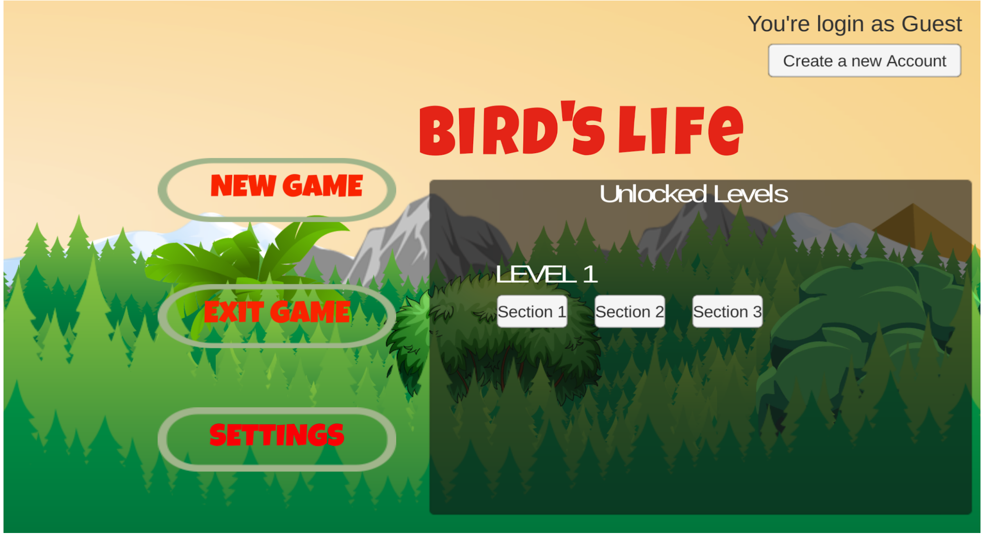
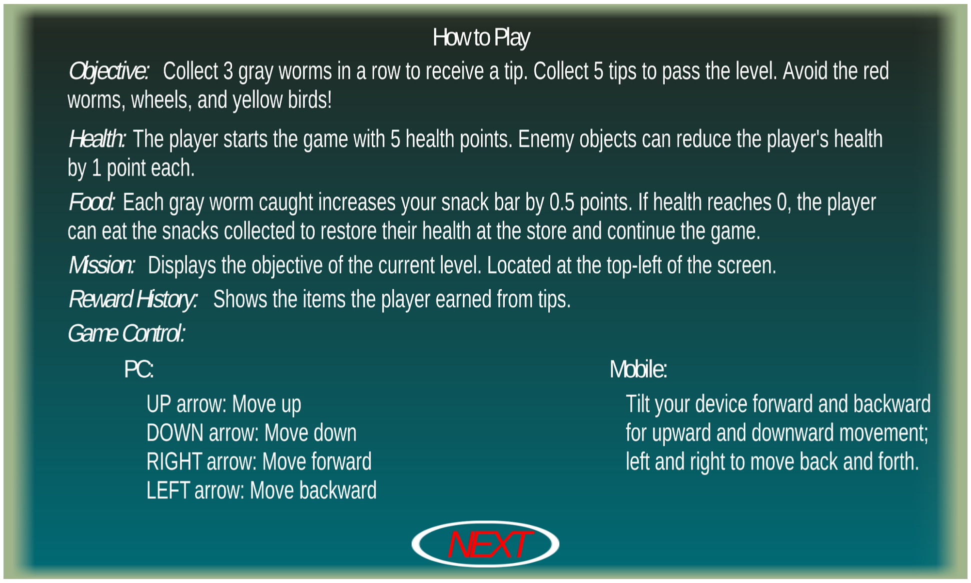


*Figure 1. Start Screen*



How to Play

*Objective:* Collect 3 gray worms in a row to receive a tip. Collect 5 tips to pass the level. Avoid the red worms, wheels, and yellow birds!

*Health:* The player starts the game with 5 health points. Enemy objects can reduce the player's health by 1 point each.

*Food:* Each gray worm caught increases your snack bar by 0.5 points. If health reaches 0, the player can eat the snacks collected to restore their health at the store and continue the game.

*Mission:* Displays the objective of the current level. Located at the top-left of the screen.

*Reward History:* Shows the items the player earned from tips.

*Game Control:*

PC:

UP arrow: Move up
DOWN arrow: Move down
RIGHT arrow: Move forward
LEFT arrow: Move backward

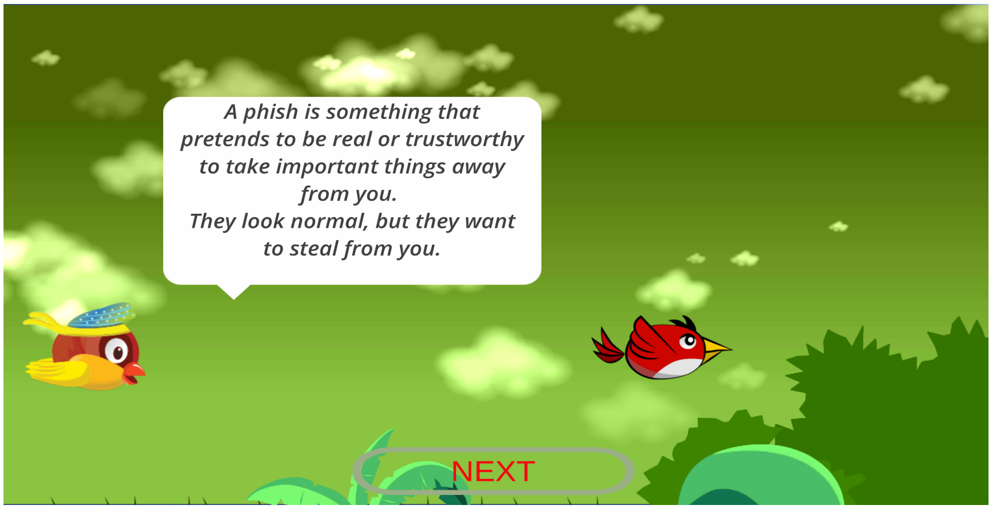
Mobile:

Tilt your device forward and backward for upward and downward movement; left and right to move back and forth.

*Figure 2. How to Play*

## Level One

We have come to understand the importance of getting players interested in the game. This level gives us the opportunity to intrigue the player and encourage them to delve into the game. The purpose of this level is to create a dialogue between two birds. Their conversation foreshadows the general ideas the player will learn throughout the game. This level places the player in an environment where he/she has to take on the characteristics of a bird. After the dialogue the player has to distinguish between good and bad worms since identifying phishing in emails is the core of prevention. A screenshot of this level is shown in the Fig.3.

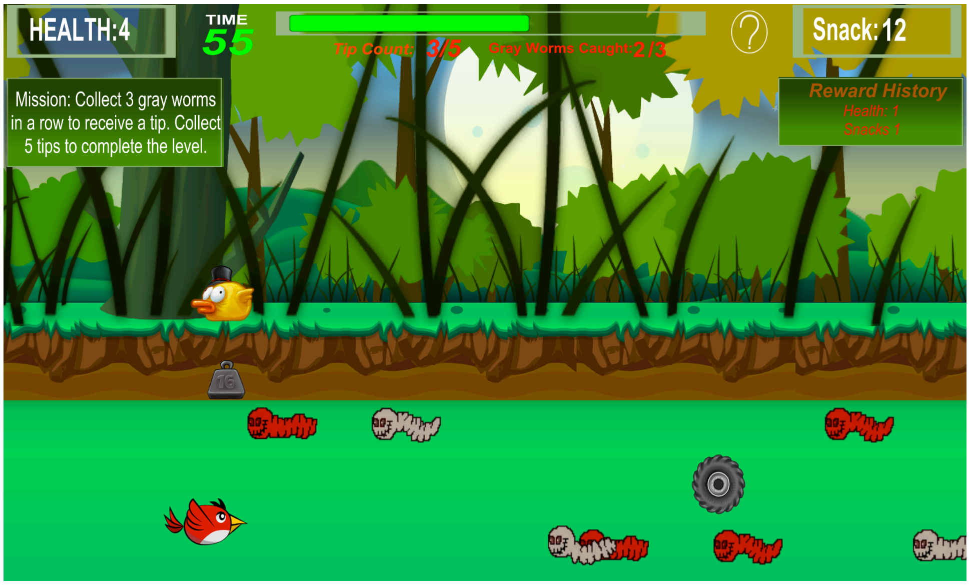


*A phish is something that pretends to be real or trustworthy to take important things away from you. They look normal, but they want to steal from you.*

*Figure 3. Gameplay Level #1*

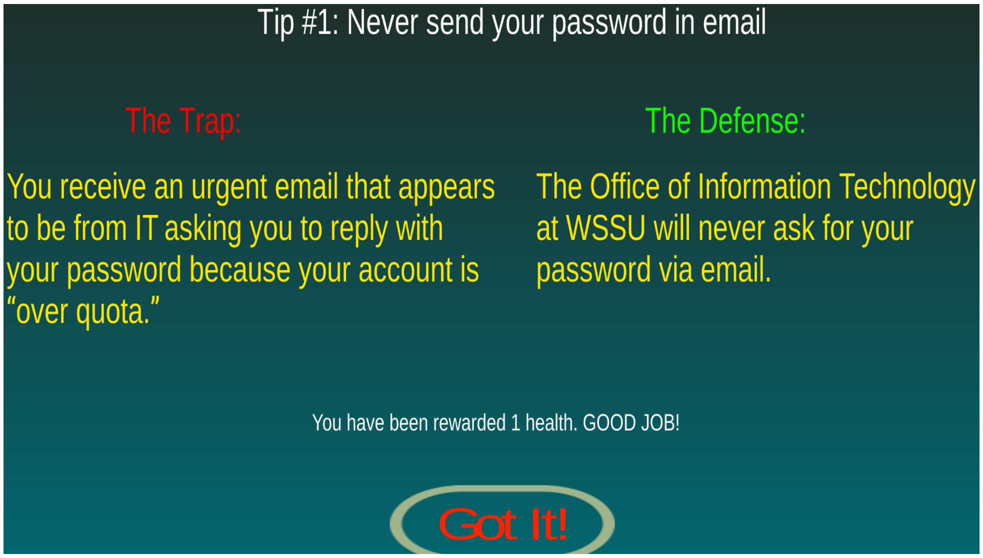
## Level Two

The game operates from a defensive aspect. The player starts with five lives and has to avoid the "red worms" which signify phishing emails and scams. As the game progresses, more obstacles appear along the way, increasing the game's difficulty. Such challenges include spiked wheels, yellowbirds, and timers. 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" consecutively to obtain a tip. The player can use the rewards to purchase more health. At the end of this level, the player is expected to know what to do when he/she encounters a phishing attack and will enter the next level to use his/her knowledge to identify phishing attacks. Screenshots for this level can be found in the Fig. 4 and Fig. 5.



Mission: Collect 3 gray worms in a row to receive a tip. Collect 5 tips to complete the level.

*Figure 4. Gameplay Level #2*



Tip #1: Never send your password in email

The Trap:

You receive an urgent email that appears to be from IT asking you to reply with your password because your account is "over quota."

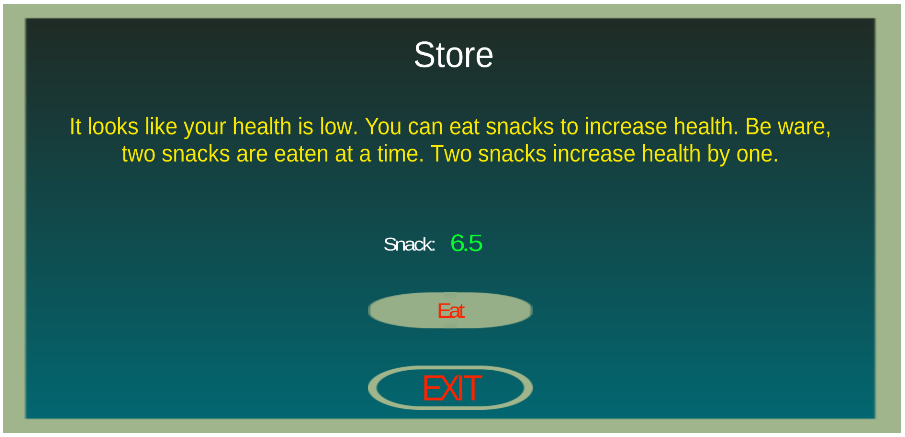
The Defense:

The Office of Information Technology at WSSU will never ask for your password via email.

You have been rewarded 1 health. GOOD JOB!

*Figure 5. Collecting Tips*

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. The time signifies the player's response time when encountering phishing attacks and how quickly the player handles the threat. We also included features such as a store, shown in the Fig. 6, where the player can replenish his/her health or time if needed.



Store

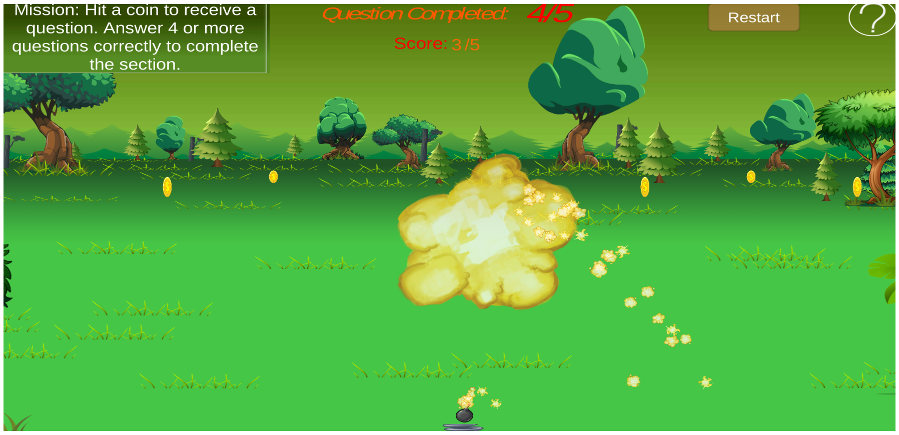
It looks like your health is low. You can eat snacks to increase health. Be ware, two snacks are eaten at a time. Two snacks increase health by one.

Snack: 6.5

*Figure 6. Game Store*

## Level Three

This level is designed to let the player utilize knowledge gained in the previous levels. Scenarios are randomly selected from a pool. The player needs to answer 80 percent (4 out 5 questions) correct to pass this level. Immediate feedback will be provided to reinforce the concepts. A gameplay screenshot for this level is shown in Fig. 7 and the phishing scenario is shown in Fig. 8.

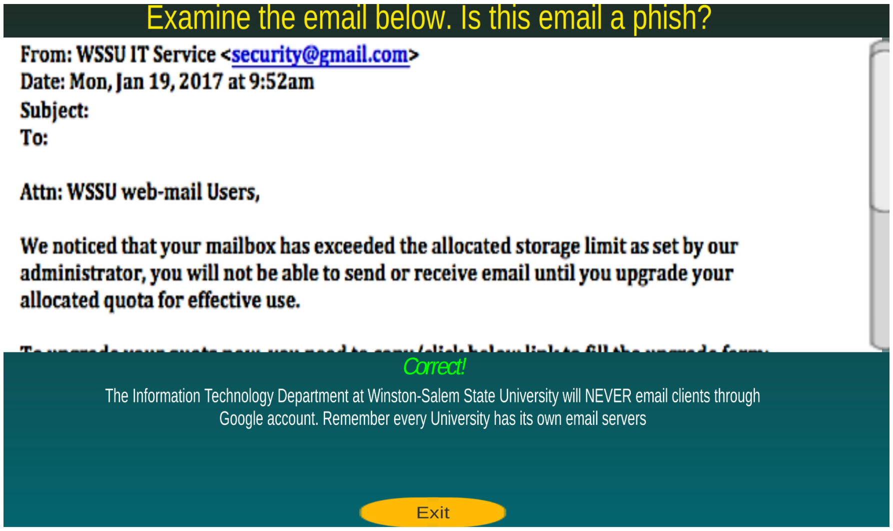


Mission: Hit a coin to receive a question. Answer 4 or more questions correctly to complete the section.

Question Completed: 4/5

Score: 3/5

*Figure 7. Gameplay Level #3*



Examine the email below. Is this email a phish?

From: WSSU IT Service <security@gmail.com>
Date: Mon, Jan 19, 2017 at 9:52am
Subject:
To:

Attn: WSSU web-mail Users,

We noticed that your mailbox has exceeded the allocated storage limit as set by our administrator, you will not be able to send or receive email until you upgrade your allocated quota for effective use.

Correct!

The Information Technology Department at Winston-Salem State University will NEVER email clients through Google account. Remember every University has its own email servers

*Figure 8. Identify Phishing Attack*

# CLASSROOM EVALUATIONS

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 students basic cybersecurity concepts. The measure of our work's success was centered on how well individuals unfamiliar with cybersecurity 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 for further analysis. We evaluated the game in both CS/IT major courses and non-CS/IT courses to see the impact in different classes.

## Evaluation in CS/IT major courses

In our evaluation process, the Windows version of the game was used in CSC1310 Computer Programming I and CSC3332 Fundamentals of Internet Systems in Spring 2017. 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, each worth two points, about phishing. Then, students played the game from start to finish. After gameplay, students took a post-test that was identical to the pre-test. We compared the 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 three students' scores were still somewhat reassuring because they remained unchanged, with one student scoring eight points both times and the other two scoring a perfect 10 both times. The Fig. 9 (a) shows the CSC1310 pre-test and post-test score comparison. The summary of the test evaluation for this group is shown in Table I. The average of the pre-test is 5.3 points and the average of the post-test is eight points. The p-value of two-tailed paired t-test is 0.0056, showing statistically significant improvement from pre-test to post-test.

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 eight points both times and four scoring a perfect 10 both times. Unfortunately, three students' scores decreased by 20% during some attempts. The pre-test and post-test performance comparison for this group is shown in the Fig. 9 (b). The summary of the test evaluation for this group is also shown in Table I. The average of the pre-test is 7.7 and the average of the post-test is 8.7. The p-value of two-tailed paired t-test is 0.037, showing statistically significant improvement from pre-test to post-test.

According to the pre-test and post-test comparison shown in Table I, the post-test average for the CSC1310 group improved 51% after gameplay. However, CSC3332 group's average improved only 13%. We found the results are aligned with our predictions. The CSC1310 group mainly consists of freshman who may not have too much knowledge about phishing before playing the game so the average for this group improved significantly after gameplay. The CSC3332 class, however, is a junior level computer science course so they already had some security knowledge before the gameplay. The pre-test average is pretty high, and we are happy to see a 13% improvement for this group.

*Table I. Summary of Pre-Test and Post-Test Evaluations in CSC1310 & CSC3332*

| **CSC1310** | | **CSC3332** | |
|---|---|---|---|
| Average of Pre-Test | 5.3 | Average of Pre-Test | 7.7 |
| Average of Post-Test | 8 | Average of Post-Test | 8.7 |
| Improvement | 51% | Improvement | 13% |
| Two-tailed p-values of t test | 0.0056 | Two-tailed p-values of t test | 0.037 |

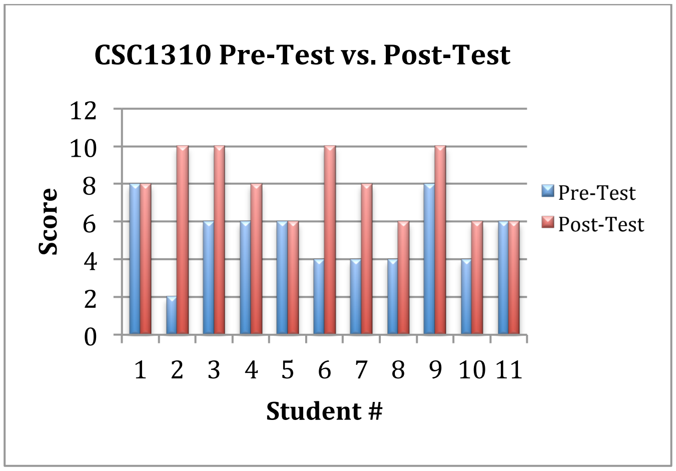


*Figure 9. (a) CSC1310 Pre-Test vs. Post-Test Comparison*

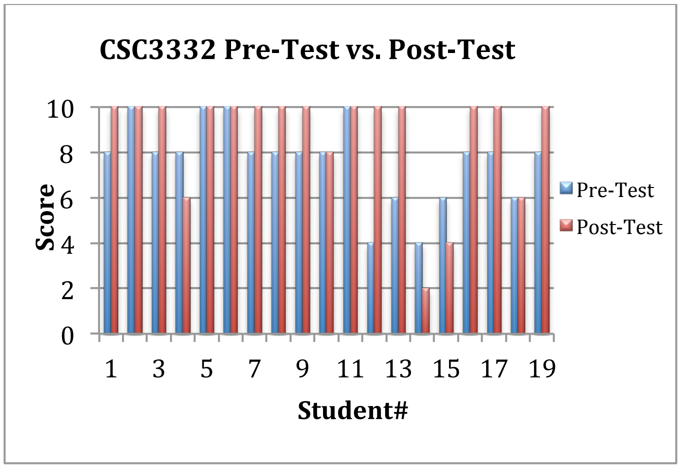


*Figure 9. (b) CSC3332 Pre-Test vs. Post-Test Comparison*

In addition to the pre-test and post-test comparison, we examined the log files in detail. Each log file contains the number of attempts the student needed in order to pass Level 3. For CSC1310, we can see that there were many players who required more than three playthroughs to receive a passing score. 80% of these players, required three to five attempts with one outlier that required nine attempts. However, the majority still required one or two attempts, showing positive reinforcement for the game's use as a teaching tool. Table II shows the log file summary for both classes. For CSC3332, no player required more than three playthroughs before they received a passing score. This reveals that there is an easy learning curve for individuals that play the game with little to no previous experience with its concepts. Furthermore, 15 of the 19 players (79%) only required at most two playthroughs to receive a passing score.

*Table II. CSC1310 & CSC3332 Log File summary*

| CSC1310 | | CSC3332 | |
|---|---|---|---|
| **Level 3 Passing Attempts** | **Percentage of Students** | **Level 3 Passing Attempts** | **Percentage of Students** |
| 1 | 25% | 1 | 32% |
| 2 | 33% | 2 | 47% |
| 3+ | 42% | 3 | 21% |

## Evaluation in Non-CS/IT major courses

To evaluate the impact of the game on students without computing background, we used the game in five sections of the CSC1306 course (The Computer and Its Use I) in Spring 2018. It is a general education course that non-CS/IT majors take to meet the information literacy requirement. This course introduces the use of digital computers, applications software, I/O devices, storage devices, systems software, software evaluation, and computer ethics.

We started the impact study with the pre-test and post-test comparison. The students need to complete the pre-test to unlock the game. After the main gameplay, students took a post-test that was identical to the pre-test. Each test has five questions, each worth two points. We then compared both scores to see if there were any improvements in overall performance. Out of 70 participants, 38 were females and 32 were males. The pre-test and post-test performance for this group is shown in Fig. 10. As shown in the pre-test and post-test comparison summary in Table III, 67% of students showed improvement in their scores, which is even better than the 51% improvement from the initial trials in CSC1310. Students had an average score of six on the pre-test. This number increased to 8.4 for the post-test. Lastly, the p-value of two-tailed paired t-test is 3.328E-9, showing statistically significant improvement from pre-test to post-test.

*Table III. Summary of Pre-Test and Post-Test Evaluations in CSC1306*

| CSC1306 | |
|---|---|
| Average of Pre-Test | 6 |
| Average of Post-Test | 8.4 |
| Improvement | 67% |
| Two-tailed p-values of t test | 3.328E-9 |

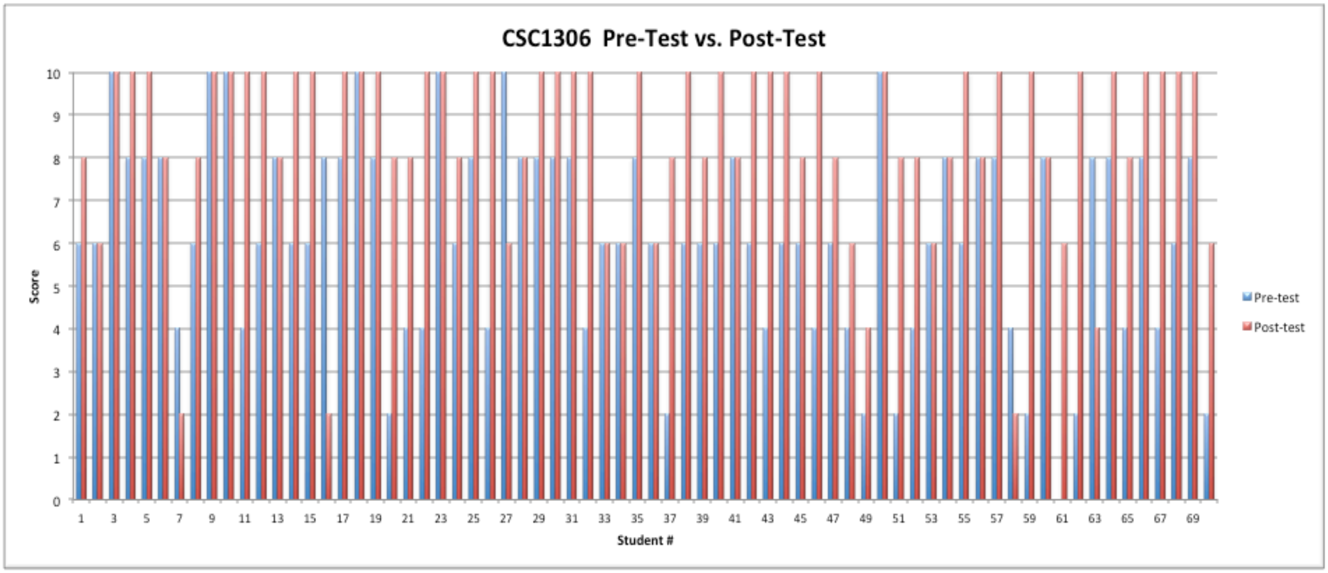


*Figure 10. CSC1310 Pre-Test vs. Post-Test Comparison*

In addition to the pre-test and post-test comparison, we examined the log files in detail. Each log file contains the number of attempts the student needed in order to pass Level 3. Over every group, players took a minimum of one playthrough and a maximum of five playthroughs to receive a passing score. 41.43% of the students passed Level 3 on their first attempt, 32.86% completed the level on their second attempt, and 25.71% needed three or more attempts. However, the majority (90%) only required one to three attempts, showing positive reinforcement for the game's use as a teaching tool. Table IV shows the log file summary for the CSC1306 group.

*Table IV. CSC1306 Log File summary*

| **CSC1306** | |
|---|---|
| **Level 3 Passing Attempts** | **Percentage of Students** |
| 1 | 41.43% |
| 2 | 32.86% |
| 3+ | 25.71% |

According to these evaluation results, the tips provided in the game had a positive effect on players' understanding about phishing. Most students were able to complete the activities (pre-test, game, post-test, and survey) in about 20 minutes. The pre-test and post-test comparison of 100 participants showed the game had a positive impact on students' learning about phishing attacks.

## Survey

We gave all the groups the opportunity to anonymously give comments and feedback on the game as an overall experience. This was extremely helpful in directing us towards delivering a higher quality gameplay experience. One of the most consistent comments we received during the game evaluation was to make the “How to Play” instructions clearer. More specifically, the level three contains a bomb launch mechanic that many people found it difficult or confusing to use. To fix this, we rewrote the instructions on how to move the bomb forward to clarify that launching is a scrolling action. There was also a suggestion for a boss level that we are currently taking into consideration.

We refined the game based on the students’ feedback. Outside of those suggestions, most of the feedback simply congratulated us on a well-made game and stated that the tips were helpful in learning the methods of protection against phishing. 138 students took the survey and the results can be found in Table V.

*Table V. Survey Results*

| Survey Questions | Percentage Agree |
|---|---|
| The game was enjoyable to play. | 88% |
| The game was easy to play. | 82% |
| I had a better understanding of Phishing attacks after playing the game. | 87% |
| The game had a good balance between "play" and "learning" time. | 90% |
| I was motivated to try hard to obtain Phishing Tips. | 73% |
| I tried my best to answer quiz questions correctly in the game. | 95% |
| The game provided immediate feedback when a mistake was made. | 91% |
| I would like to learn more security concepts using games like this. | 77% |
| I would recommend this learning game to other students. | 89% |

# CONCLUSION AND FUTURE WORK

In summary, we introduced a 2D game, *Bird’s Life,* which aims to help students learn about phishing attacks. Over 100 students in three different courses participated in this study. 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 the game. We plan to use the updated mobile version in several computer introductory courses and will post the game online to help 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. Moving forward, we plan to continue exploring the realm of cybersecurity and providing innovative methods that can help people protect themselves online.

# REFERENCES

Catuogno, L., and Alfredo D. S. (2008) "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), Madrid, Spain, 2008.

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

Compte, A. L., Elizondo D., and Watson, T. (2015) "A Renewed Approach to Serious Games for Cyber Security", *Proceedings of* the *7th International Conference on Cyber Conflict: Architectures in Cyberspace:* 203-16, 2015.

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

Herr, C. and Dennis, A. (2015) "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, Newport Beach, CA, 2015.

Irvine, C., Thompson, M. and Allen, K. (2005) "CyberCIEGE: Gaming for Information Assurance", *IEEE Security & Privacy, vol. 3, no. 3, 2005, pp. 61–64*

Jordan, C., Knapp, M., Mitchell, D., Claypool, M. and Fisler. K. (2011) "CounterMeasures: A Game for *Teaching* Computer Security", *Proceedings of the 10th Annual Workshop on Network and Systems Support for Games*, Ottawa, ON, Canada, 2011.

Klopfer, E., Osterweil, S., & Salen, K. (2009) "Moving learning games forward: Obstacles, opportunities & openness". *Cambridge, MA: The Education Arcade.*

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

Nagarajan, A., Allbeck, J. M., Sood, A. and Janssen, T.L. (2012) "Exploring game design for cybersecurity *training*", *Proceedings of the IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER'12)*.

Patel, D. and Luo, X. (2007) "Take a close look at phishing", *Proceedings of the 4th annual conference on Information security curriculum development* (InfoSecCD '07), Kennesaw, GA, 2007.

Pusey, P., Tobey, D. and Soule, R. (2014) "An Argument for Game Balance Improving Student Engagement *by* Matching Difficulty Level with Learner Readiness", *Proceedings of the 2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14*). USENIX Association, San Diego, CA

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L.F., Hong, J. and Nunge, E. (2007) "Anti-*Phishing* Phil: The Design and Evaluation of a Game That Teaches People Not to Fall for Phish", *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, Pittsburgh, PA, 2007.

Shostack, L. & Denning, K. (2013) "Control-Alt-Hack: the design and evaluation of a card game for *computer* security awareness and education", *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security,* Berlin, Germany, 2013.

Tobey, D. H., Pusey, P. and Burley, D. L. (2014) "Engaging Learners in Cybersecurity Careers: Lessons *from* the Launch of the National Cyber League", *ACM Inroads 5, 1 (2014), 53–56.*

Wen, Z., Li, Y., Wade, R., Huang, J., and Wang, A. (2017) "What.Hack: Learn Phishing Email Defence *the* Fun Way", *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems* (CHI EA '17)

Werther, J., Zhivich, M., Leek, T. and Zeldovich, N. (2011) "Experiences in Cyber Security Education*:* The *MIT* Lincoln Laboratory Capture-the-flag Exercise", *Proceedings of the 4th Conference on Cyber Security Experimentation and Test (CSET'11). USENIX Association,* Berkeley, CA, USA, 12–12.

Williams, L., Meneely, A. and Shipley, G. (2010) "Protection Poker: The New Software Security 'Game'", *IEEE Security & Privacy, vol. 8, no. 3, 2010, pp. 14–20.*