## Pizza Heist: Cybersecurity Threat Awareness Game

## Abstract: "Pizza Heist: Cybersecurity Threat Awareness Game" educates students on cybersecurity threats through engaging mini-games that simulate real-world risks like malware and phishing. Developed in Unity as part of the Technology Ambassador Program (TAP), this 2D game promotes data protection by teaching players from both hacker and defender perspectives. Presented at campus events, including the Super Saturday Series and college workshops, the game effectively increased cybersecurity knowledge and sparked student interest in technology. Feedback showed improved understanding and enthusiasm for cybersecurity, supporting interactive media as a tool for digital literacy education.

## Introduction

## As the internet becomes more integrated into our everyday lives, understanding how to protect oneself is crucial in ensuring the safety and protection of our data in a digital landscape. This study aims to educate middle school, high school, and college students on what malicious entities exist and how to prevent these entities from breaching your data. This project was inspired by the rising number of individuals falling victim to cybersecurity threats like phishing, malware, and data breaches. We will empower users to protect themselves from these growing threats by raising awareness and providing essential information. This project was developed as part of the Technology Ambassador Program (TAP) service-learning course.

## Technology Ambassador Program (TAP)

## The Technology Ambassador Program (TAP) is a service-based learning course that provides students with a collaborative environment to develop projects using the technologies of their choice that are then presented in the community [1]. These projects are intended to increase participation in IT through outreach workshops designed to showcase the fun side of technology. Our team is taking the initiative to excite and educate students about cybersecurity with an engaging workshop that allows the participants to learn about cybersecurity with mini-games from two sides: hackers and defenders. Our goal is to show how powerful someone in cybersecurity can be when it comes to protecting important data.

## Methods

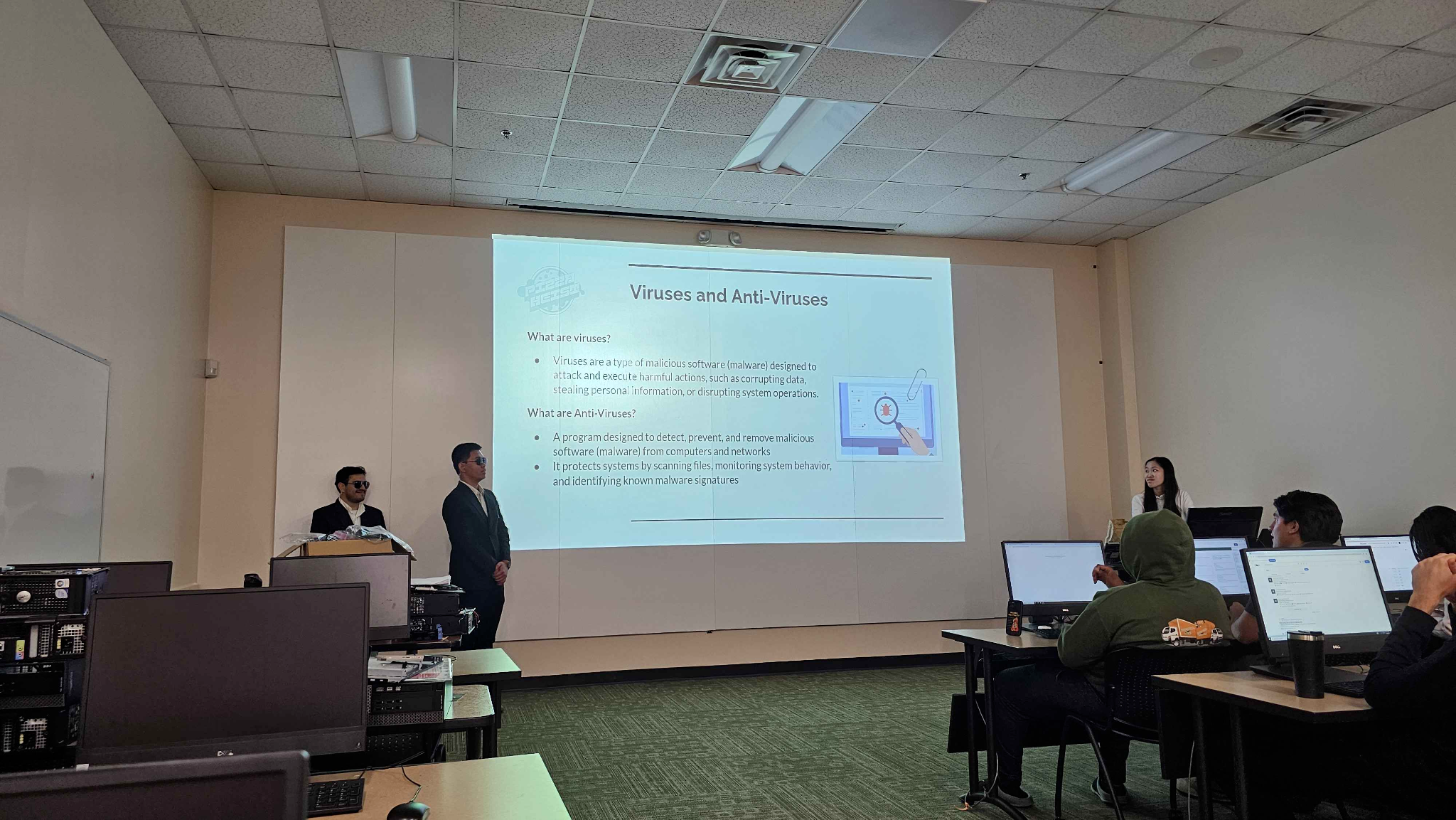
## Technology

Our project utilizes Unity [2] to create a cybersecurity-inspired 2D game designed to simplify the learning process for non-technical audiences. Unity's 2D framework enables the development of immersive mini games through its Canvas and Tile map systems, allowing players to navigate and interact with game environments. Each mini game simulates Windows applications to teach key cybersecurity concepts, leveraging Unity’s asset library and physics engine for dynamic and intuitive gameplay. The first mini game simulates sorting through emails, where students must determine whether or not an email is phishing. The second mini game incorporates viruses vs anti-viruses in a tower defense format to teach students about different viruses and ways to defend against them in real life.

**Figure 1.1:** Screenshots of the two mini-games made with Unity; left shows the malware mini-game, while the right is the phishing mini-game

**Events**

While we will present our game at various events on campus, we will focus our research efforts on the Super Saturday Series (S3) and classroom workshops. The S3 event is a volunteer event where GGC faculty and students offer in-person STEM workshops for middle school-aged students. College classroom workshops will take place in general education computing courses across campus. Both events will be hosted in computer lab classrooms so participants can access a computer and play our full game independently, which will be accessed through Unity’s website. We will start these workshops by presenting a brief slide presentation to introduce the cybersecurity topics featured in our game, such as viruses and phishing, and address the risks they pose to our privacy and safety. We will also present our project at several symposia events on campus. These events will only include demonstrations of our project where participants can play our game, without a teaching component.

**Figure 1.2:** Screenshot during one of the workshop

**Measuring Teaching Effectiveness**

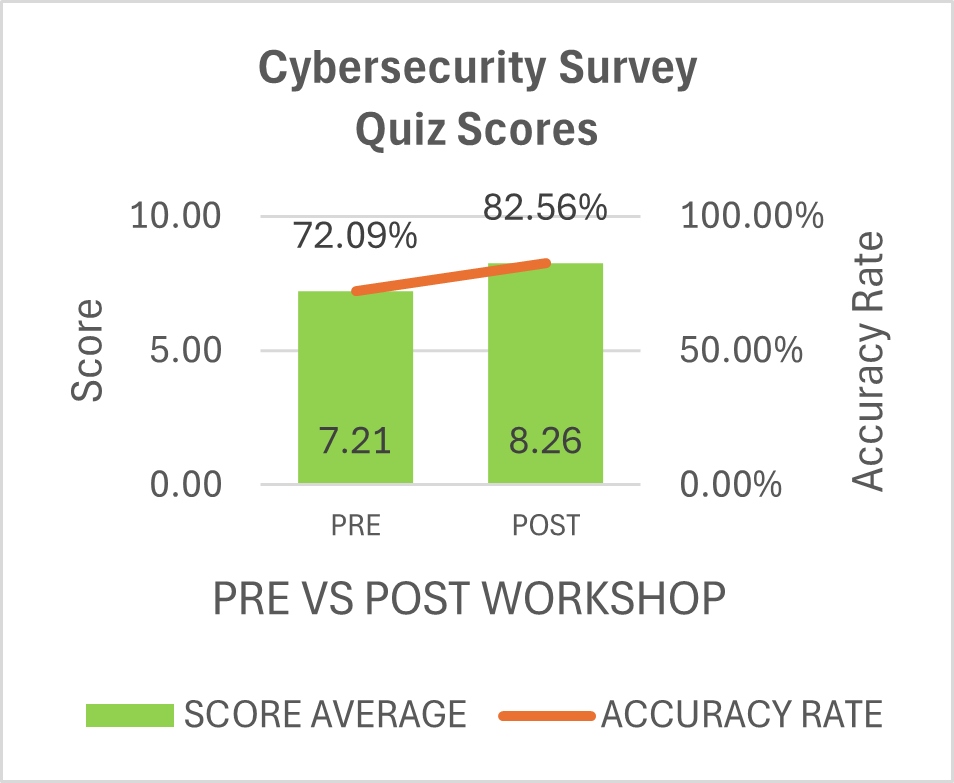
Before each workshop, participants will be asked to complete a short survey about their current cybersecurity knowledge and their expectations for the workshop. Another survey will be given at the end of the workshop, asking what participants have learned and their final thoughts. This allows us to compare the before and after results to more accurately determine the effectiveness and impact of our workshop, as well as receive more helpful feedback for future improvement. At shorter events, we will only give a single, brief survey to gather data, but not take too much time. We will ask for their thoughts after seeing our game. The results of our study will be presented in our poster.

## Results

## The workshop yielded substantial results. Participants learned the concepts taught, engaged well with the activity, and rated the event relatively positive. These findings are based on responses from 43 participants across three separate classroom workshops. The majority of our participants were Freshman students; two were in high school, and the most advanced were five juniors. The gender ratio was nearly even, with 22 male and 21 female students, representing a wide range of majors—only six students were in IT-related fields, leaving 86% from other fields.

**Figure 2.1:** Comparison of student interest in learning new technology before and after the workshop

Pre-workshop surveys assessed students' interests and prior experience in IT. Students were asked about their interest in learning new technology. 58.1% (25 of 43) were neutral, but 51.2% (22 of 43) would still enjoy using new technology. 55.8% (24 of 43) of students were undecided about taking more technology-related courses, and 69.8% (30 of 43) had no programming experience, with 9 having very little and 4 with intermediate experience. In a pre-workshop cybersecurity quiz, participants scored an average of 7.21 out of 10. The question with the lowest accuracy (44.19%) was, “What do you do when you receive a weird message from a friend through an unknown number?”

**Figure 2.2:** Comparison of students' quiz scores before vs after the workshop

Results from the post-workshop survey showed clear improvements. Participants' average cybersecurity quiz score increased to 8.26 out of 10, a 10.47% gain in accuracy. The lowest-performing question remained the same, yielding a 51.16% accuracy rate, a 6.98% improvement. Students were asked if they enjoyed learning and using the new technology respectively. In both instances, a majority of students reported yes to both, and none reported dissatisfaction. 100% of students were at least neutral or interested in new technology. 74.4% (32 of 43) enjoyed learning, and 76.7% (33 of 43) enjoyed using the new technology. 39.5% (17 of 43) of students expressed a new interest in programming, 34.9% (15 of 43) were neutral, and 25.6% (11 of 43) were disinterested. Additionally, 46.5% (20 of 43) of students expressed a new interest in game development, 20.9% (9 of 43) were neutral, and 32.6% (14 of 43) were uninterested. 27.9% (12 of 43) of students said yes to expressing an interest in taking TAP, STEC-4800, 37.2% (16 of 43) said maybe, and 34.9% (15 of 43) said no.

Pizza Heist received positive ratings. Students found the workshop fairly easy, rating the difficulty an average of 3.51 out of 10. Students reported the workshop as fun and engaging, rated 4.53 out of 5. The concepts taught were considered easy to understand, rated 4.86 out of 5. The team's performance was also rated highly, receiving a 4.84 out of 5 for how well they did in the workshop and an 8.09 out of 10 for their enthusiasm, leading to an overall average rating of 4.2 out of 5.  
  
**References**

1. Dekhane, S., Xu, X., Napier, N., Barakat, R., Gunay, C., & Nagel, K. (2018). Technology focused service-learning course to increase confidence and persistence in computing. *Journal of Computing Sciences in Colleges*, 34(2), 147-153. <https://dl.acm.org/doi/10.5555/3282588.3282609>
2. *Unity 2D tools for game dev – evolved for optimal graphics performance*. (n.d.). Unity. <https://unity.com/features/2dtools#why-unity-for-2d>

## Acknowledgments

This project has been partially funded by the National Science Foundation grant #2315804. We would also like to thank the GGC TAP faculty and students and the GGC School of Science and Technology.