OfficeGuard: The Anti-Phishing Training Game

Olivia BenAoumeur

The University at Albany community has made this article openly available. Please share how this access benefits you.

Follow this and additional works at: https://scholarsarchive.library.albany.edu/all_honors

Part of the Social and Behavioral Sciences Commons

This work is licensed under a Creative Commons Attribution-NonCommercial-Share Alike 4.0 International License. Rights Statement
OfficeGuard: The Anti-Phishing Training Game

An honors thesis presented to the
College of Emergency Preparedness, Homeland Security, and Cybersecurity,
University at Albany, State University of New York
in partial fulfillment of the requirements
for graduation with Honors in Information Sciences and Technology
and
graduation from The Honors College

Olivia BenAoumeur

Research Advisor: Kimberly A. Cornell, Ph.D.

May 2024
Abstract

Anti-phishing training is crucial for the business world. Therefore, much of the existing training is focused on employees. Education in the form of training tools and simulators helps increase the retention of information for these employees (Jampen et al., 2020). However, this education may be coming too late. Educating high school and college students on email etiquette and training during their formative years is essential to help protect students and their future employers. The gamification of training tools has the potential to “enrich the educational process and improve learning outcomes” (Lampropoulos & Sidiropoulos, 2024). The term ‘serious game’ describes a category of games that have a purpose beyond pure entertainment (Breuer & Bente, 2010). This includes the edutainment genre, which seeks to educate a player through engaging material. We propose that anti-phishing training should be given to students and geared towards them in an engaging way to prevent the formation of bad habits in the cyber world. By understanding the effects of game-based learning on students and the training materials in the workplace that have proved successful for retention, new software can be developed to bridge the gap between students and employees.
Acknowledgements

Starting this journey a year and a half ago with Dr. Kimberly Cornell was the beginning of some of the best moments that changed my life in the Information Science and Technology Department at the University at Albany. I would like to thank her for her guidance, mentorship, and expertise in the field. Working with her is a delight and has sparked my love for research. This thesis would not be possible without her support.

I would like to thank members of the College of Emergency Preparedness, Homeland Security, and Cybersecurity faculty and staff. The support I receive from this wonderful group of mentors is something that I cherish greatly. They are the reason I continue to be inspired to learn, research, and grow as an academic daily. Thank you to Dr. Abdullah Canbaz for his guidance and support as my Informatics Honors Director, and thank you to Professor Claire Thomas for the game development and serious games expertise in the early days of this project that helped to create the prototype of OfficeGuard.

I would also like to thank Dr. James Stellar for his career and academic advising these past four years. Having his guidance has helped me grow immensely as a scholar. It is safe to say I would not be in this major nor pursuing my academic passions if not for his mentorship and always believing in me. Thank you to Dr. Kathryn Fore and Matt Beebe for their academic guidance—To Kathryn, for letting me be emotional and honest in her office hours, the kind that sparks self-discovery. To Matt—for advocating for me as a student leader and his constant support as I pursued this honors journey.

Lastly, I would like to thank my friends and family for their endless support along this journey. My friends—Debby, Lily, Barbara, Chris, Grace, Michael, Alexis, Victoria, and Ben—they are my rocks, this college experience wouldn’t be right without them in it. To Alex—my sunshine, thank you for your unconditional love and support always, and listening to me read aloud every single academic paper I’ve ever written. To my sister, Chelsea, my soul twin, for getting me into a youtuber who plays Papers, Please, which helped eventually inspire pieces of OfficeGuard. And lastly, thank you to my parents. Thank you for being my number one cheerleaders, for helping me stand back on my feet every time I’ve ever slipped. The reason I get to even write an acknowledgement like this is because you inspired me to stay curious. I am forever grateful for it.
# Table of Contents

Abstract.................................................................................................................................ii

Acknowledgements...............................................................................................................iii

Introduction............................................................................................................................1

Literature Review..................................................................................................................4
  A. User personality and its psychological effect on phishing susceptibility.........................4
  B. Efficacy of previous training tools and serious games.....................................................7
  C. The effects of game-based learning in educational environments..................................10
  D. Components of a game design framework for phishing training....................................13
  E. Examining types of phishing emails for game design framework....................................14
  F. Novel Approach.............................................................................................................16

Methods Plan ........................................................................................................................16

Discussion..............................................................................................................................17
  A. Elevator Pitch and Game Summary..............................................................................18
  B. Feature Set..................................................................................................................19
  C. Gameplay and Mechanics..............................................................................................20
  D. Email Details................................................................................................................22

Conclusion and Future Work.................................................................................................23

Appendix A............................................................................................................................26

References.............................................................................................................................27
Introduction

The term ‘phishing’ describes an email scam where fraudulent users pose as a legitimate person or company to extract confidential information from the scam victim (Jampen et al., 2020). ‘Privacy’ can be described as freedom from intrusion and the ability to control the information about oneself. Hackers target private information including credit card and bank account information, private personal identification such as social security numbers, and passwords to sites with personal information about the victim (Federal Trade Commission, 2022). Phishing can also be used to attack a personal computer through malware for identity theft and stealing money. Hackers take advantage of their victims through the use of social engineering attacks, which disregard ethics and persuade victims to give away their personal, confidential information (Fatima et al., 2019). Phishing as a social engineering attack is alarmingly successful due to the emotional or contextual triggers that it may use to persuade victims to disregard security protections and interact with the scam. This disregard for online moral conduct creates a dangerous environment where the untrained eye for scams is easily susceptible to social engineering.

Phishing is often found targeting places of work and business. One of the most common types of phishing for companies and organizations involves spear phishing, which can be defined as scam emails targeted directly at a specific organization’s employees (Anawar et al., 2019). These phishing attacks are especially dangerous for companies if their employees are untrained, creating vulnerabilities in a company’s privacy. This can also be financially devastating if a company falls victim to a scammer’s fraudulent activity.
An attack on Ubiquity Network in 2015 scammed the company of $46.7 million through an attacker impersonating an upper management member. The scammer posed as the company’s CEO and lawyer and successfully convinced the company’s Chief Accounting Officer to “make a series of transfers to close a secret acquisition.” (Graphus, 2023). Another financially devastating attack in 2016 robbed the engineering company FACC of an estimated $50 million through a claimed “acquisition project,” where scammers, similar to the Ubiquity Network attack, posed as the CEO and asked for employees to comply with transferring funds. It is reported that about $10 million was prevented from transferring after the scam was discovered. However, the financial damage was too late (Graphus, 2023).

Often, companies integrate phishing training to educate their employees to protect individuals from identity theft and data breaches. One of the ways companies provide training includes simulations, which fall into the category of serious gaming. The term ‘serious games’ can be described as creating interactive software with an educational purpose or message in its gameplay (Breuer & Bente, 2010). Popular serious games span several genres, including the simulation *Microsoft Flight Simulator*, created in 1982, designed for mimicking real-life civil aviation for training purposes; *World Without Oil*, created in 2007, focusing on an alternate-reality game that educated players on possible effects of an oil crisis. For the classroom, the popular title *Minecraft Education Edition*, released in 2018, is a sandbox game built off of the best-selling game *Minecraft* (2011), where players can navigate a three-dimensional world while simultaneously crafting and building as they go. *Minecraft Education Edition* adds to the base of *Minecraft* by adding features designed for students to help build creativity, problem-solving, and STEM skills in an enriching and entertaining way (Cloke, 2023).
The gamification of training tools through serious games may allow for the knowledge to be retained for a longer period (Putz et al., 2020) and for users to receive an interactive, real-time experience that may better prepare them for real-time applications. This phenomenon can be explained by encoding specificity theory, which states that knowledge retention is higher when something is learned in a similar environment to which it is used (Wen et al., 2019). The intersectionality of cyber security and serious gaming is often to provide training and education to its players. The history of games created to support anti-phishing training has involved various gaming mediums, including board games, role-playing games (RPGs), and simulations. These games include the puzzle simulation game *Papers, Please* (2013), the card game *Control-Alt-Hack* (Denning et al., 2013), and the role-playing game *What.Hack* (Wen et al., 2019).

Simulations are a subcategory of serious games that refer to a real-life scenario that becomes gamified, often to educate or inform users (Deyo et al., 1988). Ensuring the user has a similar experience to a realistic scam scenario is essential to anti-phishing as a game design framework. Using different examples and triggers that may cause one to fall victim to a phishing attack is crucial in simulation training (Wen et al., 2019).

While there is a large discourse and resources available from anti-phishing training provided for employees in the business world, few studies are conducted in academic settings, including phishing training for college students based on training university staff. (Marsden et al., 2020). Students often benefit from game-based learning environments. Previous research theorizes that games have positive results for engagement of material and building skills in students (Adipat et al., 2021). Combining an understanding of student engagement with games and training materials that have proved successful in business can provide insight into creating novel training materials that can be administered to students in academia.
This research seeks to leverage knowledge and analysis of previous training tools and simulators created for businesses and the psychology of game-based education for students to synthesize new software. Our new training tool aims to help students achieve career readiness. Building these skills in academia through game-based learning may increase the retention of information. This direct relationship may reveal that students who begin with better emailing practices will retain this knowledge in their respective industries. This, in turn, would be beneficial for protecting the student’s personal information, and their future employers.

**Literature Review**

Research surrounding cybersecurity attacks and phishing scams has a relatively strong foundation in the scholarly world due to the urgent nature of identity theft and secure internet use. A broad section of study is dedicated to creating educational games as training tools to support employees within their respective organizations better (Görke et al., 2017). There is also a large foundation in game-based learning in educational settings and its positive impacts on student cognitive skills (Adipat et al., 2021). Studying different mediums of games created for anti-phishing training can help inform the novel approach used in this study. Understanding different factors of the individual and their relationship with technology and their psychology can be useful for developing the context within the simulation. Combining these ethics and psychological responses with the positive impacts of game-based education for students, the goals of this study can be achieved.

**User personality and its psychological effect on phishing susceptibility**

Phishing susceptibility derives from user behavior. Both experimental factors and personality traits contribute to an individual’s likelihood of being phished, including their
general and technological experiences and what is referred to as Big-Five Personality traits (Gosling et al., 2003). These traits consist of openness, conscientiousness, extraversion, agreeableness, and neuroticism, which drive the user’s behavior during phishing attacks. Of these personalities, there is a direct relationship between increased conscientiousness and reduced phishing vulnerability, while there are indirect relationships between increased openness, extraversion, and agreeableness and reduced phishing susceptibility (Parrish et al., 2009). In a study conducted to determine the validity of personality effects on phishing susceptibility, where a structured questionnaire was used to collect user personality information in a workplace, it was determined that those working in the IT Department were less susceptible to phishing due to their overall higher general and technological experiences and higher conscientiousness than Non-IT Department staff (Anawar et al., 2019).

A different study conducted by researchers at the University of Verona aimed towards determining phishing susceptibility among factors including demographics and what factors of a phishing email contribute to an effective increase in user susceptibility (DeBona & Paci, 2020). As part of this study, researchers sent simulated phishing emails to participants, creating one email that did not exploit principles of influence and another email that focused on authority and urgency for the user. Overall, 31.4% of employees in this study clicked on the fake link sent out in the first email phase, and 23.5% proceeded to submit their username and password to the fake phishing website, meaning that 69.2% of those who clicked the link also provided their credentials. Regarding the principles of influence, emails that contained urgency principles created more susceptibility than emails with authority and without principles of influence. This study also found that while there was some significance in demographics of age differences, job titles, or education, none were statistically significant (DeBona & Paci, 2020).
Organizational norms have also been analyzed regarding their susceptibility to phishing, cognitive processes that individuals use when processing an email, and user susceptibility. A study found that Heuristic Information Processing was less cognitively resourceful, characterized by the automatic processing of an email, resulting in a higher likelihood of being phished (Petrič & Roer, 2022). Systematic Information Processing proved ideal in decreasing the likelihood of being phished, as users process information in a more elaborate “stop and think” mindset. Systematic Information Processing is an encouraged form of reviewing information sent to a user. It can be beneficial as both an inherent processing mindset and a teaching tool to those more susceptible to phishing to decrease their likelihood (Petrič & Roer, 2022).

Eye-tracking studies in phishing susceptibility also provide context to how users interact with their media and vet their information. In a study by Alsharnouby et al. (2015), participants were subjected to eye tracking to record gaze information while viewing websites in a web browser at full-screen. The participants were presented with 24 websites, ten legitimate and 14 phishing sites, and were asked to determine which were legitimate or scams and how they decided. Their decision was measured on a scale of certainty. Results showed a positive correlation between time spent on areas of interest in the browser Chrome and webpage content and the participants’ performance scores, with the address bar being the most popular spot for users to check. However, their research does not account for whether the participant viewed the address bar subconsciously or if they used it to influence their decision (Alsharnouby et al., 2015).
**Efficacy of previous training tools and serious games**

Gamification that mimics real-world examples is an effective training tool that can create long-term retention of the content provided for training participants (Putz et al., 2020). “Overall, gamification turned out to have a positive effect on students’ knowledge retention, independent of age and gender” (Putz et al., 2020). Game-based education increases levels of engagement and learning when problem-solving facilitates learning (Adipat et al., 2021).

Training tools without gamified education have effective long-term results dependent on their implementation. A study was conducted using 515 participants randomly assigned to control, single-training, and multiple-training groups equally split (Kumaraguru et al., 2009). All participants were then sent three legitimate and seven spear phishing emails over 28 days, and anti-phishing interventions were shown when participants clicked on the link during the first day. In further days, if participants were part of the multiple trainings, they would receive another anti-phishing intervention if they clicked fake links. If a participant was part of a single training or control, the later days had participants receive simulated HTML pages. They were then asked to provide private credentials and fall victim to the fake scams. The anti-phishing training tool used *PhishGuru*, an embedded training system that teaches users to avoid falling for phishing attacks by delivering a training message when the user clicks on the URL in the simulated phishing emails. Results determined that users trained with *PhishGuru* retained knowledge after 28 days. Adding a second training message to reinforce the original training decreased the likelihood of users giving away their confidential information to phishing websites, and the training did not decrease the users’ willingness to click on links in legitimate messages (Kumaraguru et al., 2009).
Another tool, SAWIT – Security Awareness Improvement Tool, provides improved security awareness for employees in the workplace by enhancing cybersecurity among end-users and IT professionals (Kovačević & Radenković, 2020). SAWIT uses an artificial intelligence framework to improve employees’ cybersecurity knowledge by using collaborative learning and assessment within a knowledge-transformation model. The tool establishes a structural approach so awareness programs can add value to the organization or individual. Existing employees’ knowledge is measured through SAWIT, providing insight into the areas where security knowledge is lacking helping users build skills over time in a modular fashion. These methods are conducted in an interactive format so that users are more engaged and likely to retain the information they are learning through this tool (Kovačević & Radenković, 2020). This type of education tool is a complex simulation that bridges the gap between training tools, training message-based education, and training through gamified education.

There is no shortage of game-based education within the realm of cybersecurity training. The board game Control-Alt-Hack teaches players high-level security concepts, including phishing (Denning et al., 2013). The board game PhishI provides scenario-based learning and fosters brainstorming, interaction, and discussion. This game is useful in educating players regarding excessive online information disclosure and phishing awareness (Fatima et al., 2019). However, while these games increase awareness in this field, their design does not help simulate real-world decision-making that provides long-term retention of the information, nor the hands-on effects that this information needs to continue to be a long-term training tool. Non-phishing role-playing games such as Anti-Phishing Phil teach players to identify phishing URLs by playing as a fish, eating worms with safe URLs, and rejecting bait with phishing URLs. While this is effective for an isolated experience involving domain names and URL syntax, it does not
simulate how a user might come across the context of these URLs and other signs of phishing in email scams (Wen et al., 2019).

What.Hack is a Non-Phishing RPG that achieves a holistic anti-phishing education, teaching email phishing defense in context by replicating real-life situations and conditions for the user to interact with, providing clear goals and tasks for the user and increasing difficulty level throughout the game, and giving the user immediate feedback when they make a decision, and detailing the consequences of their decisions. The game provides a set of rules that a player must use to evaluate an email’s validity. As the game progresses, the rules become more specific and combine to create a complex rule set that simulates the reality of constraints that must be considered when users navigate their inboxes. What.Hack was concluded to be over 30% more efficient than previous non-phishing games for players to improve their skills in identifying email scams (Wen et al., 2019). This training game was inspired by the popular serious game Papers, Please (Pope, 2013), which requires players to play as a fictional border control officer and sort through documentation and determine whether they are viewing legitimate information from the characters in the game to let them into the country. The player is given rules to follow to properly background-check characters, and consequences for incorrectly identifying citizens or non-citizens in the game (Pope, 2013).

While the games previously mentioned are beneficial to the contribution of training tools proven successful for training adult employees, there is a lack of educational games geared toward students who have yet to enter the workplace environment. Studying successful educational games for this demographic may provide context and insight for a proper way to synthesize a game that aids the transition between student and employee.
The effects of game-based learning in educational environments

The proceedings by Kailani et al. in 2019 sought to review prior literature on the impact of games and their influence on learning. Much of previous research has focused on game psychology surrounding motivation, engagement, and knowledge acquisition. New research surrounds the impact of games on skill-building, such as problem-solving, communication, and critical thinking. This paper focused on how gaming research and literature from 2009 through 2016 impacted problem-solving skill development. This analysis concludes that game-based learning influences problem-solving at all academic levels. The higher the interactivity in a game, the higher the motivation and engagement of the student, which positively impacts their problem-solving skills (Kailani et al., 2019)

A study conducted in 2020 analyzed student agency within game-based learning. ‘Agency’ is a term in game-based learning that refers to an individual's “freedom to navigate a space [and] interact with game elements that foster learning” (Taub et al., 2020). This study examined 138 college students with certain levels of agency within a game environment. The impact was measured through participant’s emotions, interest, and engagement. It was concluded that students with a moderate degree of agency– not too high and not non-existent– led to higher engagement with enhanced learning experience while maintaining the highest levels of interest and enjoyment. This proves that some levels of agency impact problem-solving skills in a game-based environment (Taub et al., 2020).

Another study conducted in 2012 focused on ninth-grade classes where students had to evaluate changes in problem-solving abilities using different strategies. This study aimed to review the effectiveness of game-based learning in a digital environment on a student’s problem-
solving, learning motivation, and academic achievement. This study found that the digital game-based learning environment effectively enhanced problem-solving skills and improved learning motivation when compared to students who did not learn in a digital game-based learning environment. Game-based learning had no significant effect on academic achievement (Yang, 2012).

A study conducted in 2020 analyzed 159 student game players’ computer data while playing a serious game to understand the problem-solving process in undergraduate students. By analyzing computer log data, problem-solving performance scores, and survey data, the results concluded that learner metacognition affects learner problem-solving in a serious game, and learning goal orientation also affects learning problem-solving. This study provides helpful insight into problem-based learning pedagogy by analyzing learner characteristics and how they affect problem-based learning (Liu & Liu, 2020).

Analyzing how simulations affect problem-solving in students is also beneficial for the goals of this research. A study conducted in 2011 discussed how simulation-style gameplay influences the flow of learning experiences for students. By analyzing the feedback and problem-solving behaviors of 117 students playing a simulation game, results concluded that students who engaged in computational problem-solving within the game enhanced the flow of their learning experience compared to a traditional lecture, and found their intrinsic motivation to increase. It is also important to note that certain students who exhibited boredom and anxiety did not have in-depth problem-solving strategies and, therefore, did not engage with the material on a deeper level (Liu et al., 2011).
It is important to acknowledge what age demographics more successfully respond to phishing simulators to help determine the target age group for creating this game. For the studies previously mentioned, the outcomes that proved gamification had positive impacts on problem-solving skills and agency targeted college students for impacts of agency (Taub et al., 2020), undergraduate students for impacts of problem-solving (Liu & Liu, 2020), first-year college students and the impact of games on their flow of learning (Liu et al., 2011), and early high school students for impacts on problem-solving skills (Yang, 2012). Conducting these high school and college level studies indicates the potential for success using the same age demographic for an anti-phishing simulation game. An article in 2017 sought to analyze the efficacy of anti-phishing training for primary school-level children, finding that while the training improved the student’s knowledge of phishing in the short term by increased scores of 14%, the study found that after four weeks, the student’s phishing scores returned to pre-training levels (Lastdrager et al., 2017). This indicates a lack of retention for training primary students, which is important when deciding on what age groups to target for this new training game.

These studies provide insight into this novel approach by analyzing a positive impact on problem-solving skills within game-based learning environments. While these studies were less focused on whether games improve knowledge retention, they help understand why game-based learning is a better approach for learning and developing critical thinking skills. This research also notes the effects of a simulation-style game on problem-solving similar to other mediums of game-based learning, with an emphasis on skill building more than the medium of gameplay. These skills that game-based learning provides students are important to foster in academia, as they are transferable to career opportunities and success. A deep understanding of problem-
solving skills increases the value of the employee to the employer, which is advantageous in the labor market (Adipat et al., 2021).

*Components of a game design framework for phishing training*

Analysis of the game design framework can aid in developing meaningful gameplay for students to produce games that build a student’s critical skills and knowledge retention. The game design framework allows for creating an environment where users can interact with the learning material in an engaging way. Game patterns, user experience, and psychological aspects influence the learning experience (Fatima et al., 2019). These game patterns focus on gameplay loops reinforcing the player’s engagement and enjoyment. At the core, the gameplay loop must be effective in its educational aspect and a process that the user finds engaging enough to repeat to achieve an end goal.

Regarding cyber-security games, the design frameworks surround the presentation of the simulations and what the player must interact with to receive feedback on their consequences. It is also important to consider the difficulty of the information provided within the game and the gameplay itself to create a balance where players are learning and retaining information during gameplay. It is generally hard for users to understand phishing concepts and apply them (Fatima et al., 2019). Therefore, these learning tools must be presented at a level where, in general, users can to engage with the information at a level they can understand and grow in their knowledge and retention levels.
Examining types of phishing emails for game design framework

There is no limit to the types of phishing emails that exist and are deployed on unsuspecting users daily and globally. Many phishing emails are rooted in specific targeted strategies that are socially engineered to create the most successful attack. Some of the most common examples of phishing emails in 2023 include account deactivation emails where hackers pose as a compromised PayPal account to obtain a user's credit card credentials. Along the same vein, compromised credit card emails are also common, especially if the hacker can confirm recent purchases from the user to seem legitimate (Terranova Security, 2023). Transfer funds request emails exploit authority tactics for the user to aid their boss or company CEO, as shown in Figure 1. This scam appeals to a user’s agreeableness and willingness to “help” their company and the authoritative figure in their place of work (Terranova Security, 2023). Social media

Figure 1. Example of a scam email posing as the Vice President of Research and Economic Development from the University at Albany. Note that the email is sent from a gmail.com, not the appropriate albany.edu address.
request emails are conducted where the user accepts a friend request, and then proceeds to be
sent links to videos that install malware on you or your company’s devices (Terranova Security,
2023). Fake Google Docs logins target users to believe Google’s policies on logins have changed
and that users must change their account information by clicking the link in the email, which
takes them to a fake site to obtain their credentials (Terranova Security, 2023). Another phishing
email specific to the workplace involves company tech support requests, which victims may
believe come from their IT department requesting them to install new software on their device,
which proceeds to install ransomware on the device (Terranova Security, 2023). Other phishing
scenarios include fake giveaways, as seen in Figure 2, fake deactivation scares, look-alike
websites, and “go directly to jail,” which lures victims by tricking a user into believing that they

Figure 2. An example of a phishing email posing as a
University at Albany staff member giving away an expensive
personal belonging to scam users out of money for delivery
fees.

2023). Fake Google Docs logins target users to believe Google’s policies on logins have changed
and that users must change their account information by clicking the link in the email, which
takes them to a fake site to obtain their credentials (Terranova Security, 2023). Another phishing
email specific to the workplace involves company tech support requests, which victims may
believe come from their IT department requesting them to install new software on their device,
which proceeds to install ransomware on the device (Terranova Security, 2023). Other phishing
scenarios include fake giveaways, as seen in Figure 2, fake deactivation scares, look-alike
websites, and “go directly to jail,” which lures victims by tricking a user into believing that they
have been caught for something illegal and that the victim must pay money to the government immediately to avoid consequences (Strebe, 2017).

**Novel Approach**

The articles that have been examined aid in the understanding of phishing susceptibility and what tendencies individuals have that make them more likely to be victims of phishing. As personalities and experiences converge, it can be determined that gamified education and interactive training tools can help users learn about phishing and decrease their likelihood of falling victim. Both the SAWIT AI model and the game *What.Hack* are effective tools in training users and creating long-term retention of knowledge. Their designs are ideal for studying and understanding the framework for creating an effective training tool. This study intends to expand upon the cyber security training tools that are present by leveraging research to create a novel simulation to debut as a training tool for adolescents to increase a student’s career readiness. The model this training tool will follow is most similar to *What.Hack* in terms of its game-based training and implementation, and will seek to use a game-design framework to ensure that the game is effective in its training purposes, fun, and engaging for those that participate to increase knowledge retainment.

**Methods Plan**

This research is intended to create a new simulation geared toward students in a digital game-based learning environment. This quantitative research, as conducted by the literature review, is used to inform the creation of this software.
The simulation will be digitally developed using the Unity game engine and will be ready for deployment on personal computers. The game will consist of an office environment mimicking a private office in a business building, in which users will work through their email inbox to determine if they have received a phishing email and receive feedback on their choices.

Discussion

*OfficeGuard* aims to combine the known literature on training software for anti-phishing and the principles of problem-based learning for students with game development and design. Prior studies can be used as proof of successful training on employee retention and to build a

![C# Programming from OfficeGuard. This script runs through the library of email text available for the game.](image)
simulation structure. Games like *What.Hack* are effective in their retention. However, their design was created for the adult employee demographic. Understanding the psychology around problem-based learning in high school and college students is important in understanding what makes an effective and engaging game that will help improve problem-based learning and prepare students for industry. *OfficeGuard’s* development took into consideration a model of *What.Hack* while applying plot features, design, and information to be geared toward a younger audience.

**Elevator Pitch and Game Summary**

In *Office Guard: The Anti-Phishing Training Game*, play as an office employee as you sort through your emails and work life. But beware, some emails you receive throughout the day may be scams that attempt to rob you of your personal information. Can you determine which emails are real and avoid the ones that are not?

![Figure 4. A Screenshot of the desktop scene in OfficeGuard. A scam email, contacts list, and notifications are visible.](image-url)
In this game, players take on the role of an employee named Stacy Connors, who must sort through her emails at the beginning of her work shift. Accept invitations from coworkers to attend work parties, confirm your order for a corporate lunch, and send five thousand dollars with credit card details to a coworker stranded on vacation! Wait a moment, you just saw that coworker in the office thirty minutes ago.

In this game, your company has a major problem: they have a heavy amount of incoming phishing email scams. Navigate a contact list of people your character knows to confirm coworkers’ lives outside of work and determine which emails are legitimate and must be replied to.

**Feature Set**

This game consists of a few special features, including an email app allowing players to point and click on emails throughout the game. Determining the correct tag (legit or scam) for an email has positive or negative repercussions in the game. The contact list will remain the player’s lifeline in the game, as it contains all the correct names and contact information for real coworkers in the email lists. This game will feature one boss character and five coworker
characters with whom the main character has contact with. There will be ten emails for players to sort through in the game, featuring five real and five scam emails.

Gameplay and Mechanics

The game’s main objective is to identify and reply to the real emails while deleting the scam emails. Players will navigate their email app and tackle emails one at a time. Players will receive the appropriate consequences depending on their interaction.

The emails will appear one at a time for players to interact with. Each email has a scam or legit tag within Unity, and players may take their time to determine the email’s legitimacy. Players can look around at their desk contents and zoom in on some featured objects and devices in the game. This includes a computer that houses the email app to respond to emails and a

Figure 5. View of the 3D office environment in OfficeGuard.
contacts app to check their contact list.

![Image of OfficeGuard interface with scam email and contact list]

**Figure 6.** Desktop view in *OfficeGuard* with a scam email and contact list.

Interactable apps in this game will include an email app that appears as an icon in the corner of the computer screen. The emails will appear in a window and must be replied to or deleted to move to the next one. Some emails may include links. The contacts app will also appear as an icon in the corner of the computer screen. Players can open the contact app alongside the email app and click through different list pages, like an online content booklet. Contact information will include a contact name, job title, email address, phone number, and social media handle. This will help provide context for some emails and, therefore, cause the player to fact-check the legitimacy of the content.
The five scam emails will include an email from a coworker begging for money via providing credit card details, an email from a boss asking to pass a big budget through a payment invoice, confirmation of a package address, sending confidential documents to a scam user posing as a coworker, and an email claiming to be from the email company asking for an email address and password update. The five legit emails will include the user having to enter credit card information to order food for a corporate lunch, entering a name to sign up for a coworker’s holiday party, sending availability to a coworker for a meeting time, sending documents to a boss for an upcoming meeting, and clicking a link to view a coworker’s pictures from a vacation they recently returned from.
Conclusion and Future Work

Much of the scholarly literature surrounding phishing discussion focuses on training for the business world. It is equally important to educate high school and college students on email etiquette and training to help protect students early on and their future employers. There is a large opportunity to look into the effectiveness of phishing training on high school and college level students and determine whether it is beneficial to train students during their formative years to prepare them for the industry.

![C# Script for OfficeGuard](image)

**Figure 8.** C# Script for *OfficeGuard*. View of the Toggle Visibility function for the Contacts App to view the contact list.

Gamified education is an effective way for students to build skills beyond the specific training. By participating in game-based learning, students can improve their problem-solving
skills and their engagement with the material (Adipat et al., 2021). By combining knowledge of phishing training and the effectiveness of game-based learning for students, further study can be conducted to determine the efficacy and retention rate of anti-phishing games such as *OfficeGuard* on high school and college level students.

Future work for this study includes improvements to the current simulator and deploying the study to test whether the game effectively retains phishing training education for students. The current simulator can be improved upon in several facets. The first is a privacy breach feature, where players who continue to fall for scam emails face consequences that make the game more challenging. This can be done through notifications that warn the player of identity theft and fictional malware that affects gameplay. Another aspect of the game that improves context is implementing a fictional social media app feature on a tablet device so that players can see their coworkers’ backstories within the game. This can help contextualize certain emails within the game (i.e. suspicious emails about coworkers on vacation) and help the player make better informed decisions. The game’s current iteration alerts the player whether they correctly reacted to the email in their inbox. In a future iteration of the game, there will be more specific feedback to educate the player on their experience within the game. There will also be more interactable features, such as clickable links that take the player to fictional websites within the game, and places to insert credit card and personal information if a player chooses to follow up on an email.

The design of a future study is also interesting to determine if this game is effective for high school and college-level students. With game deployment in a classroom setting, students would receive a pre-test to determine phishing training knowledge before the game, followed by a playthrough, and a post-test to determine if there was an immediate knowledge increase from
the game. Then, after several weeks, the post-test would be given to students again to determine if they retained the information from the game. There would also be an opportunity to compare the outcomes between high school and college level students, as well as the success rates of these students.
Appendix A

To view the game on GitHub, please visit: https://github.com/oliviabena28/honors-thesis-2024


https://doi.org/10.1145/3334480.3381435


Pope, L. (2013). Papers, Please. [Video Game].

https://store.steampowered.com/app/239030/Papers_Please/


https://doi.org/10.1016/j.chb.2020.106392


https://doi.org/10.1016/j.compedu.2019.103781


https://doi.org/10.1145/3290605.3300338