INFO36206 ISS Graduation Project
Project Plan for Phase 1

Submitted by:
Arnold Tam, Kyle Meyers, Matthew Nichols, Tayyab Jafar
Submitted for: Ali Hassan

February 17th 2023

Contents

1 Problem Statement

Cybersecurity awareness training is crucial for organisations as it can significantly reduce the risk of cyberattacks and threats by educating employees on various types of attacks that they may encounter at work [1, 2]. However, such training poses challenges, including the need for frequent repetition due to the rapidly evolving digital landscape and the emergence of new cyberattack forms. Additionally, the content and delivery methods used in training may not be engaging enough, resulting in poor retention by employees [3]. As a result, they may forget the practices they learned over time. To address this issue, a new and more effective training delivery method is needed. The proposed solution is to incorporate gamification into cybersecurity awareness programs, which blends gaming and serious gaming elements. This approach is an innovative and engaging way to promote behavioural changes and ensure that employees retain the information and skills they acquire during the training. By incorporating gamification into cybersecurity training, organisations can create a more engaging, enjoyable, and effective training experience that will ultimately lead to a more secure work environment.

2 Project Goals and Outcomes

The project has several goals and outcomes it aims to achieve. The primary objective is the development of an open-source gaming tool, which will allow the creation of interactive and engaging cybersecurity awareness training regimens. The game will be inspired by existing popular games (such as Plants vs Zombies), as well as existing SA training frameworks and programs. The project also seeks to assess individuals' experiences with traditional formats of security awareness training, to determine the efficacy of traditional methods and to determine how they can be improved upon. The results of this survey will allow companies to accommodate for specific training needs and requirements.

The project will also include documentation for deployment, which will facilitate the game's accessibility and help to ensure its successful implementation. Finally, we will publish this game as an open source tool to contribute to the development of innovative and effective methods for cybersecurity education. Overall, we will attempt to make our tool an integral part of improving cybersecurity training and education, potentially benefiting a broad range of both individuals and organizations.

3 Literature Review

Gamification has become a popular solution in different industries to address behavioural problems [4, 5]. It involves applying game elements and mechanics to non-gaming situations with the goal of boosting user engagement and motivation. By using techniques like rewards, leaderboards, badges, and points, the user's interest in the activities can be enhanced. One area where gamification has been applied is in cybersecurity training, where it has been used to promote engagement, participation, and motivation. A study has explored the effectiveness of serious games and found that they outperform traditional methods of delivering content [6].

However, research is sparse on the efficacy of fully gamified training, especially in the area of cybersecurity awareness training. In addition to this, because the use of gamification in cybersecurity awareness training is still relatively new, there is currently no clear standard on which type or genre of gaming is most effective for employees.

The SA framework outlined in NIST publication 800-50 specifies several requirements that must be met by SA programs [7]. These include ease of use, scalability, accountability, and support from various industries. Additionally, a training plan that encompasses goals, covered topics, exposure frequency, and the capacity to update the material easily must be implemented to ensure that the SA program remains current with developments in the information security domain.

4 Proposed Solution

Our proposed solution is to design a fully gamified SA tool that encompasses cybersecurity awareness training topics and attempt to solve the challenges posed by Arctic Wolf.

The standard for the game will involve a mix of traditional gaming and serious gaming – wherein the game itself will become a hub for fun with challenges involved that revolve around security training. We will explore open-source programs that exist, then build our own. Leaderboards, items, perks, and other gamified features will be included for those that accomplish tasks to stand out from other employees.

We plan on building our program on the Godot engine, which is an open source, multi platform game engine, commonly used in High Schools to teach game design, as well as elementary schools as an education platform. There are multiple benefits for choosing the Godot platform: ease of learning, multiple language support, lightweight, as well as a vast array of resources for learning [2, 8].

5 Project Requirements and Constraints

The NIST guidelines state that creating a successful Security Awareness (SA) program requires multiple elements. To achieve maximum effectiveness, our gaming framework must be designed to accommodate these elements, which will help identify requirements and tasks. The four main requirements for delivering SA material are ease of use, scalability, accountability, and broad-based industry support. In addition to this, a training plan must be in place, which includes goals, covered topics, frequency of exposure, and the ability to easily update the material. To stay adaptable to the constantly changing security landscape, our SA tool must be able to accommodate updates through implementations such as a "level editor", allowing the creation of new training modules with ease.

The SA program's plan must conduct a needs assessment that caters to the individuals within an organisation and their role in handling data. This may be done through an assessment process either within or before the SA game, which will in turn determine the user's experience and training [7, 9]. The 6 role categories and 5 priority groups outlined in the NIST document may pose a challenge, as creating a different experience for each role may be overly complex.

The SA program must establish priority and address specific training needs based on the user's role in the organisation or familiarity with SA concepts [7]. Again, can be achieved through an assessment process either within or before the game. The gathered information can then be used in conjunction with a level up or difficulty system to offer a suitable learning platform regardless of experience with Information security concepts.

The NIST 800-50 outlines over 25 topics that could be covered in the SA program [7]. This may be the largest constraint, as there are too many topics to cover in a single program. To keep the scope manageable, only the most relevant and important topics should be focused on.

Finally, the SA tool must be able to receive feedback and monitor success indicators, which may be done through in-game events, surveys, or scoreboards [7]. With over 700 potential training lessons based on 6 roles, 5 priorities, and 25 topics, the scope of the project could pose a challenge. As such, a system that allows for rapid creation of new training lessons is necessary, and the number of topics should be limited to those that are relevant to the current cybersecurity landscape or the user's priority/role.

Barring the constraints mentioned above, another major constraint to consider is the shortcomings of the engine/platform which we chose to build on. In order to deploy Godot, companies must have some level of understanding regarding the programming language used. Ideally, we'll attempt to create proper documentation for the deployment of our program to compensate for this.

6 Detailed Timeline

Here's a detailed timeline for developing a game, including the identification of tasks, key milestones, and task delegation:

Planning Phase (1-2 weeks)
Task: Identify the game concept, storyline, gameplay mechanics, and target audience.
Milestone: Game design document (GDD).
Delegation: All party members.
Estimated to be completed by end of February.

Pre-Production Phase (2-4 weeks)
Task: Develop the game's art style, create a level layout, and plan out game mechanics.
Milestone: Pre-production phase complete.
Delegation: All party members.
Estimated to be completed by end of March.

Production Phase (3 months)
Task: Create 2D models, textures, animations, and sound effects. Program game mechanics, UI, and controls. Implement security training modules.
Milestone: Alpha version of the game ready for internal testing.
Delegation: All party members.
Estimated to be completed by end of June.

Quality Assurance (QA) Phase (4 weeks)
Task: Test the game for bugs and issues, refine gameplay mechanics, and balance difficulty.
Milestone: Beta version of the game ready for external testing.
Delegation: All party members.
Estimated to be completed by end of July.

Launch Preparation Phase (4 weeks)
Task: Create promotional materials, develop a marketing plan, prepare survey team for feedback.
Milestone: Game ready for launch.
Delegation: All party members.
Estimated to be completed by end of August.

Launch and Post-Launch Phase (Ongoing)
Task: Release the game on multiple platforms, monitor feedback and reviews, and plan future updates and expansions.
Milestone: Successful launch and positive feedback from the audience.
Delegation: All party members.

References

[1] A. Smith, "Pros and cons of starting a cyber security awareness campaign," *IT Security Central*, December 2017. [Online]. Available: https://itsecuritycentral.teramind.co/2017/12/28/pros-and-cons-of-starting-a-cyber-security-awareness-campaign/

[2] Godot, "Features - godot engine," *Godot Engine*. [Online]. Available: https://docs.godotengine.org/en/stable/about/list_of_features.html

[3] Arctic Wolf, "6 biggest security awareness program challenges—and what to do about them," *Arctic Wolf*, May 2021. [Online]. Available: https://arcticwolf.com/resources/blog/6-biggest-security-awareness-challenges/

[4] L. Irwin, "How gamification can transform cyber security awareness training," *GRC eLearning Blog*, July 2022. [Online]. Available: https://www.grcelearning.com/blog/serious-games-to-tackle-serious-threats-how-gamification-can-transform-your-cyber-security-e-learning

[5] Terra Nova, "5 reasons why you need gamification in your cyber security awareness program," *Fortra's TerraNova Security*, September 2021. [Online]. Available: https://terranovasecurity.com/reasons-you-need-gamification-in-security-awareness/

[6] T. van Steen and J. R. A. Deeleman, "Successful gamification of cybersecurity training," *Cyberpsychology, Behavior, and Social Networking*, vol. 24, no. 9, September 2021. [Online]. Available: https://doi.org/10.1089/cyber.2020.0526

[7] M. Wilson and J. Hash, "Building an information technology security awareness and training program," *National Institute of Standards and Technology*, 2003. [Online]. Available: https://arcticwolf.com/resources/blog/6-biggest-security-awareness-challenges/

[8] Good Passive, "How to choose a game engine for educational games," *Good Passive*. [Online]. Available: https://www.goodpassive.com/how-to-choose-a-game-engine-for-educational-games/

[9] P. Toth and P. Klein, "A role-based model for federal information technology/cybersecurity training," *National Institute of Standards and Technology*, 2014. [Online]. Available: https://csrc.nist.gov/CSRC/media/Publications/sp/800-16/rev-1/draft/documents/sp800_16_rev1_3rd-draft.pdf