INFO36206 ISS Graduation Project (Phase 1)

Deliverable 1: Initial topic submission

Tayyab Jafar - 991599234

Topic Title: Development of an open-source gaming framework for use in cybersecurity awareness training as an alternative to traditional training methods.

Problem: Cybersecurity awareness training plays a key and critical role to organizations in that employees that undergo the training can help to decrease the risk of attacks and threats on the organization by educating them on the types of cyberattacks they may encounter in the workplace. However, it can also present challenges. These training programs may need to be repeated frequently due to the rapidly changing nature of the digital world and new forms of cyberattacks emerging constantly. Additionally, employees may not retain the information or be engaged in the training due to the lack of interesting content or delivery methods. Over time, employees may lose the practices they learned. Thus, a new deliverable method of training must be developed, one that improves the likelihood of behavioural changes. The proposed solution is the gamification of cybersecurity awareness programs – one that focuses on a mixture of gaming and serious gaming.

Description: According to various resources [1, 5, 6], over half of all cyber attacks take place on SMB's (small and mid-sized businesses). As the world becomes more digital, these attacks will continue to grow larger and more frequently in scope. A key factor to all of this is people. Employees remain vulnerable to all types of attacks – social engineering, phishing, and other forms of attacks targeted towards them.

As a response to better protect organizations, security awareness programs were developed. Cybersecurity Awareness Training is a standard practice in corporate environments to help, educate and raise awareness of employees about the risks in the digital space, their workplace and to develop practices to protect themselves and the environment they work in [1, 5].

However, there are drawbacks to training programs – namely cost, efficiency, and effectiveness. Arctic Wolf poses 5 challenges due to security awareness training [2]:

- Programs become outdated fast
- Burden on administrators
- Low employee participation
- Employees lose interest in security awareness
- Employees forget what they've learned

Other cybersecurity organizations also report the same issues throughout their experiences in the industry [1]. Cybersecurity awareness training does not always guarantee results, it is beneficial,

but the long-term results tend to return to the baseline as employees will inevitably lose interest on mandatory security training covering topics they may not be interested in, with no passion for the delivery of the content – which often is dry and tedious in static formats.

One solution that has been gaining popularity across various industries to tackle these behavioural issues is gamification [4, 7]. Gamification is the application of game elements and mechanics to non-gaming contexts to increase engagement and motivation. Techniques like points, badges, leaderboards, and rewards are used to make activities more interesting for the end user. It is used in various fields already, including some aspects of cybersecurity training to improve engagement, motivation, and participation. Due to how novel the usage of gamification is in cybersecurity awareness training, there is no concrete standard for the medium and genre of gaming that is most effective for an employee. One study [8] has investigated the use of serious games and found that they improve upon traditional methods of content delivery, however, no research has yet examined the complete gamification of training, including the use of all techniques previously mentioned, specifically in the context of a cybersecurity awareness training.

The purpose of this capstone project will be to develop a game that encompasses cybersecurity awareness training topics and look to solve the challenges posed by Arctic Wolf by ensuring employee retention, keep interest active, become flexible for future updates, and overall be a fun mechanism that changes the behaviour of employees and their approach to security awareness.

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. This project will likely clone Open RuneScape game framework as said hub and revision quests as security training topics for the user to explore and solve [3]. Leaderboards, items, perks, and other gamified features will be included for those that accomplish tasks to stand out from other employees.

Should it deem difficult, other open-source game frameworks exist to research into, or one can be created from the ground-up. Should it be successful, when compared to other forms of gamification that exist in the industry, we will open source it for the industry to use and develop upon so that they may implement this format in their own cybersecurity awareness training programs.

References

[1] A. Smith, “Pros and cons of starting a cyber security awareness campaign,” *IT Security Central*, 18-Dec-2017. [Online]. Available: https://itsecuritycentral.teramind.co/2017/12/28/pros-and-cons-of-starting-a-cyber-security-awareness-campaign/. [Accessed: 26-Jan-2023].

[2] Arctic Wolf, “6 Biggest Security Awareness Program Challenges—And What to Do About Them,” *Arctic Wolf*, 08-May-2021. [Online]. Available: https://arcticwolf.com/resources/blog/6-biggest-security-awareness-challenges/. [Accessed: 26-Jan-2023].

[3] Core Framework, “Open runescape classic,” *GitLab*. [Online]. Available: https://gitlab.com/open-runescape-classic/core. [Accessed: 26-Jan-2023].

[4] L. Irwin, “How Gamification Can Transform Cyber Security Awareness Training,” *GRC eLearning Blog*, 11-Jul-2022. [Online]. Available: https://www.grcelearning.com/blog/serious-games-to-tackle-serious-threats-how-gamification-can-transform-your-cyber-security-e-learning. [Accessed: 26-Jan-2023].

[5] Proofpoint, “What is Security Awareness Training?”, *Proofpoint US*, 13-Oct-2022. [Online]. Available: https://www.proofpoint.com/us/threat-reference/security-awareness-training. [Accessed: 26-Jan-2023].

[6] PurpleSec, “2022 cyber security statistics trends & data,” *PurpleSec*, 17-Oct-2022. [Online]. Available: https://purplesec.us/resources/cyber-security-statistics/. [Accessed: 26-Jan-2023].

[7] TerraNova, “5 Reasons Why You Need Gamification In Your Cyber Security Awareness Program,” *Fortra’s TerraNova Security*, 27-Sep-2021. [Online]. Available: https://terranovasecurity.com/reasons-you-need-gamification-in-security-awareness/. [Accessed: 26-Jan-2023].

[8] T. van Steen and J. R. A. Deeleman, “Successful gamification of cybersecurity training,” *Cyberpsychology, Behavior, and Social Networking*, vol. 24, no. 9, pp. 593–598, 2021.