A Cybersecurity Awareness Escape Room using Gamification Design Principles

C. DeCusatis, B. Gormanly, E. Alvarico, O. Dirahoui, J. McDonough, B. Sprague, M. Maloney, D. Avitable, and B. Mah
Marist College
Poughkeepsie, NY USA
casimer.decusatis@marist.edu

Abstract—**Recent studies have shown that a significant fraction of cybercrimes are a direct result of user errors, which could be prevented with improved cybersecurity awareness training. We have developed a virtual cybersecurity escape room based on the three-dimensional Unity game development platform to improve cybersecurity awareness. Unlike most prior efforts, this application is based on the proven Octalysis gamification framework, which has been shown to improve user engagement and knowledge retention. Further, we integrate ethical decision making based on the IEEE Code of Ethics. Following a discussion of the application design, we present playtesting results and experimentally quantify the application's performance based on eight gamification metrics.**

Keywords—Cybersecurity, awareness, gamification, Octalysis

I. INTRODUCTION

According to recent industry reports, cybercrime will cost the global economy $6 Trillion during 2021, an increase of 50 times in the past five years [1]. Further, the cost of cybercrime is expected to escalate to over $11 Trillion per year by 2025 [1]. Human error continues to be the primary cause for 86% of these data breaches, with phishing attacks alone making up over 35% of known breaches [2]. These issues are directly related to a need for improved cybersecurity awareness training, which should help users recognize and avoid behaviors that would compromise cybersecurity. A 2021 study shows that only 27% of global information workers claim to be aware of their organization's security policy, while 8% admitted to deliberately ignoring or circumventing security guidelines when it seemed convenient [3]. The sheer number of cyberattacks resulting from incorrect user behaviors indicates that current cybersecurity awareness programs are not being effective. Recent reports on best practices to improve employee cybersecurity behaviors [4] highlight several key issues with current cybersecurity awareness training techniques. While there are many commercially available security awareness training offerings, most are based on passive learning schemes (video or written lectures) accompanied by an assessment or quiz. Users need to repeat this training until they earn a sufficiently high passing score on the assessment. This type of training has little long-term impact once the assessment is completed [4], and users often fail to retain this information and recognize threats outside of a training environment. User surveys indicate that such training is perceived as being more about passing audits and limiting liability than protecting valuable corporate assets [4]. In fact, users may resent being forced to take time for this training, since it is framed as being additional overhead on top of their regular duties. If training is an annoyance, users will try to get through it as quickly as possible so they can return to other work tasks. Worse, users often perceive security as being part of the IT department's job, rather than being a shared responsibility for everyone in the organization.

This is not just a problem for large corporations; pre-college and college environments have become a particular target for cyberattacks [1-4]. Many bad actors view students or non-technical educators as relatively inexperienced users, who can be more easily targeted. There is a global shortage of close to 4 million trained cybersecurity professionals [5] meaning that pre-college and college cybersecurity environments are often understaffed and underfunded. While it may seem that such environments lack high value assets, they are actually a rich source of personal identifying data, medical records, student loan information, and other data which can be monetized by attackers. Further, bad actors don't just steal data; they are constantly trying to plant malware which conscripts computers as part of botnets, crypto currency mining, spam broadcasting, or money laundering schemes. Educational institutions often have connections to government or private industry through grants and other joint projects, making it possible for bad actors to use education systems as a beachhead for other attacks. For these reasons, there is a particular unmet need for cybersecurity awareness training in pre-college and college level educational institutions.

Gamification has been recognized as a useful training concept, based on nearly two decades of research since the term was first coined [6]. It does not refer to simply adding a playable game to existing training approaches, as done by many organizations in an apparent effort to capitalize on the marketing value of this approach. Rather, gamification refers to a bottoms-up design process which places highest emphasis on using human motivation to promote engagement, motivation, and retention of information. This human-focused

978-1-6654-8303-2/22/$31.00 ©2022 IEEE

design methodology (as opposed to traditional function-focused design) attempts to apply the most enjoyable elements found in games to other productive activities, such as education and training. While this approach may involve game mechanics such as scoring points, earning rewards, and completing increasingly difficult challenges, the scope is actually much greater. It may include cultural, personal, economic, environmental, and other aspects. Game-based learning provides a way for students to become actively involved in the learning process, encouraging them to explore and experiment in a risk-free environment.

Many organizations treat cybersecurity awareness as a necessary overhead, rather than an essential part of their culture. This approach tends to result in limited engagement and few long-term benefits; such organizations are almost as likely to be successfully attacked in the long-term as if they had not bothered with awareness training at all [2-4]. By contrast, studies have shown that organizations and chief information security officers with a strong security culture have employees who are educated, enabled, and enthusiastic about their personal cybersafety and that of their employer [4]. Organization leadership that considers cybersecurity awareness as an investment in their employees tends to make security part of the vision and values of everyone in the organization. Creating and sustaining cultural change in this fashion is a challenging task. While the total addressable market for cybersecurity awareness training is about $1.5 Billion, and growing at a rate of four times during the next three years [3], most existing forms of awareness training do not incorporate a full range of cybersecurity education methodologies. Broadly speaking, there are two main methodologies related to awareness training, namely motivation and deployment [7]. Motivation methodologies attempt to enhance user engagement in order to achieve some educational objective; this is often the only approach applied to game-based awareness training. Deployment methodologies, which are often neglected, incorporate a comprehensive training framework, including both technical and ethical aspects, which can be quantified and applied to real world situations. Our efforts to develop effective gamification of cybersecurity awareness training take advantage of both methodologies.

A research study sponsored by Purdue University demonstrated the potential effectiveness of game-based cybersecurity training on a group of over 200 participants in the greater Chicago area [8]. Students were shown to retain about 90% of concepts they were allowed to practice, as opposed to about 20% of what they simply read or heard. Gamification was particularly effective when engaging traditionally under-represented gender groups (female students) and under-represented diversity groups (African American and Hispanic). Further, gamification of cybersecurity awareness had the additional beneficial effect of significantly increased interest among students in pursuing degree programs in cybersecurity and related fields. Despite this, the application of gamification to cybersecurity awareness has been limited [7]. There have been attempts to gamify computer and security education for young students (ages 5-10) using graphics and storytelling techniques, which have met with varying degrees of success (a brief survey is provided in [7], although recently some of these applications have been discontinued or are no longer available). There are some offerings which are not formally supported or which simply bundle actual games with conventional training as in the online card game available for enterprise users [9]. Such an approach neglects the target user's requirements and does not realize the full benefits of a gamification methodology. This same problem occurs with a number of commercially available cybersecurity awareness offerings which attempt to incorporate gamification without using a true bottoms-up design with a proven framework for measuring learning [10]. Further, existing offerings fail to target pre-college and college environments as their primary users, often being cost prohibitive for such environments. Finally, these offerings tend to focus on technical aspects of training, while neglecting equally important ethical considerations; decoupling ethics from cybersecurity can lead to significant gaps in training effectiveness [11].

In this paper, we present a novel cybersecurity awareness virtual escape room training game based on the proven Octalysis gamification framework. The escape room has a science fiction theme, and follows the playable character ARI (Automated Repair Intelligence), a robot learning about computer security as it attempts to save its creators from impending doom. The goals of this work include providing a constructive gamification experience that helps pre-college and college students, as well as other audiences, to iteratively improve their cybersecurity skills. The training incorporates before and after assessments to evaluate the effectiveness of this approach, and verify that learning has taken place.

The remainder of this paper is organized as follows. After the introduction, we describe the development and storyline for our virtual escape room training. We experimentally quantify this approach using the eight-point Octalysis framework. We then summarize our plans for ongoing work in this area.

II. Framework and Experimental Results

The ARI 3D escape room application was created using the Unity cross-platform, interactive 3D development platform using the C# language [12]. Unity is widely recognized as among the industry's leading platforms for interactive game development. We also used some open source digital assets and art from the Unity Asset Store, such as the model for the ARI robot and some of the virtual environments (figure 1). We used Amazon Web Services (AWS) for data storage and website hosting services, including AWS S3 and DynamoDB. The source code is available on our GitHub site, and a downloadable playable version of the game is available from our website [cite http://aricyberthink.com/].

978-1-6654-8303-2/22/$31.00 ©2022 IEEE

Figure 1: (top) 3D avitar for the ARI robot, from the Unity Assets open source store (bottom) example 3D environment

The robot ARI is the user's first-person point of view avatar, a utility robot who was just activated on a remote space station and is tasked with saving their creator's life in an immersive storyline. There is an emergency of unknown origin on the creator's ship which is in transit near the damaged station, and the only form of contact between ARI and its creator is through distorted audio transmissions that occur once at the end of each level. The station is in lockdown, and ARI must navigate through different rooms and sections of the station, learning and solving cybersecurity challenges to unlock doors and find the resources necessary to guide their creator back safely. There is a ticking clock, since the creator's fuel and energy are running out, so there is a limited time to recover the creator's ship. Each level completed will progress the plot by bringing the creator one step closer to safety. As the plot unfolds, ARI undergoes a character development arc and learns more about the true nature of the situation. ARI progresses through a semi-linear branching path in the station overworld (the story location), using node-based movement (point-and-click). We created a custom script for movement which includes node creation, locating nearby nodes, and movement for both the camera and point-of-view character. When the user enters a node, adjacent nodes can be unlocked for the next stage of movement; on a PC platform, for example, the left mouse button allows for movement while the right mouse button allows the user to look around without moving. Nodes can also serve as triggers for interactive game elements.

Gameplay includes randomly generated elements and "Easter Eggs" to increase replay value, mini-games that encourage the user to hone their cybersecurity skills, and interactive, informational items that contain elements of the backstory interwoven with basic cybersecurity and ethical principles. The playable character ARI allows the user to put themselves into the point-of-view role, since ARI has no prescribed gender, age, or ethnicity. It is possible to customize the avatar and create a more personal game play experience, which has been shown to increase user engagement [6].

Our novel approach concentrates on experiential learning; motivating users to practice with hands-on examples as an effective way to increase skill retention. The application is a puzzle solving game, with no violent elements, making it suitable for a broad age range. The game is designed for ludonarrative harmony (there is no conflict between the narrative told through the story and the narrative told through the gameplay) [13]. Learning is also facilitated with immersive storytelling, interactive puzzle solving, and other game mechanics. Users engage with the story through a dialog manager with interactive prompts, which initiate discussions between ARI and the Station's Artificial Intelligence (AI). We created a custom script for the dialog manager, which is a combination of user triggered and automatic dialog. Some nodes serve as triggers for story dialog popups and related audio. Interacting with objects provides a prompt to begin other dialogs. The game uses a full voice cast acting from an original story script. The Station AI serves as both narrator and guide as the user progresses through the game. These dialogs facilitate the user's learning experience; the fully voiced cast acting was performed by our application developers.

Fundamental cybersecurity concepts are introduced incrementally throughout the game, which consists of a series of cybersecurity awareness and training modules themed with different aspects of cybersecurity and ethics. The user's progress is monitored and evaluated before and after each level. Each level is designed to be playable within 20-30 minutes, and all levels are interlinked with a common story arc, supported by cut scenes, with mini-game side quests. The current game levels, structure, and inspirations for mini-games are shown in table 1. Each level is playable with three difficulty settings (novice, proficient, and expert). Long-term players are encouraged and rewarded with cumulative scoring leader boards and other digital awards.

Table 1: Cybersecurity awareness topics and gamification elements

Levels	**Cybersecurity Theme**	**Gamification Elements**
Tutorial	Bad Practices	Don't plug random USB drives into a system (ethical concerns)
Level 1	Password Security	Good password practice (roll-a-ball mini game to select enough letters, numbers, and characters to build a strong password)

		Cryptography principles (Caesar cipher mini-game) Multi-Factor Authentication (found phone lock picking mini-game)
Level 2	Internet Fraud	Phishing Scams (select legitimate emails to avoid a DDoS attack) Social Engineering (create your own scam message using a set of word blocks)
Level 3	Network Security	Defense in Depth (inspired by Frogger style mini game) Firewalls (inspired by Temple Run style mini game, with blacklisting punishments) Malware and Viruses, including Ransomware (inspired by Asteroids style mini game)

Ethical considerations are presented throughout the narrative in the form of case studies woven into the story. For example, the tutorial level incorporates best practices for handling flash drives of unknown origin, as well as the reasoning which explains why such attacks are considered unethical. Interactive dialog prompts between the user and the Station AI reinforce these topics. Ethical aspects of gamification are based on industry best practices such as the IEEE Code of Ethics [14]; note that the development team is well qualified in this area, having earned first place in the 2021 Mid-Hudson IEEE Cybersecurity Ethics Competition. A rubric developed for this competition was adapted to form the basis for ethical decision making within the cybersecurity awareness application. When the user is faced with an ethical decision or case study, they are trained to analyze the case study using a combination of weighting factors that quantify the importance of each element in the user's response, as outlined in table 2.

Table 2: A framework for analysis of ethical case studies with relative weighting factors

Restatement of relevant case study facts or paraphrasing of topical questions	5 points
Identification of stakeholders and ethically significant harms	15 points
Enumeration and prioritization of ethically significant harms based on the ten elements in the IEEE Code of Ethics	30 points

The cybersecurity escape room game was designed using the proven Octalysis framework [15]. This approach to human-centric design and incorporation of gaming elements into non-gaming contexts was introduced in 2012, and the pedagogical benefits have been well documented [16]. For this paper, we provide only a brief overview of this framework. Octalysis organizes a series of eight gamification elements or cognitive drivers into a quantitative scale which can be used to measure an application's level of user engagement and motivation. The framework and brief descriptions of the eight metrics is shown in figure 2, which also indicates how gamification elements are organized into both "white hat" gamification (positive motivators, such as providing the user with a sense of skill mastery, creativity, and higher purpose) and "black hat" gamification (negative motivators, such as fear, uncertainty, greed, or punishment). Further, these elements are organized according to whether they appeal to extrinsic motivations (logic, calculations, and ownership) as opposed to intrinsic motivations (creativity, self-expression, and social context). We note that to make this approach easier to remember, some of the literature on Octalysis uses the symbolic notation of left-brain and right-brain engagement for these categories, although it is acknowledged that these terms don't represent actual cognitive science. A "good" gamification application will utilize one or more of these eight core aspects, which can be weighted according to their level of impact. A balanced game attempts to exploit as many of these motivators as possible, and strives to excel at several of them, in order to produce desired levels of engagement, motivation, and retention among users. Examples have been published previously for online games (such as Farmville or Candy Crush) as well as other platforms that are not considered games but which apply gamification principles (such as Facebook and Twitter) [15].

978-1-6654-8303-2/22/$31.00 ©2022 IEEE

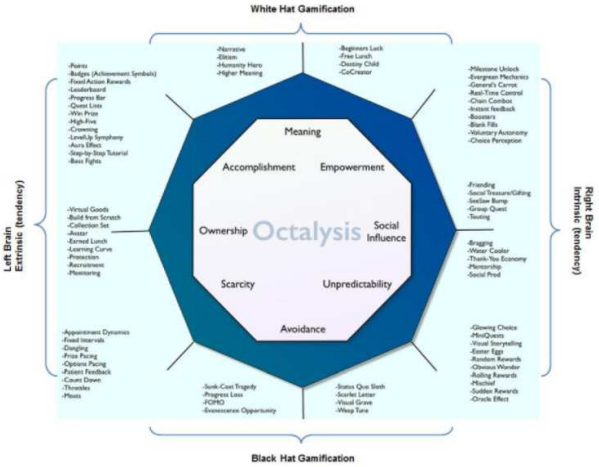

Figure 2: The Octalysis gamification framework [15]

Our application was play tested with a group of 90 pre-college students and 30 college students. Feedback was overwhelmingly positive, and the before/after assessments provided to these groups support that their cybersecurity awareness increased after completing the training. We also used the Octalysis metrics to analyze the cybersecurity awareness virtual escape room game; results are shown in figure 3. These results indicate ARI is a well-balanced game with all but three metrics achieving a score of at least 7.9 out of 10. The first area with a lower score was unpredictability (7.2), which reflects that the application currently has limited replay value. To address this, the next release plans to add more random elements to the mini-games used in each level. The second area with a lower score was social influence (6.8), which reflects that the application currently only allows users to play against the game itself, rather than against other players, and that a leaderboard scoring system with digital badges for different achievement levels has not yet been implemented. The third area with a lower score was ownership (3.2), which reflects the lack of a badge/achievement system as well as other factors such as limited customizability. Since the application is trying to teach fundamental cybersecurity principles, gameplay is a quasi-linear branching tree, rather than an open world; this means the user has limited opportunities to affect the outcome. More significantly, the next release plans to address this issue by incorporating customizable options for ARI, either as part of initial configuration or unlockable cosmetic items. This has been shown to provide an effective way to encourage investment and ownership, as well as encouraging our secondary goal of diversity and outreach to encourage traditionally under-represented groups in the cybersecurity field.

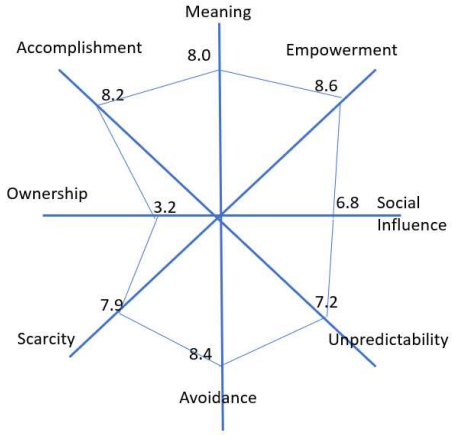

Figure 3: Octalysis analysis of the cybersecurity awareness application

III. Summary and Conclusions

As evidenced by the high number of cybersecurity breaches that can be traced back to user error, there is a need for improved cybersecurity awareness training, particularly in highly vulnerable environments such as colleges and universities. Gamification has been shown to provide improved engagement and retention compared with other approaches, provided that both motivational and developmental methodologies are engaged. We have developed a bottoms-up approach to gamification of cybersecurity awareness training using a first-person perspective application. This application was built in the Unity gaming engine using C# and trains users on fundamental principles including good password practices, multi-factor authentication, cryptography, recognizing social engineering and phishing scams, and defense in depth principles which can be used to mitigate various types of malware. This application was play tested with a group of 90 pre-college students and 30 college students with good results and positive feedback on the design. We quantified application effectiveness using the proven Octalysis framework with eight metrics. Results exceeded a score of 7.9 out of 10 efficiency in all but three areas, which have been identified for additional development to improve their scores during the next development cycle.

References

[1] S. Morgan, "Cybercrime to cost the world over $10.5 Trillion annually by 2025", Cybersecurity Ventures 2020 annual cybercrime report (October 2020), https://cybersecurityventures.com/annual-cybercrime-report-2020/ (last accessed December 8, 2021)

[2] R. Addiscott, C. Mandy, and W. Candrick, Gartner Group report, "Market guide for security awareness computer based training" (July 2021),https://www.gartner.com/doc/reprints?id=126YYDB8Z&ct=210729&st=sb (last accessed December 8, 2021)

[3] Forrester Report, "How to manage human risk in cybersecurity" (September 2021)

[4] Forrester Report, "Best practices: successfully influencing employee cybersecurity behavior" (September 2021) https://reprints2.forrester.com/#/assets/2/2010/RES176219/report (last accessed December 8, 2021)

978-1-6654-8303-2/22/$31.00 ©2022 IEEE

[5] HDI Worldwide Report, "The cybersecurity skills gap: 4 million professionals needed worldwide" (December 2020) https://www.hdi.global/infocenter/insights/2020/cyber-skills-gap/ (last accessed December 8, 2021)

[6] D. Economou, I. Doumanis, F. Pedersen, P. Kathrani, M. Mentzelopoulous, and V. Bouki, "Evaluation of a dynamic role playing platform for simulations based on Octalysis gamification framework", Proc. Workshop of the 11th International Conference on Intelligent Environments, D. Preuveneers, editor (2015)

[7] H. Qusa and J. Tarazi, "A gamification framework for cybersecurity awareness for high school students", Proc. 11th annual IEEE Computing and Communications Workshop and Conference (CCWC), virtual conference (January 27-30, 2020)

[8] G. Jin, M. Tu, T. Kim, J. Heffron, and G. White, "Evaluation of game-based learning in cybersecurity education for high school students", Journ. Education and Learning vol 12, no 1 https://www.researchgate.net/publication/324228918_Evaluation_of_Game-Based_Learning_in_Cybersecurity_Education_for_High_School_Students (last accessed December 8, 2021)

[9] IBM M.U.S.E. Cues cybersecurity game, https://community.ibm.com/community/user/ibmz-and-linuxone/blogs/sneha-kanaujia1/2021/03/30/muse-cues (last accessed December 8, 2021)

[10] Forrester Wave Report: Security Awareness and Training Solutions (first quarter 2021), https://www.knowbe4.com/forrester-wave-security-awareness-training (last accessed December 8, 2021)

[11] A. Soldatov and I. Boregan, *The Red Web*, PublicAffairs Publishing, New York, NY (2015)

[12] Unity Game Development Platform, https://unity.com/solutions/create-games (Last accessed December 8, 2021); see also G. DeVynck, "Unity technologies aims to bring video game tools into the real world", Bloomburg (May 7, 2020) https://www.bloomberg.com/news/articles/2020-05-07/unity-technologies-aims-to-bring-video-game-tools-into-the-real-world (last accessed December 8, 2021)

[13] F. Seraphine, "Ludonarrative dissonance: is storytelling about reaching harmony?" https://www.academia.edu/28205876 (September 2016) (last accessed December 8, 2021)

[14] IEEE Code of Ethics, https://www.ieee.org/about/corporate/governance/p7-8.html (last accessed December 8, 2021)

[15] Y. Chou, "Actionable Gamification: Beyond Points, Bdadges, and Leaderboards", CreatSpace Independent Publishing (2015)

[16] T. Bissell, *Why video games matte*r, Pantheon Books, New York, NY (2010)

978-1-6654-8303-2/22/$31.00 ©2022 IEEE