Teaching and Learning Cybersecurity Awareness with Gamification in Smaller Universities and Colleges

Richard Matovu, Joshua C. Nwokeji, Terry Holmes, Tajmilur Rahman
Computer and Information Science
Gannon University, Erie, PA
{matovu001, nwokeji001, holmes022, rahman007}@gannon.edu

***Abstract*—This research to practice full paper presents our investigation into the use of gamification in teaching cybersecurity awareness to students. Although there are evidences of increasing research activities in cybersecurity, cyberattacks continue to be pervasive. Academic institutions are largely responsible for educating and producing skilled professionals with cybersecurity competences. However, cybersecurity education can be challenging, especially to smaller institutions, usually characterized by meagre resources. In literature, one of the beneficial pedagogical methods for teaching cybersecurity awareness is gamification, which is based on constructivist theoretical framework. While this method has proved very useful, one major challenge is that gamification platforms can be costly to develop and difficult to maintain. This may discourage smaller institutions from using gamification to teach cybersecurity awareness. Freemium gamified platforms e.g., Kahoot! can offer an alternative that is affordable, easy to use and requires very little to no overhead cost. The research questions under investigation are: *what is the impact of gamification (as an instructional method) on students' learning of cybersecurity awareness?*, *which game elements and what aspect of gamification best motivate students?*. Using questionnaire, we asked the students, from a small university in Northwestern Pennsylvania, USA, to rate their knowledge and awareness of cyberattacks. Afterwards, we taught a cyber awareness module with 5 learning objectives to these students using gamification in Kahoot! platform. At the end of the class, we administered another questionnaire to the students and asked them to rate their knowledge and awareness of those same cyberattacks. Our analysis and statistical results show that gamification is an effective technique for knowledge acquisition in cybersecurity awareness. Furthermore, students are mostly motivated by game elements that give them a sense of achievement. Finally we found that students are more interested in the knowledge acquisition aspect of gamification rather than the entertainment and winning aspects. The results of our study may be beneficial for instructional design of introductory cybersecurity awareness courses.**

***Index Terms*—Gamification, Game Elements, Cybersecurity, Cyber Security, Social Engineering**

I. Introduction

The recent burgeoning shift from traditional to online operational models, such as employees working remotely from their homes, students studying online via Zoom, and businesses operating off cloud-based platforms, has significantly increased avenues for cyberthreats leading to a surge in cyberattacks and data breaches. The FBI's Internet Crime Complaint Center released the 2020 Internet Crime report that indicated an increase of more than 300,000 suspected internet crime and reported losses exceeding $4.2 billion [1]. Ransomware attacks were also reported to have increased by 158% in North America between 2019 and 2020, according to The 2021 SonicWall Cyber Threat Report [2]. Taking advantage of the greater exposure of users to cyber risk and the crisis caused by COVID-19 pandemic [1], [3], [4], attackers are increasingly launching more aggressive, severe and sophisticated cyberattacks, such as [5], [6], [7], and [8], targeting critical infrastructure and services.

As cybercrimes are growing exponentially, the shortage of a skilled cybersecurity workforce to protect cyber assets continues to be a lingering problem, as corroborated by numerous reports. For instance, the United States had very low supply of cybersecurity workers with a shortfall of almost 319,720 cybersecurity professionals as of March 2021, according to CyberSeek [9], an initiative funded by the National Initiative for Cybersecurity Education. CyberSeek further noted that on average cybersecurity roles took 21% longer to fill than other IT jobs while Cybersecurity Ventures projected that there would be 3.5 million unfilled cybersecurity jobs globally by 2021 [10].

This dire need of skilled cyber professionals has not only necessitated the teaching of cybersecurity competencies in academic institutions but also created an urgent need for teaching and learning of cybersecurity awareness by computing and non-computing students. Because a considerable number of cyberattacks and data breaches are due to human error and insufficient awareness of cybersecurity concepts as well as lack of knowledge, improving (technical and non-technical) end-user knowledge and cybersecurity awareness have been considered essential steps towards cybersecurity [11]. Focusing on only technical countermeasures isn't fullproof and sufficient enough to protect users and IT infrastructure against cyberattacks and data breaches [11]. It is therefore imperative to teach and learn cybersecurity awareness in universities to both computing and non-computing students.

To effectively teach cybersecurity awareness, instructors have adopted a wide range of pedagogical methods such as flipped classroom [12], project-based learning [13], serious games [14], multimedia tools [11], to mention but a few. Beneficial for increasing learner's engagement, motivation,

and comprehension of complex concepts, gamification is one of the most effective pedagogical methodologies used for teaching cybersecurity awareness [15], [16]. While this method has proved to be very useful and effective, one major challenge is that gamification tools and platforms can be costly (in terms of resources and time) to develop and difficult to maintain. This challenge limits smaller institutions, with very limited resources, to use gamification for teaching cybersecurity awareness concepts.

Free online gamification platforms, on the other hand, offer an alternative that is affordable, easy to learn, quick to deploy and requires very little to no overhead cost. In this paper, we investigate the use of freemium gamified platform in teaching cybersecurity awareness, specifically social engineering attacks and defenses, to computing and non-computing students. We leverage Kahoot![1], a popular online game-based learning platform, to teach cybersecurity awareness, particularly relating to social engineering. Kahoot! incorporates a number of gaming elements, such as leader board, instant rewards, timing, etc., that adds interactivity, increases learner's engagement, and comprehension of the cybersecurity concepts.

For our study, we teach cybersecurity awareness concepts using gamification in Kahoot! platform, in two different class sessions, to students from a small university in Northwestern Pennsylvania, USA. Before each class session, the students rated their knowledge and awareness of 13 cyberattacks and cyberthreats, using a questionnaire. We then taught the students a cyber awareness module, focusing on social engineering (6 specific attacks), with 5 learning objectives using Kahoot!. At the end of the class session, we administered another questionnaire asking the students to rate their knowledge and awareness of the same social engineering attacks and threats, covered in class.

Our analysis and statistical results (using the paired sample t-test) showed that gamification is an effective technique for knowledge acquisition in cybersecurity awareness. Also, our findings show that students are mostly motivated by game elements that give them a sense of achievement and that the students are more interested in the knowledge acquisition aspect of gamification rather than winning/entertainment aspects. These results from our study may be beneficial for instructional design of introductory cybersecurity awareness courses.

A. Research Questions and Study Significance

Gamification is gaining attention in literature and increasing being used by educators across disciplines, especially in STEM areas. Nonetheless, the application of gamification in cybersecurity awareness is currently in the developing stage. Cybersecurity educators agree with the conventional definition of gamification as the use of game elements to spur interest in a non-game context [17], [18]. Various game elements that may be useful within the cybersecurity discipline have been identified by scholars, see Table I for instance. However, it is difficulty to find studies that have validated the usefulness of each of these game elements in motivating students to learn cybersecurity awareness. Currently, it is unclear which game elements is best suited for student engagement and motivation in cybersecurity awareness course.

Furthermore, scholars have proposed various aspect of gamification that can motivate student to learn cybersecurity awareness. These include winning, entertainment, knowledge acquisition, and teamwork. But, we are yet to gain insight into how and which of these aspects best motivate students. For instance, do students engage in gamification to learn or to win or to entertain themselves? Hence, in addition to understanding the impact of gamification on academic performance of cybersecurity awareness students, we also provides insight into the other aspects of gamification that are often neglected. Gaining understanding into these often neglected aspects of gamification has potentials to improve the use of gamification in cybersecurity education. Our research questions therefore include the following:

- **RQ1:** What is the impact of gamification (as an instructional method) on students' learning of cybersecurity awareness?
- **RQ2:** Which game elements best motivate students in cybersecurity awareness class?
- **RQ3:** What aspect of gamification interest students the more e.g., entertainment, winning, gaining knowledge, teamwork?

The rest of this paper is organized as follows: Section II discusses a review of literature and related works about gamification, followed by our research methodology in Section III. We then present and discuss the results of our study in Section IV. Lastly, the limitations, conclusion, and future plan of our work are presented in Section V.

II. Review of Literature

Contemporary educators employ various techniques to motivate and keep learners engaged in classroom, some examples are gamification [18], game-based learning [19], project-based learning [13], flipped classroom [12], persuasive technologies [20], and many others. Among these techniques, gamification and game-based learning (GBL) are increasingly becoming popular and widely used. Although both terms are related, they differ in definition and scope of usage.

A. Gamification, Game-based Learning & Game Elements

Gamification relates to the use of game elements or mechanism (e.g., rewards, collaboration and badges) in a non-game context, while game-based learning are serious games played to support learning process and achieve definite learning objectives [17], [21], [22].

Any game played with the intention to educate and inform, rather than to entertain is called a "serious game", this differs from "non-serious games" which are primarily used for entertainment purposes [23]. In this context, a game is an

[1]Since our study focuses on smaller universities with meagre resources, we signed up and use only the free features of Kahoot!

effort made to achieve goals or resolve conflicts using a set of definite rules [17], [24]. Even though game-based learning and serious games are equally important subjects, the focus of our study is gamification. Hence the rest of this literature review section will focus on gamification.

We found no generally accepted definition of gamification in literature. However, there appears to be a general consensus that gamification involves the use of *game element* or 'mechanism' to arouse game-like experience in a non-game scenario or context [17], [18], [21], [22], [25]. This is easily seen from the definitions of gamification we gathered literature, see Table I. For instance, Plass and Homer [17] define gamification as the use of *game elements* to motivate players to engage in tasks. Similarly, Figueroa-Flores [24] agrees that gamification relates to the use of *game elements* in a non-game context. Although Karagiorgas and Nieman [25] agree that gamification is the use of *game elements* to learn without entertainment. They extended the definition of gamification with the phrase *motivational affordance*. According to their definition, gamification refers to the use of motivational affordances to create gamely experience. The second column in Table I shows that game elements is used consistently to define gamification by various authors in literature.

Many advantages of gamification have been reported in literature, some of these include its positive impact on learners' cognitive, emotional, and social abilities [17]. Gamification positively impacts cognitive abilities by appealing to learners' curiosity, helping them to explore challenges, solve problems and acquire knowledge through inquisition, experimentation and discovery [17]. Likewise, games elements such as collaboration and rewards provides an avenue for peer interaction, team playing, and peer recognition of achievement among learners; thereby helping them to develop their social abilities. Finally, game elements such as lives and missions help learners to acquire emotional character traits such as ability to persist or persevere, which may be useful in learners' career and professional development [17].

Other benefits of gamification reported in literature include its potential to improve student learning, motivate students and make learning more fun [26]. Some scholars have found gamification to support learners' assessment. As reported by Wood et al [18], game elements such as Save Points and Multiple Lives can be combined to provide opportunities for multiple assessment or reassessment of learners performance in an academic activity.

The advantages stated above, together with the various definitions of gamification in Table I, show that game elements are critical to the concept of gamification. The aim of this study is to access the impact of gamification on student performance and to validate the contributions of popular game elements to such impact. To achieve this aim, we identify game elements reported in literature and summarized these in the third column of Table I. We then used these game elements to design our questionnaire.

Definition of Gamification	Game Elements	Ref
Define gamification as the use of game elements to motivate players to engage in tasks they would not find attractive while game-based learning is any game played with defined learning outcomes.	• Game Mechanics • Incentive System • Musical Score • Content & skills • Narrative design	[17]
Defines gamification as "the use of game elements and game design in a non-game context" while game-based learning is the use of video-games to support teaching and learning.	• Points • Badges • Leader boards • Progress boards • Quest • Level • Avatar • Rewards	[24]
No specific definition of gamificati-on and game-based learning but agree that gamification is the use of game elements. Further explains how game elements influences learning	• Rewind • Ghost Image • Save Points • Multiple Lives • Time • Space Control	[18]
Defines gamification as the process of enhancing services by using motivational affordances to arouse gameful experience and advance outcomes in behavior. Gamification is further defined as the use of game elements to learn without entertainment	• Awards • Badges	[25]
Defines gamification as the use of game elements or gaming mechani-sm to motivate learning while game-based learning is the use of games to improve teaching and learning process	• Emblems • Points • Challenges • Leaderboards • Missions	[21]
Defined gamification as using game mechanics in a project or situation	• Badges • Analytics • Progress bars • Points/Score • Lives • 3D Portfolio • Adventure Map • Avatars	[26]
Gamification the applying game elements or mechanism in non-game context while game-based learning is the intentional application of digital or non-digital games/simulation to achieve a defined objective	• Rewards • Leader Board • Badges • Levels • Trophies	[19]
Gamification, the use of game elements in non-game context	• Badges • Leaderboard • Points • Level • Challenges • Avatar	[27]

TABLE I: Definition of Gamification and List of Games Elements

B. Related Work

The use of gamification and game-based learning as instructional approaches in cybersecurity education is receiving a considerable attention in literature. This is seen by the increasing number of publications [14], [28]–[32] in this area. However, the majority of these publications seem to focus on how games or game elements are developed and applied to educational activities. We found limited studies that empirically validate the effectiveness of gamification as an instructional approach for cybersecurity awareness.

Marco Orlando et al [28] developed a computer game known as *Security Empire* which is is intended to help instructors to teach cybersecurity concepts to high school students. One of the reported benefits of this game is the ability to motivate and engage high school students in learning cybersecurity concepts. In a similar study conducted by Jin et al [29], 4 different computer games were developed with the aim of helping high school students to learn cybersecurity concepts. These games were deployed during a summer camp wherein the following cybersecurity concepts were covered: social engineering, security first principles, information security concepts and secure online behaviours. The authors found that game-based learning helped students acquire knowledge cybersecurity concepts covered during the summer camp. Other authors such as Guimaraes et al 2012 [30] and Svabensky et al 2018 [14] have also designed and implemented various serious games and use these to teach cybersecurity classes. In both cases, these authors agree that the use of games as instructional approach has considerable potentials in cybersecurity education.

Studies that perform literature review to synthesize existing applicaiton of game-based learning and gamification are also receiving attention in literature. Among these studies, we found authors that conduct structured literature review to investigate whether games are effective technologies for cybersecurity training [31]. Another structured literature review conducted by Alotaibi et al 2016 [33] conclude that although gaming applications are useful tools in teaching and learning cybersecurity awareness, further studies are required to tailor gaming applications to learners' needs and adequately evaluate how these gaming applications impact students or users. The systematic literature mapping conducted in [34] aims to examine the context and extent to which gamification has been applied to teach software engineering courses. The authors conclude that further empirical studies are needed to evaluate and validate the impact of gamification as a pedagogical approach in software engineering [34].

Indeed, the related studies above make remarkable contributions with respect to the use of gamification, game-based learning and gaming application in education. However, they failed to carry out empirical validation of how gamification impact student performance and learning. This can dissuade instructors from adopting gamification as a learning approach. Empirical validation of the effectiveness of gamification is thus needed to further strengthen and encourage the use of gamification as an alternative teaching and learning technique. Hence, our study complement existing research in gamification by performing an empirical study to validate the impact of gamification on student performance.

III. Research Methodology

A. Research Design

The aim of our study is to assess the effectiveness of gamification in teaching and learning cybersecurity awareness in smaller universities and colleges. We specifically focused on social engineering aspect of cybersecurity because our study targets learners with little to no prior knowledge about cybersecurity, and numerous studies (e.g., [35], [36]) have shown that human beings are often the weakest link in the security chain. Social engineering attacks involve manipulating human weakness for malicious gain [36], such as, divulging sensitive information from an individual through social interaction. In our study, we covered popular techniques employed by adversaries to conduct social engineering attacks, namely phishing, spear-phishing, vishing, smishing, baiting, and tailgating.

The design of our study was in three-folds: (1) designing a course unit with specific learning objectives, (2) implementing or teaching the course unit with a gamified tool that requires little to no overhead to the instructor, and (3) assessing learners' acquired knowledge using surveys.

1) Course Unit and its Learning Objectives::

To contextualize our gamification approach as a pedagogical strategy, we began by designing a course module/unit with specific learning objectives. Essential for aiding effective student learning and design of instruction materials [37], these learning objectives guided the concepts covered in our course unit, and helped in designing our course materials and gamified activities. This ensured that our study sufficiently covered the essential elements of social engineering in line with our study goals. Below are the learning objectives we designed for our course module in this study, that can easily be adapted into undergraduate courses at freshmen or sophomore level.

- *Define and identify common social engineering techniques used by attackers.*
- *Understand and describe the various social engineering techniques used by adversaries.*
- *Apply basic cyber awareness knowledge to identify and detect common social engineering threats/attacks.*
- *Analyze common scenarios and identify the kind of social engineering attacks.*
- *Apply countermeasures to mitigate these attacks/threats.*

These lesson objectives were modeled based on Bloom level taxonomy [38], a popularly renown framework for classifying educational objectives. Since our target students are fairly new to the concepts with little or no prior formal cybersecurity education, we focused on Bloom level 1, 2, and 3. Achieving these objectives would help students identify, analyze, and counter social engineering baits, critical skills that have been underscored by numerous studies as needed for curtailing the surging cyberthreats and attacks from the non-technical perspective. The course unit can be delivered structure as two 60-minute or one 80-minute class lecture. In our study, we delivered it as two separate 80-minute class lecture, allowing us to obtain various diverse views about our study.

2) Our Gamification Approach Leveraging Kahoot!:

As discussed in Section II-A, gamification is one of the recent pedagogical technique used by educators to motivate and keep learners engaged. Employing gamification, however, requires a significant time and amount of work by instructors to design and incorporate them into their courses. This can be challenging in smaller universities.

To minimize the cost and amount of time required for developing and incorporating the serious game or gamified activities, we retained the traditional teaching method used by most instructors, of slides, images, and videos. In addition, we incorporated gamified activities using Kahoot! during the teaching session. Kahoot! [39] is a popular online game-based learning platform, that is easy to use. It has two (free and paid) editions and a wide range of gaming elements. Since our study targets institutions with meagre resources, we focused on integrating the free edition of Kahoot! to our course.

To this end, we designed a Kahoot! game consists of four major sessions covering general social engineering, identifying social engineering attacks, countermeasures against those attacks. The gamified activities employed leaderboards, instant reward, badges, timed component as the game elements to motivate and keep the students engaged. Please refer to Section II-A for more details about these and more game elements used in gamification. Our lecture sessions consisted of short presentation slides that were used by the instructor to introduce the students to different concepts followed by game sessions. Students played the gamified activities using their phones, and weren't required to know or have used any gamification technology before.

3) Survey Design: To assess the impact of our pedagogical strategy i.e., gamification leveraging Kahoot!, we designed two (pre-test and post-test) surveys to collect quantitative and qualitative data from our participants. Surveys are research tools that are widely used for collecting information to describe, compare, or explain subjects' knowledge [40]. In our study, participants took a pre-test and post-test survey to rate their knowledge about cybersecurity awareness concepts covered in our lecture sessions. For both surveys, participants rated their knowledge using a 5-point Likert scale, with 5 representing *Very Knowledge* and 1 representing *Not Knowledgeable*.

The pre-test survey included questions on general demographic information (excluding personal identification) and rating knowledge on social engineering, phishing, spear-phishing, vishing, smishing, baiting, tailgating, malware, viruses, cyberbullying, cyberstalking, identity theft, and worms. On the other hand, the post-test survey focused on rating knowledge on social engineering concepts only. The post-test survey also included the rating and open-ended questions on gamification to assess the impact of our approach, as follows:

- *SQ1*: Gamification (Kahoot!) motivated you to learn more about the cybersecurity concept.
- *SQ2*: I learned better using gamification (Kahoot) than the traditional way of teaching.
- *SQ3*: Rank the following gamified elements in Kahoot! according how they motivated you to learn more (1 for least helpful and 4 for most helpful)?
  - Leader board *(Ranking scores after every question).*
  - Instant Reward *(Receiving reward after a question).*
  - Badges *(Displaying name at the end of each session).*
  - Time *(Answering questions within a limited time).*
- *SQ4*: Rank the following items according to how Kahoot! motivated you to do them (1 for lowest and 4 for highest): *Understanding the purpose of the concepts (SQ4a), Learning with others (SQ4b), Mastering the concepts (SQ4c), Winning (SQ4d).*
- *SQ5*: Would you recommend using gamification (Kahoot!) in other courses?
- *SQ6*: What was it that you like most about gamification?
- *SQ7*: What was it that you dislike about gamification?

B. Data Collection

We collected data from thirty eight (22 male, and 16 female) participants. Prior to our data collection, we sought Institutional Review Board (IRB) approval, and all approved IRB guidelines were followed during our study. All the participants in our study were students from two (2) courses. Both courses are offered in the College of Engineering and Business at a small university in Northwestern Pennsylvania (US). The data was collected from one class lecture session of each of these two courses. At the beginning of the class session, students were informed about the study and that their participation wasn't compulsory. The students then filled out the pre-test survey, followed by our study experiment. At the end of our lecture, the students again filled out the post-test survey.

The pre-test and post-test surveys were designed and conducted using Survey Monkey. Students provided informed consent for participating in the surveys. During the data collection, the student names weren't recorded to avoid identifying them. However, student's response from the pre-test and post-test surveys were matched using the unique IP addresses for our statistical analysis.

C. Data Analysis

To analyze our collected data, we adopted the sequential explanatory design method — a highly popular mixed research approach for collecting and analyzing data [41], [42]. This method starts with analysis of the quantitative data followed by a qualitative phase. The qualitative phase helps to explain or elaborate the results from the quantitative data [41].

In our study, the quantitative data is primarily about students' perceptions about cybersecurity awareness concepts and gamification. We used this data for our plots and descriptive analysis of our students' knowledge about various cybersecurity concepts. We also assessed the students' knowledge acquired through our gamification approach by comparing the students' ratings before and after our study. To determine the statistically significance of the observed differences, we performed various one-sided paired sample t-tests at a level of significance, $\alpha = 0.05$. Our general hypothesis is that students are more knowledgeable about social engineering and its specific attacks after our study than before.

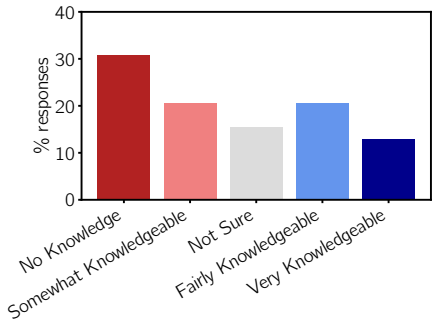
All our data analysis was done using popular Python packages, including Pandas, SciPy. Prior to our analysis, we computed the *Cronbach's alpha* [43] coefficient to test the reliability of the instrument we used for data collection. In our study, the cronbach's alpha for the 5 item scale was *.915* and *.973* for the pre-test and post-test surveys respectively,

indicating a high degree of reliability and consistency. We then proceed to our quantitative and qualitative analysis.

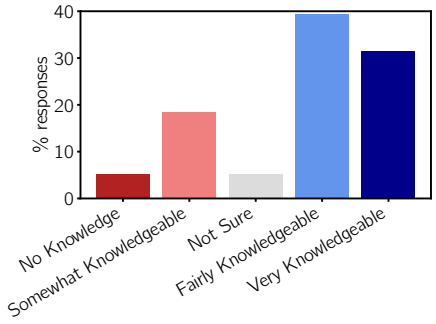
IV. Results and Discussion

In this section, we present and discuss both the quantitative and qualitative results of our study.

A. Students' Knowledge Before And After Our Study



(a) Pre-test ratings.



(b) Post-test ratings.

Fig. 1: Pre-test and post-test responses of students' knowledge about social engineering, in general.

Figure 1a presents the pre-test while Figure 1b shows post-test results for the overall students' perceptions of social engineering, in general. During the pre-test, as shown in the Figure 1a, half (50%) of the students rated their knowledge about social engineering in the *No Knowledge* and *Somewhat Knowledge* category, and about 32% of the students rated themselves as fairly and very knowledgeable about general social engineering. On the other hand, the post-test results in Figure 1b shows that most students rated themselves as knowledgeable about social engineering. Over 70% of the students felt that they were fairly and very knowledgeable, and only 23% were in the No and Somewhat Knowledgeable category. Comparing the students' ratings in Figures 1a and 1b, there was a considerable improvement in the knowledge of students about social engineering, before and after our study.

In Figures 2 and 3, we delve into students' perceptions of the specific attacks used in social engineering. Similar to the results in Figure 1, Figure 2 shows that most students weren't knowledgeable about vast majority of different social engineering attacks before the study. Notably among these

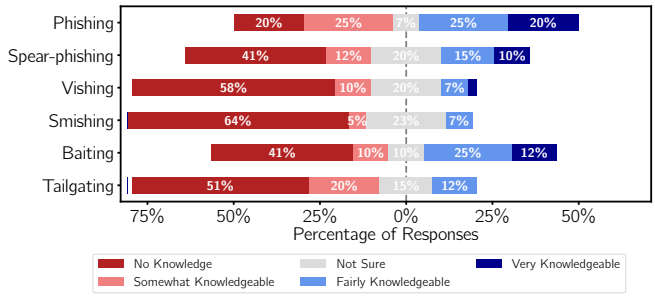


Fig. 2: Pre-test ratings of students' knowledge about the specific social engineering attacks.

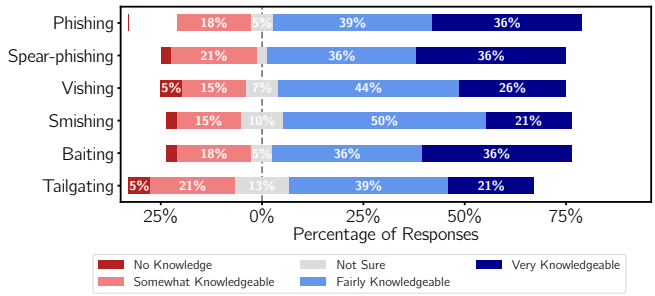


Fig. 3: Post-test ratings of students' knowledge about the specific social engineering attacks.

were the smishing and vishing attacks that 64% and 58% respectively of the students indicated they had no knowledge about. Smishing and vishing are social engineering attacks that use SMS and voice respectively. Surprisingly, these attacks are very popular, especially in this era of mobile phones, yet many students had no knowledge about them. This emphasizes the need of cybersecurity awareness studies, such as ours.

Figure 3 presents the post-test ratings about the specific social engineering attacks. The vast majority of the students' knowledge in each of the social engineering attack had improved, with between 36% - 50% of the students rating themselves as fairly knowledgeable, and between 21% - 36% rating themselves as very knowledgeable. Again, there was a considerable improvement in the students' knowledge. The majority of the students rated themselves fairly and very knowledgeable in each of the specific social engineering attacks.

Overall, the results in Figures 1, 2, and 3 indicate that there was considerable improvement in the knowledge of students about social engineering and the specific social engineering attacks. The results shows a major positive shift in students' perception of their cybersecurity awareness from "*No Knowledge/Somewhat Knowledgeable/Not Sure*" (the low side) to "*Fairly Knowledgeable/Very Knowledgeable*" (the high side) as illustrated in Figures 2 and 3. Moreover, these improvements or positive shift happened in one class of 80 minutes duration. For instance, Phishing and Spear-phishing Pre-test ratings of "Not Sure" to "No Knowledge" were 46% and 73%, respectively. Their post-test ratings for "Fairly" and "Very

Attack Type	$t-statistic$	$p-value$
Phishing	-3.8319	0.0002
Spear-Phishing	-5.1189	0.0000
Vishing	-7.2942	0.0000
Smishing	-7.9701	0.0000
Baiting	-4.3237	0.0001
Tailgating	-6.1016	0.0000

TABLE II: Results of our statistical tests about the different types of social engineering attacks.

Knowledgeable" became 75% and 72%, respectively.

B. Statistical Analysis Of Our Results And Their Significance

The results in the previous subsection indicated a considerable improvement in the students' knowledge about social engineering in general, and about the specific social engineering attacks. To determine the statistically significance of the observed improvement, we performed statistical testing using paired samples t-test at a level of significance of $\alpha = 0.05$.

The paired samples t-test indicated that the difference in students' perceptions regarding social engineering, in general, was statistically significant with $t(37) = -3.6181$, $p = 0.0004$. This implies that our gamification approach (Kahoot!) significantly improved their knowledge in social engineering, according to the student ratings. Table II presents the rest of the results for the paired samples t-test performed about the specific social engineering attacks. All the p-values obtained from the paired samples t-test for each of the social engineering attack was below 0.05, as seen in Table II. These results indicate that there was a statistically significant improvement in the knowledge of the students for each of the attack. By implication, gamification (Kahoot!) improves the students awareness of social engineering attacks.

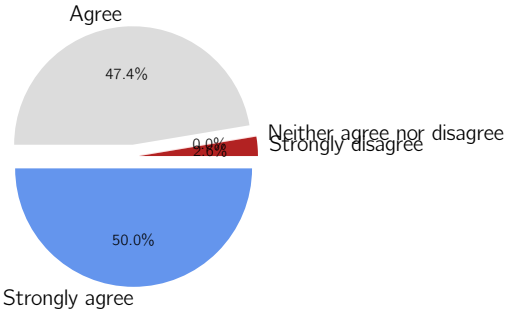


Fig. 4: Students' responses on whether gamification motivated them to learn more about cybersecurity.

C. Students' Perceptions About Our Gamification Approach

To gain more insights about students' perceptions of our gamification approach as a teaching pedagogy, we asked three specific questions (i.e., SQ1, SQ2, and SQ5), about our gamification approach.

Figure 4 shows the student's ratings, on a 5-likert scale, on how gamification motivated them to learn more about cybersecurity concepts. Over 97% of the students agreed (strongly agree and agree) that the gamified activities in our study motivated them to learn the cybersecurity concepts being taught. Only 2.6% strongly disagreed with the notion that they were motivated by the Kahoot! games.

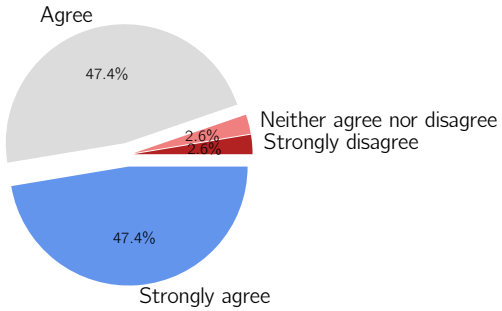


Fig. 5: Students' responses of whether Gamification (Kahoot!) is better than traditional teaching style.

Figure 5 shows the students' responses in regards to whether gamification (Kahoot!) is better than the traditional method of teaching. The majority i.e., over 94%, of the students agreed (strongly agree and agree) that gamification was better than the traditional style of teaching. Only 2.6% strongly disagree with this notion, and another 2.6% neither agreed nor disagreed.

All the students, with the exception of only one student, in our study indicated that they would recommend using gamification (Kahoot!) in teaching other courses. Overall, our results, thus far, imply that the vast majority of the students were motivated and preferred the gamification approach of teaching. Hence, introductory cybersecurity awareness courses can benefit from this pedagogical style of teaching.

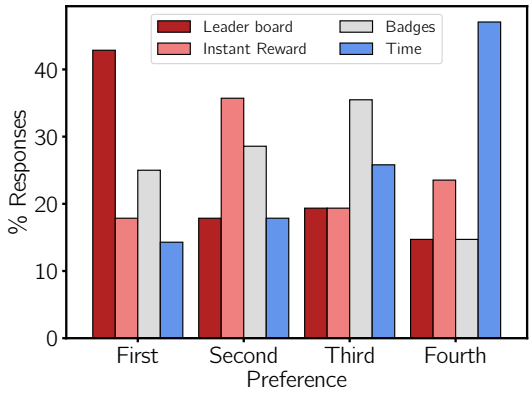


Fig. 6: Rankings of game elements that motivated students.

D. Students' Preference on Motivating Game Elements And Aspects of Gamification That Motivated Them

To further understand the students' preference on which game elements motivated them the most and which aspects of gamification most motivated them, we plotted their rankings (first to fourth) based on responses from Question *SQ3* and *SQ4*. Figure 6 summarizes the students' rankings of game elements used in our study, in regards to motivating them

to learn more. The students ranked leader board as the most preferred game element with 42%, as shown in Figure 6. Instant reward was the second preferred game element with 35%, followed by badges with 35%. Timing was ranked the least preferred game element followed by badges. These results, in Figure 6, indicate that the most motivating game elements were those that gave students a sense of achievement.

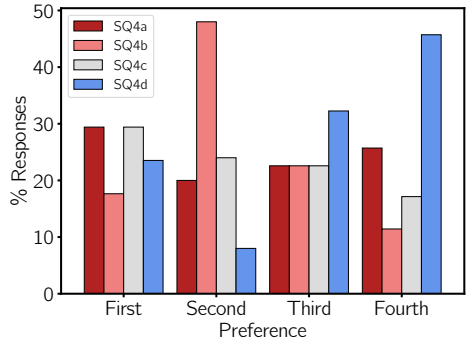


Fig. 7: Rankings of the aspects of gamification that best motivated students.

Figure 7 shows the students' rankings of the different aspects of gamification that motivated them the most. SQ4a (*Understanding the purpose of the concepts*) and SQ4c (*Mastering the concepts*) were ranked the most motivated with 29.4% each, while winning was ranked third. These results imply that the students were more interested in knowledge acquisition aspect of gamification than other non-educational aspects like winning, entertainment, etc.

E. Qualitative Feedback

Our last two survey questions were open-ended questions about what students liked and disliked about our gamification approach. These acted as the source of our qualitative data, giving us more insights into students' perceptions and preferences above. In general, the students' likes about gamification were overwhelming positive and in line with other previous studies fronting gamification. The majority of the likes centered around gamification providing fun and interactive method of learning, and the competition among students encouraged them to learn more. Below, we provide a selected sample of the notable responses we received.

- *Mastering the knowledge and timed component as well as understanding the purpose of the class.*
- *Its an interesting application which gives kind of interest to gain quick knowledge and keep pace with time.*
- *Competition among students*
- *It's modern and fun to learn*
- *I like the way Kahoot! testifies. It's fun and enjoy and very helpful for learning.*
- *I am competitive, so it encouraged me learn the most so I could win.*

While some students liked enjoyed thinking within a short amount of time, the majority of dislikes centered around time. Not surprisingly, this directly supports our findings in Figure 6 where students rated the timing component as the least motivating factor. Another notable dislike worth noting was from two students (included in the list below) who didn't like the competition among others, that is introduced by gamification. Based on this dislike, as instructors leveraging this pedagogical style, attention and focus needs to be paid to optimize the competition that could affect some students. Again, we list some of the notable dislikes from the students below.

- *The time in some question was short*
- *Its not about winning its all about gaining the knowledge*
- *Confusion on multiple answer questions*
- *If you mess up a lot you fall behind fast*
- *I don't like that it makes students who aren't fast readers/learn fast are embarrassed in front of the whole class.*

V. Conclusion, Limitation and Future Work

There are evidences that the use gamification as an instructional approach offers various advantages, including enhanced engagement, improved academic performance and enhance knowledge of subject matter. However, the use of gamification in cybersecurity awareness is still developing. The few instance where of gamification was used to teach cybsersecurity awareness, are in large universities and colleges with resources that are often not available in smaller institutions. Our aim in conducting this research is to examine how gamification can be used to teach cybersecurity awareness in smaller universities and colleges. To achieve this aim, we conducted an empirical study in a small liberal college university in Northern Pennsylvania.

Our results show that gamification is equally an effective pedagogical approach for teaching cybersecurity awareness in smaller institutions. Affordable, easy to use and available gamification tools such as Kahoot are efficient in the delivery key learning objectives in cybersecurity awareness. We also found that game elements that give sense of achievement e.g., leader board and instant rewards, motivate and engage students more than the others. On the other hand, students dislike game elements like time that tend to put them under pressure. Among the various aspects of gamification *(e.g., knowledge acquisition, winning, entertainment)* that are attractive, students appear to be more interested in knowledge acquisition than other aspects.

While these findings may be useful to instructors, academic programs and institutions that are already using or planning to adopt gamification in cybersecurity course. It is important to note various factors that may threaten the ability to generalize these results. One of these is the sample size used in our study. The number of students that participated in our study (n=38) are relatively small. Secondly, the data collection is based on students' perception, which can affect the results, since perceptions may vary depending on prevailing factors such as previous knowledge and exposure to gamification and cybersecurity awareness.

Our future plan is to design a robust experiment that may address the limitations above. We plan to increase the sample size used to ensure that our future study is more generalizable. Secondly, we are interested in conducting a more rigorous statistical analysis to determine the exact impact of each game elements on student motivation, engagement, and academic performance.

REFERENCES

[1] FBI. 2020 IC3 Report. btxdoc.pdf. Last accessed in July, 2021. [Online]. Available: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

[2] SonicWall, "2021 sonicwall cyber threat report," https://www.sonicwall.com/2021-cyber-threat-report/, last accessed in May, 2022.

[3] Deloitte, "Impact of covid-19 on cybersecurity," https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html, last accessed in May, 2022.

[4] Microsoft, "Exploiting a crisis: How cybercriminals behaved during the outbreak," https://www.microsoft.com/security/blog/2020/06/16/exploiting-a-crisis-how-cybercriminals-behaved-during-the-outbreak/, last accessed in May, 2022.

[5] CNBC, "Twitter hackers who targeted elon musk and others received $121,000 in bitcoin, analysis shows," https://www.cnbc.com/2020/07/16/twitter-hackers-made-121000-in-bitcoin-analysis-shows.html, last accessed in May, 2022.

[6] Reuters, "Solarwinds hack was 'largest and most sophisticated attack' ever: Microsoft president," https://www.reuters.com/article/us-cyber-solarwinds-microsoft/solarwinds-hack-was-largest-and-most-sophisticated-attack-ever-microsoft-president-idUSKBN2AF03R, last accessed in May, 2022.

[7] N. Times, "Pipeline attack yields urgent lessons about u.s. cybersecurity," https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html, last accessed in May, 2022.

[8] C. News, "Jbs paid $11 million ransom after cyberattack," https://www.cbsnews.com/news/jbs-ransom-11-million/, last accessed in May, 2022.

[9] CyberSeek. Cybersecurity supply/demand heat map. Last accessed in May, 2022. [Online]. Available: https://www.cyberseek.org/heatmap.html

[10] C. Ventures, "Cybersecurity talent crunch to create 3.5 million unfilled jobs globally by 2021," https://cybersecurityventures.com/jobs/, last accessed in May, 2022.

[11] L. Zhang-Kennedy and S. Chiasson, "A systematic review of multimedia tools for cybersecurity awareness and education," *ACM Computing Surveys (CSUR)*, vol. 54, no. 1, pp. 1–39, 2021.

[12] J. C. Nwokeji, R. Stachel, and T. Holmes, "Effect of instructional methods on student performance in flipped classroom," in *2019 IEEE Frontiers in Education Conference (FIE)*. IEEE, 2019, pp. 1–9.

[13] J. C. Nwokeji and P. S. T. Frezza, "Cross-course project-based learning in requirements engineering: An eight-year retrospective," in *2017 IEEE Frontiers in Education Conference (FIE)*. IEEE, 2017, pp. 1–9.

[14] V. Švábenskỳ, J. Vykopal, M. Cermak, and M. Laštovička, "Enhancing cybersecurity skills by creating serious games," in *Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education*, 2018, pp. 194–199.

[15] J. C. Nwokeji, R. Matovu, and B. Rawal, "The use of gamification to teach cybersecurity awareness in information systems," 2020.

[16] Z. C. Schreuders and E. Butterfield, "Gamification for teaching and learning computer security in higher education," in *2016 {USENIX} Workshop on Advances in Security Education ({ASE} 16)*, 2016.

[17] J. L. Plass, B. D. Homer, and C. K. Kinzer, "Foundations of game-based learning," *Educational Psychologist*, vol. 50, no. 4, pp. 258–283, 2015.

[18] L. Wood, H. Teras, T. Reiners, and S. Gregory, "The role of gamification and game-based learning in authentic assessment within virtual environments," *Research and development in higher education: The place of learning and teaching*, pp. 514–523, 2013.

[19] B. E. Wiggins, "An overview and study on the use of games, simulations, and gamification in higher education," *International Journal of Game-Based Learning (IJGBL)*, vol. 6, no. 1, pp. 18–29, 2016.

[20] A. M. Abdullahi, R. Orji, and J. C. Nwokeji, "Personalizing persuasive educational technologies to learners' cognitive ability," in *2018 IEEE Frontiers in Education Conference (FIE)*. IEEE, 2018, pp. 1–9.

[21] E. Junior, A. C. B. Reis, A. M. Mariano, L. B. Barros, D. de Almeida Moysés, and C. M. A. da Silva, "Systematic literature review of gamification and game-based learning in the context of problem and project based learning approaches," in *11th International Symposium on Project Approaches in Engineering Education (PAEE) 16th Active Learning in Engineering Education Workshop (ALE)*, 2019.

[22] E. Çeker and F. Özdaml, "What "gamification" is and what it's not." *European Journal of Contemporary Education*, vol. 6, no. 2, 2017.

[23] T. C. Clapper, "Serious games are not all serious," pp. 375–377, 2018.

[24] J. F. Figueroa-Flores, "Gamification and game-based learning: Two strategies for the 21st century learner," *World*, vol. 3, no. 2, 2016.

[25] D. N. Karagiorgas and S. Niemann, "Gamification and game-based learning," *Journal of Educational Technology Systems*, 2017.

[26] S. Villagrasa, D. Fonseca, E. Redondo, and J. Duran, "Teaching case of gamification and visual technologies for education," *Journal of Cases on Information Technology (JCIT)*, vol. 16, no. 4, pp. 38–57, 2014.

[27] M. E. Ortiz Rojas, K. Chiluiza, and M. Valcke, "Gamification and learning performance: A systematic review of the literature," in *11th European Conference on Game-Based Learning (ECGBL)*. ACAD CONFERENCES LTD, 2017, pp. 515–522.

[28] M. Olano, A. Sherman, L. Oliva, R. Cox, D. Firestone, O. Kubik, M. Patil, J. Seymour, I. Sohn, and D. Thomas, "{SecurityEmpire}: Development and evaluation of a digital game to promote cybersecurity education," in *2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14)*, 2014.

[29] G. Jin, M. Tu, T.-H. Kim, J. Heffron, and J. White, "Game based cybersecurity training for high school students," in *Proceedings of the 49th ACM Technical Symposium on Computer Science Education*, 2018.

[30] M. A. Guimaraes, H. Said, and R. Austin, "Experience with video games for security," *Journal of Computing Sciences in Colleges*, vol. 27, no. 3, pp. 95–104, 2012.

[31] M. Hendrix, A. Al-Sherbaz, and B. Victoria, "Game based cyber security training: are serious games suitable for cyber security training?" *International Journal of Serious Games*, vol. 3, no. 1, 2016.

[32] R. Kerestes, R. Clark, and Z. Wu, "Enhanced student engagement through teamwork, gamification, and diversity & inclusion best practices in an electromagnetics course," in *2021 IEEE Frontiers in Education Conference (FIE)*. IEEE, 2021, pp. 1–6.

[33] F. Alotaibi, S. Furnell, I. Stengel, and M. Papadaki, "A review of using gaming technology for cyber-security awareness," *Int. J. Inf. Secur. Res.(IJISR)*, vol. 6, no. 2, pp. 660–666, 2016.

[34] M. M. Alhammad and A. M. Moreno, "Gamification in software engineering education: A systematic mapping," *Journal of Systems and Software*, vol. 141, pp. 131–150, 2018.

[35] F. Mouton, L. Leenen, and H. S. Venter, "Social engineering attack examples, templates and scenarios," *Computers & Security*, 2016.

[36] F. Mouton, L. Leenen, M. M. Malan, and H. Venter, "Towards an ontological model defining the social engineering domain," in *IFIP International Conference on Human Choice and Computers*. Springer, 2014, pp. 266–279.

[37] N. E. Gronlund, *How to write and use instructional objectives*. Simon & Schuster Books for Young Readers, 1995.

[38] D. R. Krathwohl, "A revision of bloom's taxonomy: An overview," *Theory into practice*, vol. 41, no. 4, pp. 212–218, 2002.

[39] Kahoot. Kahoot! — learning games — make learning awesome! https://kahoot.com/. Last accessed in March, 2022.

[40] S. L. Pfleeger and B. A. Kitchenham, "Principles of survey research: part 1: turning lemons into lemonade," *ACM SIGSOFT Software Engineering Notes*, vol. 26, no. 6, pp. 16–18, 2001.

[41] N. V. Ivankova, J. W. Creswell, and S. L. Stick, "Using mixed-methods sequential explanatory design: From theory to practice," *Field methods*, vol. 18, no. 1, pp. 3–20, 2006.

[42] J. W. Creswell, V. L. Plano Clark, M. L. Gutmann, and W. E. Hanson, "Advanced mixed methods research designs," *Handbook of mixed methods in social and behavioral research*, vol. 209, pp. 209–240, 2003.

[43] J. M. Bland and D. G. Altman, "Statistics notes: Cronbach's alpha," *Bmj*, vol. 314, no. 7080, p. 572, 1997.