Aug 10th, 12:00 AM

The Impact of Gamification on Students' Learning Outcome and Career Interest in Cybersecurity Education

Chen Zhong
The University of Tampa, czhong@ut.edu

J.B. (Joo Baek) Kim
The University of Tampa, jkim@ut.edu

Hong Liu
Indiana University Kokomo, hlius@iu.edu

The Impact of Gamification on Students' Learning Outcome and Career Interest in Cybersecurity Education

Emergent Research Forum (ERF)

Chen Zhong
ITM Department, Sykes College of Business, University of Tampa
czhong@ut.edu

J.B. Kim
ITM Department, Sykes College of Business, University of Tampa
jkim@ut.edu

Hong Liu
School of Sciences,
Indiana University Kokomo
hlius@iu.edu

Abstract

Effective cybersecurity education is a critical domain in addressing the shortage of the cybersecurity workforce. To prepare students for real-world workforce challenges, hands-on practice is an important component in cybersecurity education. We integrated gamification into hands-on cybersecurity practice and conducted an empirical study on how gamification impacts students' learning outcome and career interests. Questionnaire data have been collected and will be analyzed to test our hypotheses. The expected results will address the impact of gamification on learning outcomes and suggest how gamification can be most effectively applied to cybersecurity education.

Keywords

Gamification, cybersecurity education, career interest.

Introduction

The 2021 (ISC)² Cybersecurity Workforce Study reported 2.72 million unfilled cybersecurity jobs ("A Resilient Cybersecurity Profession Charts", 2021). To address the shortage of workers in cybersecurity, effective cybersecurity education in universities is a key area. Multiple prior research (e.g., Anderson & Romney, 2014; Vigna, 2003) suggested that cybersecurity education needs to be grounded in hands-on practice to prepare students with knowledge and skills to address real-world challenges. Gamification is extensively used in competitions which is a common recruitment method to attract students into cybersecurity careers. However, few studies have evaluated the impact of gamification on students' learning outcome and career interest in classroom settings. We believe it is worthwhile to fill the gap of knowledge of the gamified cybersecurity learning process related to students' career interest. Therefore, accurate analysis of the impact of gamification in cybersecurity education is critical to guide educators on using gamification effectively in cybersecurity courses. This study integrates gamification into hands-on cybersecurity labs and evaluates the impact of gamification on students' learning outcome and career interests. The objectives of the research-in-progress include (1) to assess the relationship among gamified lab challenges, students' intrinsic and extrinsic motivation, learning outcome, and career interest, and (2) to suggest how gamification can be most effectively applied in cybersecurity courses.

The paper begins with a literature review in the related fields followed by a description of the research model, and the data collection method. We also provide a plan to analyze the data and describe the expected results.

Theoretical Background

Gamification in cybersecurity education

Using game elements, such as competition, instant feedback, interaction, etc., in non-entertaining contexts, which is known as gamification (Deterding, et al., 2011), has recently been gaining attention in higher education and business training. Gamification is considered an appropriate method to teach young generations various skills as they are familiar with games and seek fun when learning (Donovan & Lead, 2012). Cybersecurity is a developing field in which gamification can be used to engage learners and improve the learning experience. Students are expected to pay greater attention and be more motivated in the learning process in gamified cybersecurity lab exercises (Demmese et al., 2020). It is also expected to enhance the effectiveness and efficiency of educating students and training workforces by applying gamification in the cybersecurity field (Wolfenden, 2019; Karagiannis & Magkos, 2021; Coenraad et al., 2020; Beuran et al., 2016).

Motivation theory

Motivation, as a critical component of the learning process, is important in educational theories. Studies have shown that motivations are closely related to academic achievement (Lepper et al., 2005). Motivating students to enjoy studying and participate in the learning process is the key to obtaining good learning outcomes. According to self-determination theory (SDT; Deci & Ryan, 1985; Ryan & Deci, 2000), persons tend to behave in line with their wants and fulfillment of those needs. In that sense, the learner's desire to seek psychological self-growth, changed by educational contexts, may impact the learning process. According to SDT, intrinsic motivation and extrinsic motivation are the two primary forms of motivation (Deci & Ryan, 1985). Extrinsic motivation relates to doing something because of a separate consequence, whereas intrinsic motivation refers to doing something because of an innate interest or satisfaction (Ryan & Deci, 2000).

Theory of career interest

Career interest is a critical factor that drives learners to gain an understanding of the opportunities and requirements in the cybersecurity field. Career exploration has been described as a lifelong process of professional learning and development, a continuous process rather than a static state with a definite endpoint (Blustein, 1997). Previous research found that interests, self-efficacy expectations, and stable dispositional tendencies are three key factors that influence people's career choices (Lent et al., 1994). It is important to understand whether and how personal characteristics and circumstances affect career interests. The existing career theory was supported by the findings of the study of participants from the National Cyber League competition that participating in the competition mainly increased the interests of the participants who were already skilled in cybersecurity tasks (Tobey et al., 2014). Another study also found an individual's background knowledge of cybersecurity is a critical factor that makes it difficult to maintain interest after the competitions, especially in the competitions with high knowledge barriers (Cheung et al., 2012). In addition to an individual's background knowledge, a comprehensive study of the profile of cybersecurity competition participants shows that the individuals with high perceived self-efficacy in cybersecurity tasks, rational decision-making style, and investigative interests were more likely to take a cybersecurity career after the competition (Bashir et al., 2017).

Hypothesis Development

After reviewing the past literature and theoretical frameworks mentioned in the previous section, we propose a research model that incorporates the significant elements of students' learning process through gamified cybersecurity labs. More details of the proposed model and its hypotheses are described as follows:

An appropriate amount of challenge in the cybersecurity labs positively affects intrinsic motivation. It is well known that human beings will pursue an activity through which they can develop competence and a feeling of efficacy. Flow theory (Csikszentmihalyi, 1990) also emphasizes the appropriate level of challenge

is essential for people to be immersed in an activity. Learners feel an activity is trivial when it is too easy, whereas they feel frustrated when they do activities that are too difficult. In the gamified cybersecurity labs, learners can be intrinsically motivated which is accompanied by a feeling of accomplishment by overcoming embedded challenges. Hence, a learner will likely feel motivated when engaged with a gamified activity if the game incorporates an appropriate level of challenge that contains an uncertain outcome.

> H1: Appropriate amount of challenge will positively affect learners' intrinsic motivation in gamified cybersecurity labs.

Previous studies claimed that learners' situational interests (immediate affective response to activity) can lead to the development of individual interests, that is increase their intrinsic desire and inclination to engage in specific topics and activities (Hidi & Renninger, 2006). Druckman (1995) concluded that games are effective in enhancing motivation and increasing student interest in the subject matter. In addition, previous research has found that career exploration is a dynamic process throughout the lifespan, rather than a static state with a definite endpoint (Blustein, 1997). Therefore, we expect that well-designed gamified labs will increase students' intrinsic motivation, thereby increasing their interest and confidence in cybersecurity, and thus have a positive effect on increasing career interest.

> H2: Intrinsic motivation will positively affect learners' career interest after completing gamified cybersecurity labs.

It is generally considered that high motivation generally yields better performance. Previous literature suggests that there is a significant connection between intrinsic motivation and performance (Tauer & Harackiewicz, 2004). When people are intrinsically motivated, they focus on the task by which they earn better skills to produce a favorable performance level. Therefore, intrinsic motivation is considered an important locus for performance, especially in the long term (Tauer & Harackiewicz, 2004). Thus, in the game-based learning process, intrinsic motivation will be positively related to the learners' game performance.

> H3: Intrinsic motivation will positively affect learners' game performance in gamified cybersecurity labs.

Although it is known that the degree of influence of extrinsic motivation on performance is relatively less than intrinsic motivation (Harackiewicz et al., 2002;), extrinsic motivation still plays a role in learning to some degree (Lin et al., 2001). Extrinsic motivation, such as recognition by peers, better grades, etc. in the college classroom can help students keep attentive to the task and focus. Especially in gamified cybersecurity labs, most tasks require learners to manage a substantial amount of time spent on the tasks, which could be harder to achieve without being highly motivated by external rewards than only by internal motivation. Thus, we hypothesize that extrinsic motivation will positively affect the learners' game performance in gamified cybersecurity labs.

> H4: Extrinsic motivation will positively affect learners' game performance in gamified cybersecurity labs.

The gamified cybersecurity labs are designed to help students learn the topics and skills related to cybersecurity issues. As learners through the designed gamified labs, they will be challenged by various tasks, and by understanding the instructions and completing the tasks, they will get points in the game, so-called game performance. Good performance in a cybersecurity lab indicates a learner managed to address lab tasks using the knowledge and skills learned from class. It is reasonable to believe learners with good lab performance not only acquire knowledge and skills from the lab but also gain confidence (i.e., self-efficacy). Existing studies have suggested that good background knowledge and high perceived self-efficacy help increase an individual's career interest (Tobey et al., 2014, Cheung et al., 2012, Bashir et al., 2017). Therefore, we hypothesize that game performance will positively affect learners' career interests after completing the lab.

> H5: Game performance will positively affect learners' career interests after completing the lab.

A learner's performance in the gamified labs is a good indicator of how well they understand the topic. By playing the game, their competencies of cybersecurity problem-solving skills are expected to improve and

will be reflected by their performance in the game. Hence, it is reasonable to claim that game performance is directly connected to learning outcome in gamified cybersecurity labs.

H6: Game performance will positively affect learners' learning outcome in gamified cybersecurity labs.

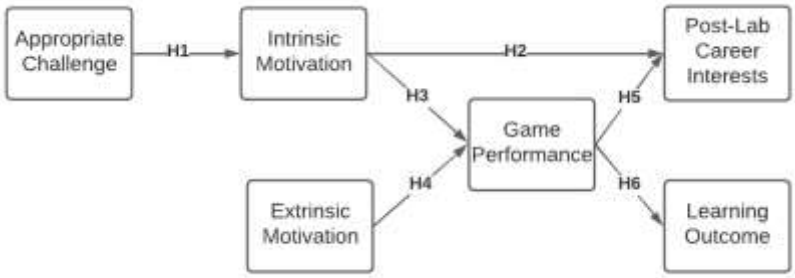

Figure 1. Research Model

Research Design and Method

We developed six gamified cybersecurity labs that cover the topics of symmetric encryption, hashing, public-key encryption, digital signature, network traffic analysis, and wireless network security based on the gamification principles. The game elements used in the labs include game storytelling, game rewards, leaderboard, and badges. All labs are structured as a sequence of tasks, each containing a scenario, mission description, lab instructions, and challenges. These labs were used as assignments in multiple cybersecurity courses.

To test the hypotheses above, we conducted an empirical study at a mid-sized private university in the United States. There were 122 students recruited for the study, including both undergraduate and graduate students. Each student was asked to complete a survey that measures the constructs in the proposed research model after he/she completed a gamified cybersecurity lab developed by the authors. The constructs in the research model were assessed by the instruments that were developed based on the existing literature.

Hypothesis Testing and Expected Results

A structural equation model will be used to test our hypotheses. The expected testing results reveal the relationships between the appropriate game challenge, intrinsic and extrinsic motivation, game performance, career interest, and learning outcome. The survey results are expected to demonstrate that gamification is beneficial and can be added to course assignments to improve students' learning outcomes. Besides, the results are also expected to indicate that the student's motivation and game performance positively influences their career interest. Additionally, the verification of the relationships among appropriate challenges, intrinsic and extrinsic motivations will enhance the understanding of how to improve the gamified lab learning outcome and suggest how gamification can be most effectively applied in cybersecurity education.

Limitations

This study has some limitations. First, this study uses data from gamified labs that deal with limited topics. Second, the research model is designed to analyze cross-sectional survey data, which cannot trace the longitudinal change of the relationships among the elements in the model.

REFERENCES

Anderson, R. C., & Romney, G. W. (2014). Student experiential learning of cyber security through virtualization. Journal of Research in Innovative Teaching, 7(1).

Bashir, M., Wee, C., Memon, N., & Guo, B. (2017). Profiling cybersecurity competition participants: Self-efficacy, decision-making and interests predict effectiveness of competitions as a recruitment tool. Computers & Security, 65, 153-165.

Beuran, R., Chinen, K.-i., Tan, Y., & Shinoda, Y. (2016). Towards effective cybersecurity education and training. Research report, 2016, 1-16.

Blustein, D. L. (1997). A context-rich perspective of career exploration across the life roles. The Career Development Quarterly, 45(3), 260-274.

Cheung, R. S., Cohen, J. P., Lo, H. Z., Elia, F., & Carrillo-Marquez, V. (2012). Effectiveness of cybersecurity competitions. In Proceedings of the International Conference on Security and Management (SAM) (p. 1). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp)

Coenraad, M., Pellicone, A., Ketelhut, D. J., Cukier, M., Plane, J., & Weintrop, D. (2020). Experiencing cybersecurity one game at a time: A systematic review of cybersecurity digital games. Simulation & Gaming, 51(5), 586-611.

Csikszentmihalyi, M. Flow: The psychology of optimal experience. New York: HarperPerennial, 1990.

Deci, E. L., & Ryan, R. M. Intrinsic Motivation and Self-Determination in Human Behavior. Springer, 1985.

Demmese, F., Yuan, X., & Dicheva, D. (2020, December). Evaluating the Effectiveness of Gamification on Students' Performance in a Cybersecurity Course. In Journal of the Colloquium for Information System Security Education (Vol. 8, No. 1).

Deterding, S., Dixon, D., Khaled, R., & Nacke, L. (2011, September). From game design elements to gamefulness: defining" gamification". In Proceedings of the 15th international academic MindTrek conference: Envisioning future media environments (pp. 9-15).

Donovan, L., & Lead, P. (2012). The use of serious games in the corporate sector. A State of the Art Report. Learnovate Centre (December 2012).

Druckman, D. (1995). The educational effectiveness of interactive games. In Simulation and gaming across disciplines and cultures: ISAGA at a watershed (pp. 178-187). Sage Publications.

Harackiewicz, J. M., Barron, K. E., Pintrich, P. R., Elliot, A. J., and Thrash, T. M. Revision of achievement goal theory: Necessary and illuminating. Journal of Educational Psychology, 94, 3 (2002), 638–645.

Hidi, S., & Renninger, K. A. (2006). The four-phase model of interest development. Educational psychologist, 41(2), 111-127.

(ISC)², Inc. (2021). A Resilient Cybersecurity Profession Charts the Path Forward. (ISC)2 Cybersecurity workforce study 2021. Retrieved February 26, 2022, from https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx

Karagiannis, S., & Magkos, E. (2021). Engaging Students in Basic Cybersecurity Concepts Using Digital Game-Based Learning: Computer Games as Virtual Learning Environments. In Advances in Core Computer Science-Based Technologies (pp. 55–81). Springer, Cham.

Lepper, M. R., Corpus, J. H., and Iyengar, S. S. Intrinsic and Extrinsic Motivational Orientations in the Classroom: Age Differences and Academic Correlates. Journal of Educational Psychology, 97, 2 (2005), 184–196.

Lent, R. W., Brown, S. D., & Hackett, G. (1994). Toward a unifying social cognitive theory of career and academic interest, choice, and performance. Journal of vocational behavior, 45(1), 79-122.

Lin, Y.-G., McKeachie, W. J., & Kim, Y. C. (2001). College student intrinsic and/or extrinsic motivation and learning. Learning and Individual Differences, 13(3), 251–258.

Ryan, R. M., & Deci, E. L. Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. American Psychologist, 55, 1 (2000), 68.

Tauer, J. M., & Harackiewicz, J. M. The Effects of Cooperation and Competition on Intrinsic Motivation and Performance. Journal of Personality and Social Psychology, 86, 6 (2004), 849–861.

Tobey, D. H., Pusey, P., & Burley, D. L. (2014). Engaging learners in cybersecurity careers: Lessons from the launch of the national cyber league. ACM Inroads, 5(1), 53-56.

Vigna, G. (2003). Teaching hands-on network security: Testbeds and live exercises. Journal of information warfare, 2(3), 8-24.

Wolfenden, B. (2019). Gamification as a winning cyber security strategy. Computer Fraud & Security, 2019(5), 9-12.