Gamification of MOOCs and Security Awareness in Corporate Training

Serafeim A. Triantafyllou[a] and Christos K. Georgiadis[b]
Department of Applied Informatics, University of Macedonia, Greece

Keywords: Gamification, MOOCs, Security Awareness Training, Gamification of Training.

Abstract: The rapid development of digital technology in today's times can enrich distance learning in the corporate sector, in a variety of ways. Nowadays, instructors have the capability to incorporate gamification into their teaching and make use of digital tools to create powerful online learning environments for research and problem analysis and simulation projects to improve training. Gamified MOOCs (Massive Open Online Courses) can enhance the motivation and engagement of trainees in a meaningful way to achieve learning goals. This paper aims to present innovative insights on the content of gamified MOOCs in the corporate training context, to enhance Security Awareness Training. Our methodology is based on Deterding's 2015 framework for gameful design, the lens of intrinsic skill atoms and we go a step further in our paper to propose a new approach, that is a structural model as a variation to Deterding's framework, that can find practical implementation in Integrated Development Environments (IDE) for gamified MOOCs. Gamified MOOCs when used as part of a cyber security awareness program, can play a significant role in the improvement of the overall training program as we describe in our case studies for Security Awareness Training.

1 INTRODUCTION

Digital technology is part of our everyday life, research, and teaching. Gamification can be used to facilitate training in every educational process. Gamification has strengthened the role of instructors, while at the same time offered great opportunities for distance learning utilization in the learning process (Beblavý et al., 2019; Bates, 2011; Nicholson, 2012). The employees that participate in a training program, using technological tools, tailor the course to their needs, analyze and evaluate the information they receive directly and learn how to learn by developing critical thinking (Reigeluth et al., 2015). Gamification, when used as part of a cyber security awareness program, has a significant role on the improvement of the overall training program. A common implementation of gamification adopts game-like features such as points, levels, badges, leaderboards, and achievements and rewards, and applies them to an educational context (Nicholson, 2012).

MOOCs are a very rapidly developing field and the main reasons for learners to participate in such online courses are motivation for learning and previous relevant learning experiences (Lock & Kingsley, 2007; Yang, 2014; Hew & Cheung, 2014). However, there are some key points of MOOCs that should be taken into consideration regarding their educational use (Ramesh et al., 2013; Milligan & Littlejohn, 2017;#Egloffstein & Ifenthaler, 2016), that is: (i) Familiarity with the use of ICT is essential, (ii) The trainees have to invest time and effort for their learning, (iii) Each course is a continuously evolving environment, following its own course without being tied to a curriculum, (iv) The trainee should have the necessary skills to self-regulate his/her learning.

Gamified MOOCs when used as part of a cyber security awareness program, can strengthen the overall training program and this paper aims to present innovative insights on the content of gamified MOOCs in the corporate training context, and answer to a basic research question, that is how the properly gamified MOOCs can enhance security awareness. For a more detailed presentation of the subject the

[a] https://orcid.org/0000-0003-2115-8934
[b] https://orcid.org/0000-0003-0897-9009

Triantafyllou, S. and Georgiadis, C.
Gamification of MOOCs and Security Awareness in Corporate Training.
DOI: 10.5220/0011103000003182
In *Proceedings of the 14th International Conference on Computer Supported Education (CSEDU 2022) - Volume 1*, pages 547-555
ISBN: 978-989-758-562-3; ISSN: 2184-5026

paper's structure consists of the following basic sections: 1) Introduction, 2) Focusing on the central importance of Cyber Security Awareness Training, 3) Efficacy of gamification, 4) Methodology and 5) Conclusions.

2 FOCUSING ON THE CENTRAL IMPORTANCE OF CYBER SECURITY AWARENESS TRAINING

In December 2020, the European Commission, and the European External Action Service (EEAS) introduced a new EU cybersecurity strategy ("European Council", 2020). Often, companies think that cybersecurity is exclusively an IT activity. However, numerous studies show that risks in a company's security sometimes stem from insiders. Insider threats even if they happen by accident, can cause financial damage, and affect the reliability of a company. To effectively treat user-caused problems inside the company, IT professionals need to implement security awareness training to all employees (Silic & Lowry, 2020).

In terms of software security, threat modeling is the most important part of software design and development. It is impossible to develop software applications that comply with corporate security policies and privacy requirements without evaluating and reducing threats. Threat modeling can help us to determine the threat environment and take the necessary measures and security controls to secure an organization. Threat modeling should study potential vulnerabilities and check for malicious code because these threats could damage financially an organization ("Deloitte", 2021).

3 EFFICACY OF GAMIFICATION

3.1 Confusions about Gamification

Gamification is the process of embodying game dynamics into non-game contexts with the basic goal to solve a typical problem or helping the users/trainees to change creatively some aspects of their behavior (Deterding, 2015; Antonaci et al., 2018). In a gamified training program, the basic learning goals are clearly defined for a set of activities and game elements like points or badges are given, to track user's behavior and give the necessary feedback to help him/her in training (Kapp et al., 2013). Also, we urge the users to achieve mastery to a specific task or activity by competing each other and afterwards when they finish their tasks/activities, we urge them to compare their final scores by adding leaderboards (Deterding, 2015).

In Human Computer Interaction (HCI) and Game Studies a lot of research is focused not only to the ease of use of a graphic interface, but also to what makes an interface to be enjoyable. The key point is to focus on the right game design principles to design enjoyable and playful interfaces (Malone, 1982). Research in Human Computer Interaction (HCI) tries to give us a better understanding of playfulness and the design principles that can lead to playful experiences. For example, we can mention the following about some game-like features (Deterding, 2015): (a) **Scores**: We should try to provide users with feedback on their actions as a rating score that allows comparison to a reference point, (b) **Role-Playing**: We should study the fact if the gamified system gives users particular roles to play and gain learning experiences, (c) **Leave gaps to fill**: We should leave gaps in a gamified set of activities and encourage users to fill them, (d) **Collections**: We should study the incentives that urge users to collect prizes, rewards, and items in a gamified activity.

Deterding help us with a detailed description to understand some misunderstandings about gamification (Deterding, 2015). The first confusion is the term 'reward' that is used commonly about gamification. The underlying model behind that concept is based on Skinner's theory where reward is a reinforcing stimulus. In positive reinforcement, a behavior is encouraged by rewards, leading to a continuous repetition of the desired behavior (Vargas, 2015). According to Raph Koster, who wrote the book titled "A theory of fun for game design", 'fun' is just another word for learning (Koster, 1971). Therefore, we come up to the conclusion that the fun in playing games, arises just from intrinsic enjoyment, not from extrinsic incentives (Deterding, 2015).

The second misunderstanding is that "gaminess" is not a feature that someone simply can add (Deterding, 2015). That means that it is not so simple to create an enjoyable activity by just adding some game like features or game elements. We should focus our attention on not just adding new game elements to a software system, but we should emphasize on the structure of the system and see if the system is well-structured, to generate experiences of intrinsic enjoyment. Motivational design is a

promising plan that will help us to restructure a system to support intrinsic motivation and enjoyment.

3.2 Flow Model and Structural Gamification

The father of positive psychology Mihaly Csikszentmihalyi (Csikszentmihalyi, 2014), trying to understand what leads to an optimal experience, he introduced the Flow Model in his book "Flow: The Psychology of Optimal Experience". He introduced 8 characteristics of flow: a) challenge/skill balance, b) well-explained goals, c) complete focus on the task, d) control, e) instant feedback, f) loss of self-consciousness. g) an experience becomes autotelic, h) Transformation of time. From Csikszentmihalyi's proposed model, instructors can take in mind some of these 8 characteristics to help trainees engage in learning tasks (Kim, Song, Lockee & Burton, 2018).

Structural gamification according to professor Kapp (Kapp et al., 2013) is: “the application of game-elements to propel a learner through content with no alteration or changes to the content." Structural gamification provides important information to both the trainees and the instructors as trainees complete parts of a training program, take quizzes to gain new knowledge and try to achieve the desirable educational goals. Also, gamification helps to identify the strong and weak points in the training program. For instance, an organization when it wants to implement structural gamification in training, it can provide learning content to trainees through a daily security quiz-type game for a period via email or a mobile app. If the trainees answer correctly, they can earn points, digital badges, and a specific place on a leaderboard for their continuous learning progress. If they answer incorrectly, they are immediately given hints to retry and answer the question (Kapp et al., 2013).

4 METHODOLOGY

4.1 Defining the Basic Steps of Our Methodology

Our research methodology was based on a basic research question (RQ) that is the following:
(RQ): How is gamification being designed and implemented on gamified MOOCs to enhance security awareness?

Our research methodology is based on review of previous works and the following basic steps show our basic research plan (see Figure 1):

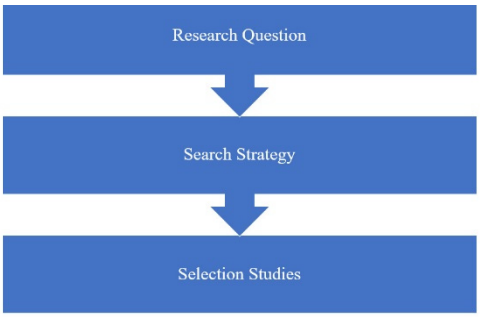

Figure 1: Steps of our methodology.

Step 1: Initial Search in Bibliographic Databases

The basic aim of our research methodology was at first to direct our research in order to find relevant studies about gamified MOOCs that can enhance security awareness in the corporate training context. We ran an initial search in Google Scholar database (a search with 'Skill atoms, security awareness and gamified MOOC' in the field including titles, abstracts and keywords, accessed 21 November, 2021) in order to find relevant publications about gamified MOOCs that can enhance security awareness.

After the initial search process, we continued with a more detailed and focused search process in other relevant bibliographic databases such as Scopus database, SpringerLink and Science Direct (Elsevier) (a search with 'skill atoms, security awareness and gamified MOOC' in the field including titles, abstracts and keywords in the Scopus, the SpringerLink and Science Direct (Elsevier) databases, accessed 22 November, 2021) in order to find more publications of high scientific rigor.

Step 2: Defining Selection Criteria

To select our papers, we defined the following criteria:

1. Peer-reviewed full-text papers published in an international venue that focused on gamified MOOCs to enhance security awareness were selected for review.
2. Research methods in the papers are clearly explained.

Step 3: Selected Studies

The number of selected papers is presented in Table1:

Table 1: MOOC studies.

Papers type	Studies
Research articles	(Bashir et al., 2015; Blohm, I., & Leimeister, J. M. (2013); Cabaj et al., 2018; Fini, 2009; Mirkovic & Benzel, 2012; Murphy et al., 2015; Paulsen et al., 2012; Paja et al., 2015; Salah, 2014; Vaibhav & Gupta, 2014)
Doctoral dissertation	(Ferrer Mico, et al., 2016)
Books	(Dalpiaz et al., 2016)

We have decided next to examine four online learning platforms that could be the basis for gamified MOOCs in order to enhance security awareness. With a spreadsheet, we have conducted a comparative analysis for four platforms (Khan Academy, Stack Overflow, Codecademy and Microsoft Virtual Academy) across two basic factors identified in the gamification literature area: (i) gamification mechanics and (ii) basic elements that enhance interaction. Within each of two factors, specific points were awarded. Specifically, we awarded one point for simple implementations aimed to enhance interaction and two points for a more advanced implementation. Next, we tried to make a plot of the final results in the following graph (see Figure 2):

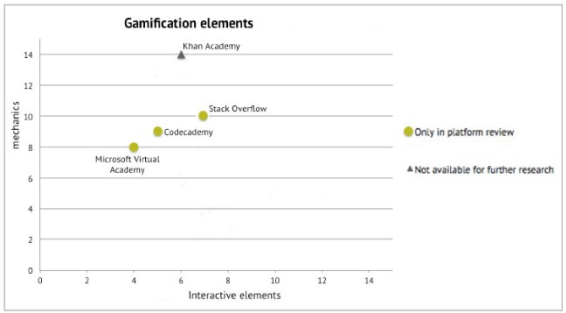

Figure 2: Graph of reviewed platforms.

To verify how gamified MOOCs can enhance security awareness, we tried to identify metrics for the success and effectiveness of eLearning platforms. There are two basic types of metrics for eLearning platforms: those for success and those for effectiveness. Metrics that emphasize on success, stem from the DeLone and McLean model of information systems success (D&M model) (see Figure 3) (DeLone & McLean, 2003; Manisi et al., 2018). Also, it is important to be measured to what extent trainees accept and adopt eLearning platforms as technological tools that can help them construct their knowledge (Lin, 2007;Fleming, Becker & Newton, 2017). The satisfaction of trainees is a strong motivator that urges them to participate in the training program.

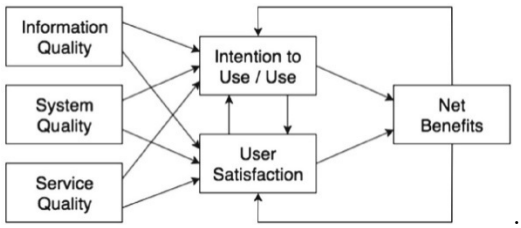

Figure 3: Updated D&M model (DeLone & McLean, 2003).

Manisi et al. (2018) have proposed a literature review summarizing the basic categories of the D&M model. The first category is 'Intension to Use/Use'. Manisi et al. (2018) describe that the users' intention can pre-exist before the real usage of an eLearning platform. This specific category measures the frequency of usage of an eLearning platform, that means in simple words that if the eLearning platform is useful the user would recommend the eLearning platform to others. (Wang, Wang & Shee, 2007). The following category is 'User Satisfaction'. The D&M model describes the satisfaction of the user after the process of interaction with the system. The following category 'System Quality' describes that the quality of the eLearning platform stems from the real quality of its hardware and software (Tate et al., 2014). The category 'Information Quality' is defined as the overall quality of the outcomes of the eLearning platform (Hassanzadeh, Kanaani & Elahi, 2012). Hagen, Albrechtsen & Ole Johnsen (2011), mention also that security should also be carefully taken into consideration when trying to measure information quality. Users should ask if the eLearning platform's educational content is right and matches the teaching material that is taught in the course (Lin, 2007). Hassanzadeh, Kanaani & Elahi (2012) mention that the 'Service Quality' category is responsible for the analysis of the effectiveness and efficiency of the technical support provided to the eLearning platform. This category is crucial to the overall success of the eLearning platform. The last category is 'Net Benefits' and describes after a total check if the eLearning platform brings real benefit to users (Aparicio, Bacao & Oliveira, 2016).

4.2 A Proposed Structural Model for Gamification

Game elements synthesis includes a certain goal that the trainee has in combination with a certain set of skills that is asked from the trainee to develop by participating in structured gamified tasks of a software system with main aim to succeed and achieve the desirable learning goals. Also, there is a rule system with transparent rules that determines if the final actions of the trainee were successful or not. Afterwards, immediate feedback about the trainee's progress can help him/her to go to the next level and achieve mastery of competence when he/she completes a challenge with success. We propose as a variation to Deterding's structural model, the following structural model (see Figure 4) inspired by the concept of skill atoms (Deterding, 2015).

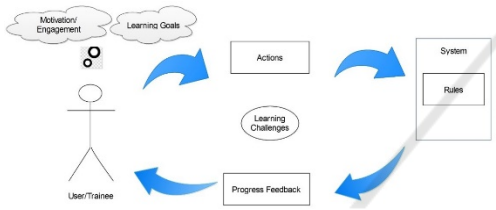

Figure 4: Structural Model for gamified MOOCs.

In our proposed structural model for gamification, skill atoms constitute the basic elements that clarify the feedback repetitive cycle between the user/trainee and the system that is based on a basic challenge or skill (Deterding, 2015). A game atom contains smaller particles that cannot be divided into smaller entities without the game system to lose his "gaminess" (Deterding, 2015). Through the repetitive and continuous interaction via multiple run-throughs of the atom, the trainee gains the necessary knowledge and masters new skills. The above-mentioned structural model's utility is apparent, when we focus on trainees with basic competence that participate in a gamified MOOC to develop new skills through motivating and enjoyable learning challenges. For example, Codecademy trains users to program by using game-like features such as points and digital badges. The core of this structured model of Codecademy is the programming editor where users can learn to code by typing the code and check the repetitive cycle of programming process in a gameful way by running the code and seeing the final outcomes.

4.3 MOOCs and Gamification Tools for Enhancing Security Awareness

4.3.1 Conceptualizing MOOCs and Gamification Tools

MOOCs have been qualified as the revolution of online learning and training. Therefore, many researchers focused their research on why learners still face difficulty in studying the educational material of these courses. Researchers to answer this question carefully studied theories of motivation, because motivation is acknowledged to be one of the most important predictors of learners' performance in learning. Self-Determination is a theory of human motivation developed by psychologists Edward Deci and Richard Ryan. The key point of this theory is motivation that drives a person to act. According to this theory each learner has three basic needs and only when these needs are satisfied the individual can have a better performance in learning. These needs are: (a) autonomy, (b) competence, (c) relatedness (Deci & Ryan, 2002; Niemiec & Ryan, 2009).

Self-regulation strategies in MOOCs are mostly based on self-regulated learning (SRL) theory, which describes how learners can take control of their learning (Jonassen et al., 1995). In our paper, we determine to choose the combination of self-regulated learning with collaborative learning. Collaborative learning is considered to bring many benefits ranging from better learning outcomes to improved social skills because it creates the conditions for effective interactions between team members (Staubitz et al., 2015; Dillenbourg, Järvelä and Fischer, 2009; Jonassen et al., 1995; Jonassen, 2013 ; Thornton & Francia, 2014; Antonaci et al., 2018).

4.3.2 Valorization of Gamification for Cyber Security Awareness Training

Empirical evidence shows that gamification has the potential to drive user engagement and cause behavior change (Silic & Lowry, 2020). The idea of using gamification in security awareness training programs derives from many studies. Thornton and Francia (2014) have focused on their study on designing two games for security awareness training. The first Brute Force game was designed with the main aim to teach and persuade users to use strong and complex passwords while the second Friend or Foe game was designed for phishing awareness training. Employees unintentionally make actions without realizing the damage they can cause to the organization's cybersecurity (Silic & Lowry, 2020).

Most common human errors are related to account passwords (Scholefield and Shepherd, 2019).

To make right use of gamified techniques and tools for security awareness training at a company or an organization we must first clarify which are the basic goals of the security awareness training course (Korpela, 2015). Gamification of training programs can help a lot to enhance employees' motivation and engagement to the learning process (Kyewski and Krämer, 2018; Adams and Makramalla, 2015). Along with the game-like features and tools that are attractive to trainees, games also provide the tools so as the courses to be taught through trial-and-error methods without causing any harm or risk to the company. Successful training on cybersecurity fundamentals should be provided in different formats and the trainings must run across all levels of the workforce (Jordan et al., 2011). The most effective security awareness training programs use phishing simulations and other practical simulations to teach users how to protect against cyber threats like phishing, ransomware, malware and other cyberthreats. For cyber security awareness training, gamification can create playful and engaging ways that will help companies to promote and create a security culture.

4.3.3 Case Studies for Security Awareness Training

To enhance the interest in security awareness, Deloitte introduced a game-based learning experience in the form of an escape room game. In the escape room game, the maximum number of participants comes to 5 to 6 participants per rotation. The basic challenge for employees is to solve 7 challenges within 20 minutes to finish the game. In the gamified scenario participants are asked to unlock a laptop that is infected with ransomware to keep secure sensitive company data. Every challenge is designed to test participants' security knowledge and to incentivize them to adopt a secure behavior (Deterding, 2015).

Cybersecurity hackathons constitute a form of training organized by using training platforms. Cyber security training can include training exercises that might be structured in the form of a game. Games force players to take decisions depending on how they perceive the game through their personal observations. CyberCIEGE is a network security simulation in the form of a video-game with basic goal to inspire and teach measures that protect and defend information (Irvine & Thompson, 2010). Players through a three-dimensional interface, spend virtual money for the necessary network equipment (servers, network devices etc.) that is needed to construct, set in operation, and defend an enterprise network by taking instant decisions and estimating the results of their decision, while the network is still under cyber-attack. With this form of training, employees are involved to effective cybersecurity practices and extend their knowledge to the technologies involved to cyber security.

TableTop eXercise Web Environment is a game-based part of Cyber Security Training platform developed at Vilnius University that defines user roles and includes TableTop eXercises, and the best practices to effectively handle a security incident. A security incident has its lifecycle, and the TableTop eXercise Web Environment provides incident scenario simulation and online web-based software for incident reports that help in the process of solving the incident (Brilingaitė et al., 2017).

Gonzalez-Manzano and Jose de Fuentes have completed an important and wide-ranging (from beginner to advanced level) scientific work of examining and identifying 35 free cybersecurity MOOCs from the most well-known MOOC platforms. Plenty of these courses (25/35) were constructed and released by American universities, but there were also free MOOCs that were available to the users. These courses (33 courses) were focusing on 52 work roles that find practical application in any sector and 33 different areas of specialization in cybersecurity such as Software Development (DEV), Systems Requirements Planning (SRP), Systems Development (SYS), Risk Management (RSK) and others among them (González-Manzano and de Fuentes, 2019).

5 CONCLUSIONS

This paper tries to answer a basic research question, that is how the properly gamified MOOCs can enhance security awareness. Gamified MOOCs when used as part of a cyber security awareness program, can play a significant role in the improvement of the overall training program as we have described in our case studies for Security Awareness Training. However, further investigation of the proposed structured model in gamified platforms, could help to test its utility, because gamification is not a stagnant but a continously evolving area of research.

In a training program, trainees have to self-regulate their learning. Every active participant in a team must first have himself/herself adjust his/her learning goals and personal time in such a way that

he/she can then collaborate properly with the other members of the team. Security awareness training gives trainees the basic knowledge they need to keep the sensitive data of a company safe, and to be successful, this training needs to be appealing and meaningful. Gamification with the use of MOOCs is a user-centered approach and provides a technology-driven learning environment for proper cyber training. MOOCs that are well designed by using cybersecurity scenarios can lead to better protection against cyber-attacks. Future work will include more research analysis with practical implementation of our proposed structural model, in the continuously evolving research area of gamification for security awareness training.

REFERENCES

Adams, M. and Makramalla, M., 2015. *Cybersecurity Skills Training: An Attacker-Centric Gamified Approach. Technology Innovation Management Review, 5(1), pp.5-14.*

Antonaci, A., Klemke, R., Kreijns, K., & Specht, M. (2018). *Get Gamification of MOOC right!. International Journal of Serious Games, 5(3), 61-78. doi: 10.17083/ijsg.v5i3.255*

Aparicio, M., Bacao, F., & Oliveira, T. (2016). *Cultural impacts on e-learning systems' success. The Internet and Higher Education, 31, 58-70. doi: 10.1016/j.iheduc.2016.06.003*

Bashir, M., Lambert, A., Wee, J. M. C., & Guo, B. (2015). *An examination of the vocational and psychological Characteristics of Cybersecurity Competition partici-pants. In 2015 {USENIX} Summit on Gaming, Games, and Gamification in Security Education (3GSE 15).*

Bates, T. (2011). *Changing cultures in higher education: moving ahead to future learning. Distance Education,* 32(1), 143-148. doi: 10.1080/01587919. 2011.565507

Beblavý, M., Baiocco, S., Kilhoffer, Z., Akgüç, M. & Jacquot. *M. Index of Readiness for Digital Lifelong Learning Changing How Europeans Upgrade Their Skills* Final Report November 2019. [accessed 25 july 2021].

Blohm, I., & Leimeister, J. M. (2013). *Gamification: Design of IT-Based Enhancing Services for Motivational Support and Behavioral Change. Business & Information Systems Engineering, 5(4), 275-278.*

Brilingaitė, A., Bukauskas, L., Krinickij, V., & Kutka, E. (2017, October*). Environment for cybersecurity tabletop exercises. In ECGBL 2017 11th European Conference on Game-Based Learning (pp. 47-55). Academic Conferences and publishing limited.*

Cabaj, K., Domingos, D., Kotulski, Z., & Respício, A. (2018). *Cybersecurity education: Evolution of the discipline and analysis of master programs. Computers & Security, 75, 24-35.*

Csikszentmihalyi, M. *(2014). Toward a Psychology of Optimal Experience. Flow And The Foundations Of Positive Psychology, 209-226. doi: 10.1007/978-94-017-9088-8_14*

Dalpiaz, F., Paja, E., & Giorgini, P. (2016). *Security requirements engineering: designing secure socio-technical systems. MIT Press.*

Deci, E. L & Ryan, R. M. (2002). Overview of self-determination theory: An organismic dialectical perspective. Handbook of self-determination research, 3-33.

Deloitte. Serious Gaming: *The Security Awareness Escaperoom. A gamified approach to cyber security awareness training. August 17, 2021. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/risk/deloitte-nl-cyber-risk-the-security-awareness-escape-room.pdf*

DeLone, W. H., & McLean, E. R. (2003). *The DeLone and McLean Model of Information Systems Success: A Ten-Year Update. Journal of Management Information Systems, 19(4), 9–30. http://www.jstor.org/stable/40398604*

Dillenbourg, P., Järvelä, S., & Fischer, F. (2009). The *Evolution of Research on Computer-Supported Collaborative Learning. Technology-Enhanced Learning, 3-19. doi: 10.1007/978-1-4020-9827-7_1*

Deterding, S. (2015). *The Lens of Intrinsic Skill Atoms: A Method for Gameful Design. Human–Computer Interaction, 30(3-4), 294-335. doi: 10.1080/07370024.2014.993471*

Egloffstein*, M., & Ifenthaler, D. (2016). Employee Perspectives on MOOCs for Workplace Learning. Techtrends, 61(1), 65-70. doi: 10.1007/s11528-016-0127-3*

European Council. 2020. *Cybersecurity: how the EU tackles cyber threats. [Accessed 3 August 2021].*

Evans, S., & Myrick, J. (2015). *How MOOC instructors view the pedagogy and purposes of massive open online courses. Distance Education, 36(3), 295-311. doi: 10.1080/01587919.2015.1081736*

Ferrer Mico, M. T. (2016). *Community of Inquiry (COI) and Self-Directed Learning (SDL) in Online Environments: An Exploratory, Correlational and Critical Analysis of MOOCs. Introduction to Cybersecurity MOOC Case Study (Doctoral dissertation, Universitat Ramon Llull).*

Fini, A. (2009)*. The technological dimension of a massive open online course: The case of the CCK08 course tools. International Review of Research in Open and Distributed Learning, 10(5).*

Fleming, J., Becker, K., & Newton, C. (2017)*. Factors for successful e-learning: does age matter?. Education + Training, 59(1), 76-89. doi: 10.1108/et-07-2015-0057*

González-Manzano, L. and de Fuentes, J., 2019. *Design recommendations for online cybersecurity courses. Computers & Security, 80, pp.238-256.*

Hassanzadeh, A., Kanaani, F., & Elahi, S. (2012). *A model for measuring e-learning systems success in universities. Expert Systems with Applications, 39(12), 10959-10966. doi: 10.1016/j.eswa.2012.03.028*

Hew, K., & Cheung, W. (2014). *Students' and instructors' use of massive open online courses (MOOCs): Motivations and challenges. Educational Research Review, 12, 45-58. doi: 10.1016/j.edurev.2014.05.001*

Irvine, C. E., & Thompson, M. F. (2010, October). *Simulation of PKI-enabled communication for identity management using CyberCIEGE. In 2010-MILCOM 2010 Military Communications Conference (pp. 906-911). IEEE.*

Jonassen, D. (2013). *Transforming Learning with Technology. The Nature of Technology, 101-110. doi: 10.1007/978-94-6209-269-3_7*

Jonassen, D., Davidson, M., Collins, M., Campbell, J., & Haag, B. (1995*). Constructivism and computer-mediated communication in distance education. American Journal of Distance Education, 9(2), 7-26. doi: 10.1080/08923649509526885*

Jordan, C., Knapp, M., Mitchell, D., Claypool, M. and Fisler, K., 2011. *CounterMeasures: A game for teaching computer security. 2011 10th Annual Workshop on Network and Systems Support for Games,.*

Kapp, K. M. (2012). *The gamification of learning and instruction: Game-based methods and strategies for training and education. Hoboken: Wiley.*

Kim, S., Song, K., Lockee, B., & Burton, J. (2018). *Gamification in Learning and Education. doi: 10.1007/978-3-319-47283-6*

Korpela, K. (2015*). Improving Cyber Security Awareness and Training Programs with Data Analytics. Information Security Journal: A Global Perspective, 24(1-3), 72-77. doi: 10.1080/19393555.2015.1051676*

Koster, R. 1971-. A *Theory of Fun for Game Design. Scottsdale, AZ :Paraglyph Press, 2005.*

Kyewski, E. and Krämer, N., 2018. *To gamify or not to gamify? An experimental field study of the influence of badges on motivation, activity, and performance in an online learning course. Computers & Education, 118, pp.25-37.*

Lin*, H. (2007). Measuring Online Learning Systems Success: Applying the Updated DeLone and McLean Model. Cyberpsychology & Behavior, 10(6), 817-820. doi: 10.1089/cpb.2007.9948*

Lock, R., & Kingsley, K. (2007). *Empower Diverse Learners with Educational Technology and Digital Media. Intervention In School and Clinic, 43(1), 52-56. doi: 10.1177/10534512070430010701*

Malone*, T. (1982). Heuristics for designing enjoyable user interfaces. Proceedings of The 1982 Conference On Human Factors In Computing Systems - CHI '82. doi: 10.1145/800049.801756*

Manisi, P., Jantjies, M., & Kimani, L.W. (2018). A *Conceptual Integrated Model for Measuring the Success of eLearning in Developing Countries: Literature Review. 2018 IST-Africa Week Conference (IST-Africa), Page 1 of 9-Page 9 of 9.*

Milligan, C., & Littlejohn, A. (2017). Why Study on a MOOC? *The Motives of Students and Professionals. The International Review Of Research In Open And Distributed Learning, 18(2). doi: 10.19173/irrodl.v18i2.3033*

Mirkovic, J., & Benzel, T. (2012). Teaching cybersecurity with DeterLab. IEEE Security & Privacy, 10(1), 73-76.

Murphy, J., Kalbaska, N., Horton-Tognazzini, L., & Cantoni, L. (2015). *Online learning and MOOCs: A framework proposal. In Information and Communication Technologies in Tourism 2015 (pp. 847-858). Springer, Cham.*

Niemiec, C., & Ryan, R. (2009*). Autonomy, competence, and relatedness in the classroom. Theory and Research In Education, 7(2), 133-144. doi: 10.1177/1477 878509104318*

Nicholson, S. (2012). A User-Centered Theoretical Framework for Meaningful Gamification.

Paja, E., Dalpiaz, F., & Giorgini, P. (2015). Modelling and reasoning about security requirements in socio-technical systems. Data & Knowledge Engineering, 98, 123-143.

Paulsen, C., McDuffie, E., Newhouse, W., & Toth, P. (2012). NICE*: Creating a cybersecurity workforce and aware public. IEEE Security & Privacy, 10(3), 76-79.*

Ramesh, A., Goldwasser, D., Huang, B., Daumé III, H., & Getoor, L. (2013*). Modeling learner engagement in MOOCs using probabilistic soft logic. In NIPS workshop on data driven education (Vol. 21, p. 62).*

Reigeluth, C., Aslan, S., Chen, Z., Dutta, P., Huh, Y., & Lee, D. et al. (2015). *Personalized Integrated Educational System. Journal Of Educational Computing Research, 53(3), 459-496. doi: 10.1177/0735 633115603998*

Salah, K. (2014, March). Harnessing the cloud for teaching cybersecurity. In Proceedings of the 45th ACM technical symposium on Computer science education (pp. 529-534).

Scholefield, S., & Shepherd, L. (2019*). Gamification Techniques for Raising Cyber Security Awareness. HCI For Cybersecurity, Privacy and Trust, 191-203. doi: 10.1007/978-3-030-22351-9_13*

Silic, M., & Lowry, P. (2020). *Using Design-Science Based Gamification to Improve Organizational Security Training and Compliance. Journal Of Management Information Systems, 37(1), 129-161. doi: 10.1080/07421222.2019.1705512*

Staubitz, T., Pfeiffer, T., Renz, J., Willems, C., & Meinel, C. (2015, November). *Collaborative learning in a MOOC environment. In Proceedings of the 8th annual international conference of education, research and innovation (pp. 8237-8246).*

Tate, M., Sedera, D., McLean, E., & Burton-Jones, A. (2014). *Information Systems Success Research: The "20-Year Update?" Panel Report from PACIS, 2011. Communications of the Association for Information Systems, 34, pp-pp. https://doi.org/10.17705/1CAIS .03466*

Thornton, D., & Francia, G.A. (2014). *Gamification of Information Systems and Security Training: Issues and Case Studies.*

Vaibhav, A., & Gupta, P. (2014). *Gamification of MOOCs for increasing user engagement. In 2014 IEEE International Conference on MOOC, Innovation and Technology in Education (MITE) (pp. 290-295). IEEE.*

Vargas, E. (2015). *B.F. Skinner's theory of behavior. European Journal of Behavior Analysis, 18(1), 2-38. doi:10.1080/15021149.2015.10 65640*

Wang, Y., Wang, H., & Shee, D. (2007*). Measuring e-learning systems success in an organizational context: Scale development and validation. Computers In Human Behavior, 23(4), 1792-1808. doi: 10.1016/j.chb.2005.10.006*

Yang, Q. (2014). *Students Motivation in Asynchronous Online Discussions with MOOC Mode. American Journal Of Educational Research, 2(5), 325-330. doi: 10.12691/education-2-5-13*