MEMORABLE: a Multi-playEr custoMisable seriOus game fRAmework for cyBer-security LEarning

Jingyun Wang[1 [0000−0001−9325−1789]], Ryan Hodgson[1 [0000−0002−7704−2562]], and Alexandra I. Cristea[1 [0000−0002−1454−8822]]

Durham University, Durham, DH1 3LE United Kingdom
jingyun.wang@durham.ac.uk

Abstract. In this paper, we propose an educational game framework allowing instructors to customise the game's learning content in the context of cyber-security, with the aim of ensuring learners are engaged with educational games. This can further support them continuing to acquire useful cyber-security knowledge, while playing with their peers. Based on this framework, a prototype digital game called "Cyberpoly" was implemented and evaluated. This game allows unfamiliar or potentially unappealing, 'dry' learning contents (on cyber-attacks and incidents) to be placed in a context similar to a "monopoly" game board, encouraging multiple players to take an active role when landing on various cyber-attack or incident squares. The learner can not only answer the questions generated by the game, but also actively send cyber-attacks to other players, when landing on another's land. Learner data was collected from 30 undergraduate participants, with results suggesting that most found it engaging and felt motivated to learn. Further to this, we also obtained feedback from two academic professors, to discuss not only game-play but also game element management.

Keywords: Customisable game content · Cyber-Security knowledge · Multi-player · educational games.

1 Introduction

With the proliferation of online conferences and business meetings during the Coronavirus pandemic, cyber-security knowledge has become an essential necessity for users of technology. It is reported that more data was compromised in 2020 than in the previous 15 years combined [1]. It is found that 90 percent of security incidents and breaches were caused by human errors [15], and a fundamental aspect of the issue is the lack of awareness and knowledge on cyber-security of the end users. On the other hand, it is challenging to teach cyber-defense knowledge in an accessible and enjoyable way, especially to those without a technical background. One approach to address this issue is through educational digital games [16]. Combining the enjoyable game features with a serious educational objective may be beneficial in motivating a user to learn about a subject [14], particularly if they have no prior knowledge of the domain. Additionally, this may assist in the retention of any learned knowledge [12]. This is especially promising for highly-technical subjects, such as cyber-security, where users may not find the subject interesting, or may be unfamiliar with the subject.

To support cyber-security learners in an engaging way, we propose a *customisable multi-player educational game framework for cyber-security*. The most prevalent motivation is to provide a serious game element bank, serving as a template, which can be reused by various games, with the aim of supporting cyber-security education. All of the educational contents within the serious game element bank are organised and maintained by instructors, in order to support serious games to focus on conveying key cyber-knowledge to learners and help them to develop their skills and understanding. Furthermore, a prototype digital game was implemented and evaluated based upon this framework. Based on the feedback from experiment participants, we seek to evaluate if this educational game may enhance learning motivation due to its competition environment.

The main contributions of this research are: **(1) A fine-granularity approach for game element placement.** Placing game elements in a meaningful context is essential for serious game design [9]. The educational contents chosen to be incorporated into our game framework are various existing cyber-incidents, cyber-attacks, which exploit the different vulnerabilities, and the laws related to cyber-security, as well as the countermeasures that can be applied, to prevent cyber-attacks. With this game element placement. Intelligent Tutoring functions could be easily implemented to identify the knowledge status of learner and provide adaptive learning path based on their behaviour in the game. **(2) Customisable game elements.** In previous educational games in cyber-security [3–5, 2, 6], the content being taught is built into games and fixed, which limits the scope and flexibility. Since the cyber-security topics are continuously expanding and changing, being able to create new content and adjust existing content in educational games can keep them relevant for a large number of players. We proposed to support the instructors to manage the contents used in the educational games, which can ensure they have up to date contents in response to the emerging cyber-attacks, cyber incidents, countermeasures and laws. Moreover, by making use of contents in these three areas, the instructors are expected to easily create/edit questions. Those questions, together with contents related to the three areas consisting of the "serious game element bank" (defined in this research) should be able to be further reused by multiple games. **(3) Gameplay.** The gameplay of most previous educational games on cyber-security [3–5, 2, 6] consisted simply of individually answering different categories/topics/difficulty level of questions delivered automatically, suggesting that more enjoyable gameplay could be obtained by interaction with peers, to hold the player's interest. In our prototype multi-player game "Cyberpoly", the player can actively send a cyber-attack, using one of the attack cards to others, when landing in their land, and the landlord needs to respond to the attack. This scenario not only increases the interaction between players but also simulates reality in which the players need to respond to any received cyber-attack.

2 Related work

Digital educational games, which offer the players the opportunity to take roles, think and act the way they cannot experience in reality, has been proven to be a powerful tool to enable knowledge acquisition, by providing engaging and motivational contexts [9]. Instead of focusing on providing entertainment, the main purpose of educational games is to incorporate pedagogical theories and educational content into game elements. Therefore, the pedagogical theory behind the game design is the most essential issue for the educational effectiveness [9].

Several educational games have been developed for supporting cyber-security learning. CyberSprinters [3] was developed by the National Cyber Security Centre (NCSC) as an educational resources toolkit, requiring learners aged 7-11 to answer questions while guiding an avatar through a virtual world. Keep Tradition Secure [4] by Texas A&M University required players to simply answer questions, as they made their way around campus. Targeted Attack [5] by Trend Micro was a video-based single mode simulation game based on the format of the old "Choose Your Own Adventure" books. The player acted as the Chief information officer of a global organisation, on the verge of making the first release of a biometrically authenticated mobile payment application, to deal with various cyber-security situation related to such a framework. Cybersecurity Lab [2] by PBS allocated players the role of the chief technology officer of a social network company and required them to answer questions to gain coins for strengthening their cyber-defenses. The UK National Crime Agency, together with Cyber Security Challenge UK, have provided a selection of interactive games [6], which require players to complete various tasks in different scenarios. However, the fixed educational content in such games leads to inflexibility, due to limiting to a given user type. Therefore, in this work, we propose an educational game framework which may enable instructors to organise teaching materials for serious games aiming to support various cyber-security learners.

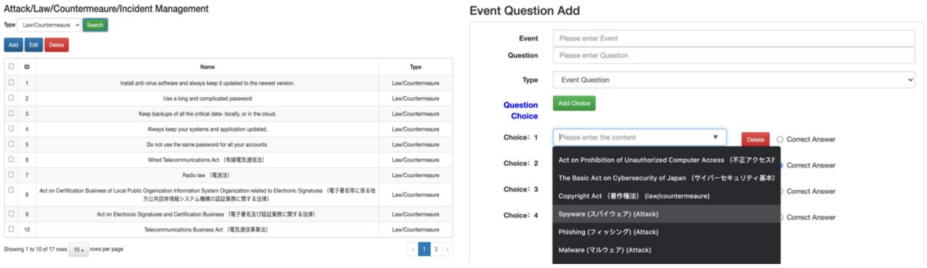
Moreover, existing serious games targeted at cyber-security learning only support learners to practice alone (single player mode), with none providing a multiplayer mode [18] with a collaborative learning environment.The primary objective of collaborative learning[10] is to allow learners to interact in ways such that certain learning mechanisms are triggered. In a cooperative setting, players may combine complementary skills, knowledge or resources, when completing in-game tasks; in contrast, competitive play styles encourages players to achieve better results based upon specified performance evaluation metrics, such as score, or time goals[17]. Pirates Treasure Hunt[8], targeted towards European elementary school children aged 7-10 years, was presented to stimulate the interest and attention on other cultures and lifestyles. Multi-players were tasked with using their acquired knowledge to spot non-European objects within the 2D game environment. VocaMomo [11] was intended to teach English vocabulary, with stakeholders being students and their parents. The game applied the basic rules of Monopoly and Scrabble strategy game, where players take turns rolling dice, with the aim at each turn to find a correctly spelled word, through dragging and dropping alphabet tiles. The use of popular games as a base for the serious game is a common pattern. Similarly, [13] proposed an multi-player game to educate children about nutrition and health using a Bingo process, where the player picked a number from the table, with each number representing a question on nutrition. Players were rewarded in experience points and the team with the maximum points won the quiz. Therefore, a multi-player serious game environment, which combines the merits of collaborative learning, is designed and implemented for cyber-security learning in this paper.

3 MEMORABLE: a customisable serious game framework

For this work, we demonstrate the implementation of an educational game framework, which allows instructors to customise the game's learning content (serious game element) in the context of cyber-security: cyber-incidents, attacks, laws/countermeasures, and questions created conveniently based on the first three types of content (as shown in Fig.1). This framework design ensures that the educational game is usable by a variety of audiences through enabling customisation, thus allowing for game content to be tailored to different countries, age groups, etc., contrasting to existing educational games with fixed content limited to a single demographic. Additionally, emphasis is placed upon the requirement for the modification of learning material to be as simple and intuitive as possible. The educational aspect of the game incorporates multiple choice questions, aiming for instructors to be able to easily create a large quantity of questions and answers, for use in the game. Therefore, we ensured that system design would account for the capability of instructors to modify basic building blocks of two categories of the multiple-choice questions related to cyber-security laws/countermeasures, attacks, and incidents, so that these components could be reused and combined in different ways.

3.1 Game element management panels

Fig. 1 (a) shows the cyber elements management panel, in which the instructors can add, edit and delete 3 types of elements (cyber-attacks, cyber-incidents, and laws and countermeasures). The system also provides a question management panel for organizing two types of questions. Event questions involving an incident (i.e. a story about a cyber-security event that has occurred) and multiple answer options, which can either be about laws/countermeasures, or attacks. Attack card questions, involving knowledge about a specific cyber-attack are demonstrated in Fig.2(b). When creating questions and corresponding answers, the instructor can choose the content organised in the three cyber-element lists from a drop-down menu, so that they may easily create questions and edit choice options, as shown in Fig.1(b). This framework supports two types of users: Instructors, with the ability to input and modify the learning materials of the game, and students, who may play with peers in any corresponding educational games built on those materials. Multiple game sessions can take place at the same time, ensuring a large number of learners can play educational games concurrently and keep track of their progress in all the games. Furthermore, a learner's playing record is saved within a database, allowing the instructor to analyse the learning status of each learner, and adjust learning contents or provide individual instruction.



Attack/Law/Countermeaure/Incident Management

Type: Law/Countermeaure

□	ID	Name	Type
□	1	Install anti-virus software and always keep it updated to the newest version.	Law/Countermeaure
□	2	Use a long and complicated password	Law/Countermeaure
□	3	Keep backups of all the critical data- locally, or in the cloud.	Law/Countermeaure
□	4	Always keep your systems and application updated.	Law/Countermeaure
□	5	Do not use the same password for all your accounts.	Law/Countermeaure
□	6	Wired Telecommunications Act （有線電気通信法）	Law/Countermeaure
□	7	Radio law （電波法）	Law/Countermeaure
□	8	Act on Certification Business of Local Public Organization Information System Organization related to Electronic Signatures （電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律）	Law/Countermeaure
□	9	Act on Electronic Signatures and Certification Business （電子署名及び認証業務に関する法律）	Law/Countermeaure
□	10	Telecommunications Business Act （電気通信事業法）	Law/Countermeaure

Showing 1 to 10 of 17 rows 10 rows per page

(a)

Event Question Add

Event: Please enter Event

Question: Please enter Question

Type: Event Question

Question Choice

Choice：1 Please enter the content ▼ Delete ○ Correct Answer

Choice：2 Correct Answer

Choice：3 Correct Answer

Choice：4 Correct Answer

Act on Prohibition of Unauthorized Computer Access （不正アクセス
The Basic Act on Cybersecurity of Japan （サイバーセキュリティ基本
Copyright Act （著作権法） (law/countermeaure)
Spyware (スパイウェア) (Attack)
Phishing (フィッシング) (Attack)
Malware (マルウェア) (Attack)

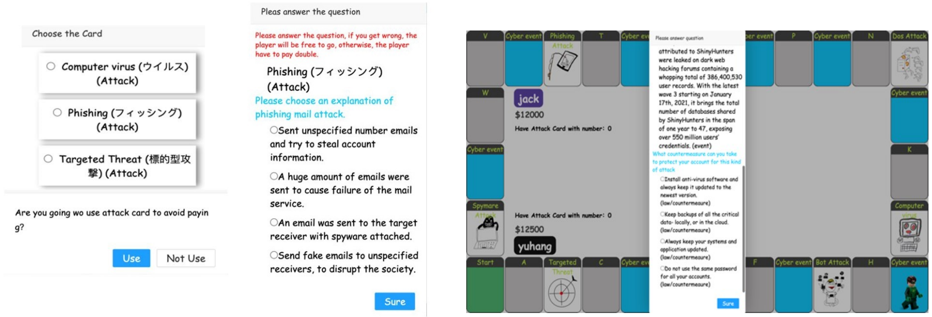
(b)

Fig. 1: Learning content management interfaces.

3.2 A prototype multi-player game: "Cyberpoly"

A prototype digital game called "Cyberpoly" was implemented based on this architecture. When a player logs in the game lobby, they are presented with a room of tables, ensuring players may take part in a game with other players on a table. Each table allows 4 players maximum, and a minimum of 2 once all players present have agreed to start. Fig. 2 depicts the main game-play interface of two players. Rules of play are the following: 1. The player moves the specified numbers of grid spaces in turns, based upon a dice roll. 2. Upon landing on an area, a player may choose to buy the area, if it does not belong to anyone already. 3. The player may choose to use an attack card to avoid paying (event 1, as shown in Fig.2(a-1)) or to pay the corresponding fee when landing at the other player's area. If the landlord correctly answers the received question (as shown in Fig.2(a-2)), the attacker will need to pay double, otherwise, the attacker does not need to pay anything. 4. A player landing on the blue area will trigger a cyber-security incident (event 2, as shown in Fig.2(b)). and cyber-attack cards will be rewarded, if they correctly answer the question appearing. 5. Upon landing on an area with a cyber-attack image, a question relevant to the attack will be asked (event 3, the question is similar to Fig.2(a-2) but with different punishment and reward). If the player correctly answers this question, they are rewarded with in-game money, if they fail to answer correctly, the player will lose money. 6. Each player starts the game with the same amount of in-game money. The players to lose all their money will lose the game.

The formulation of this play structure is designed to ensure students take in cyber-security knowledge at a deeper level through competition, by stimulating the students' learning interest. As noted, we divide cyber-security knowledge into



Choose the Card

○ Computer virus (ウイルス) (Attack)

○ Phishing (フィッシング) (Attack)

○ Targeted Threat (標的型攻撃) (Attack)

Are you going wo use attack card to avoid payin g?

Use Not Use

Pleas answer the question

Please answer the question, if you get wrong, the player will be free to go, otherwise, the player have to pay double.

Phishing (フィッシング) (Attack)

Please choose an explanation of phishing mail attack.

○Sent unspecified number emails and try to steal account information.

○A huge amount of emails were sent to cause failure of the mail service.

○An email was sent to the target receiver with spyware attached.

○Send fake emails to unspecified receivers, to disrupt the society.

Sure

Please answer question

attributed to ShinyHunters were leaked on dark web hacking forums containing a whopping total of 386,400,530 user records. With the latest wave 3 starting on January 17th, 2021, it brings the total number of databases shared by ShinyHunters in the span of one year to 47, exposing over 550 million users' credentials. (event)

What countermeasure can you take to protect your account for this kind of attack

○Install anti-virus software and always keep it updated to the newest version. (law/countermeaure)

○Keep backups of all the critical data- locally, or in the cloud. (law/countermeaure)

○Always keep your systems and application updated. (law/countermeaure)

○Do not use the same password for all your accounts. (law/countermeaure)

Sure

jack
$12000
Have Attack Card with number: 0

Have Attack Card with number: 0
$12500
yuhang

(a-1) use a attack card

(a-2) a quesion received by landlord

(a) Sending an attack card (Event 1).

(b) A cyber-security incident (Event 2) .

Fig. 2: The main interface of the prototype game "Cyberpoly".

cyber-attacks,incidents, and countermeasures, with the aim of ensuring that in-game events represent common attacks, incidents and countermeasures employed within the cyber-security domain.The educational features present within the game are implemented with the aim of providing educational value, which is relevant to the industry, with cyber-incidents in event 2 representing the cyber-incidents happening everyday in a real-world setting. Cyber-attack cards in event 1 allow a user to choose to attack any players landing upon an owned property. By this design, a player who is familiar with all cyber-security knowledge (in the game) should not be concerned regarding such an attack card. On the other hand, attackers should learn that there is an element of risk when starting a cyber-attack, both in the game and in reality. In order to stimulate a player's memory, not only the punishment and reward mechanisms as shown in red sentences on Fig.2(a-2), but also images representing specific attacks on the pre-marked board are formulated.

4 Results

4.1 Experimental Setup

An experiment was conducted on a set of 30 undergraduates and 2 academic professors teaching an 'Introduction to Cyber-Security' module in a Japanese university for 4 years. After learning the rules of play, students played "Cyberpoly" in pairs, while the two professors firstly were guided to add new questions through content management interfaces (as shown in Fig.1) to the game and then play against each other. Students were required to respond to a questionnaire consisting of 16 questions on 3 dimensions: Game mode, game design and system usability [7]. Response options are a seven-point Likert scale (1-3: strongly to slightly disagree, 4: neutral, 5-7: slightly to strongly agree). Additionally, students were asked 3 open questions for comments and suggestions in addressing these 3 dimensions. Academic professors were required to evaluate the game from a instructor's perspective, focusing not only on the content of the game, but also on the evaluation of the management system. Therefore, in addition to the first 3 questions related to game modes and a corresponding open question asking for suggestion addressing game modes (these 4 questions are the same as the first 4 questions in the questionnaire for students), a one hour in-depth interview was conducted, to collect more detailed feedback from the two professors.

4.2 Learner and Instructor Feedback

The first question asked for feedback on whether a single player mode would be useful for memorising questions and gameplay. The students' average rating of this question is 4.6 (S.D.=1.47). 4 student participants (2 strongly disagree, 1 disagree, 1 slightly disagree) mentioned that the single mode is similar with doing a exam, so it is not necessary; 16 student participants (2 strongly agree, 7 agree, and 7 slight agree) would still prefer a single player mode to practice alone first, prior to joining a multiplayer game mode, which is consistent with the opinion of two academic professors (both agree). In terms of the multiplayer game mode, the students' average ratings of question 1-2 (The ability for multiple players to play together in groups makes the game more enjoyable.) is 6.37 (S.D.=0.66) while the professors' ratings both at 5; and the average rating of question 1-3 (The ability for multiple groups to play the game at the same time is useful.) is 5.7 (S.D.=1.00) while the professors' ratings are both 5.

In terms of Educational element and game design feedback from students, the average rating of question 2-1 (The design of the game interface is attractive and appealing.) is 5.80 (S.D.=0.79); the average rating of question 2-1 (The game-play is fun and motivates the player to keep playing.) is 5.67 (S.D.=0.87) ;the average rating of question 2-3 (The system is useful because it can support learning some cyber security knowledge.) is 6.00 (S.D.=0.52). These suggest that most participants agreed that the game may assist in enabling motivation to learn cyber-security knowledge.

In terms of system usability feedback from students, the descriptive data is shown in Table 1. Among these 10 statements, questions 3-1, 3-3, 3-5, 3-7 are positive statements, which acknowledge the system usability, and the rest are negative statements. The average rating of the 5 positive statements is 5.83 ($>$ 4 (the neutral point); the average rating of the 5 negative statements is 2.63 ($<$ than 4 (the neutral point)).This suggests that most of student participants are satisfied with the system usability.

Given that the current interface allows addition, removal and editing of cyber-security events and questions, the professors identified several areas after being interviewed, which could enhance future iterations of the interface. Firstly, they requested the introduction of an AI player, to ensure that games are playable, without a human opponent. Secondly, they requested the addition of a spectator mode, to allow players, to view other tables without joining. This allows those who are unfamiliar with gameplay or lack security knowledge to learn from the perspective of bystanders. Regarding the educational elements and basic design of the game, the professors believed that the game may promote cyber-security learning; however, more attractive elements could be brought in the

Table 1: The descriptive data of rating of the system usability.

Question (id)	Mean	S.D.
3-1. I think that I would like to use this system frequently.	4.83	1.16
3-2. I found the system unnecessarily complex.	2.97	1.22
3-3. I thought the system was easy to use.	6.10	0.40
3-4. I think that I would need the support of a technical person to be able to use this system.	2.40	0.92
3-5. I found the various functions in this system were well integrated.	6.03	0.55
3-6. I thought there was too much inconsistency in this system.	2.43	1.05
3-7. I would imagine that most people would learn to use this system very quickly.	6.27.	0.51
3-8. I found the system very cumbersome to use.	2.07	0.68
3-9. I felt very confident using the system.	5.93	0.51
3-10. I needed to learn a lot of things before I could get going with this system.	3.30	1.19

game. Suggestions include the addition of features such as introduction of a mechanism that allow landlords to set up various in-game security devices to reinforce their lands. Regarding the design of the game, the professors agreed that it has a potential as a good platform for cyber-security learning, in particular, through the rule of attack cards (using a attack card whilst taking the risk of double payment).

5 Conclusion and Future Work

In this paper, we have proposed the MEMORABLE framework for multi-player customisable serious games in cyber-security and implemented an instance of this platform via the 'Cyberpoly' game, demonstrating how this approach increases the motivation of students. In summary, though triggering a variety of cyber-security incidents, using cyber-attack cards to attack other players, and responding to questions about cyber-countermeasures, the player of "Cyberpoly" would be able to learn knowledge about cyber-security in the game. By aiming to reach the in-game goal, players may achieve the real-life goal of acquiring new cyber-security knowledge. Further to this, the introduction of a management interface ensures that instructors may tailor the game to their module's content or player knowledge level.

The feedback from users suggests that the game achieves the goal of stimulating learning interests and motivating players to learn the cyber-security content, through rewards and punishment. Whilst successful, the current game state is relatively primitive and lacking in important features, such as features enabling interaction between players, promoting meta-knowledge about the learning process to the learner, and further flexibility, in terms of expansion of topics and content. Thus, we aim to implement communication functionality between learners in future iterations of the game. By discussing the tasks presented, learners may achieve further knowledge retention. Limitations to this work are presented through a focus upon the cyber-security field, however, the approach may be generalised to any educational domain through adapted placement of the game elements.

References

1. Cybersecurity investment 2020, https://www.canalys.com/newsroom/cybersecurity-investment-2020
2. Cybersecurity lab, https://www.pbs.org/wgbh/nova/labs/lab/cyber/
3. Cybersprinters: Game and activities, https://www.ncsc.gov.uk/information/cybersprinters-game-and-activities
4. Keep tradition secure, https://keeptraditionsecure.tamu.edu/
5. Targeted attack: The game – defend your data. choose wisely. succeed or fail., http://targetedattacks.trendmicro.com/
6. Uk national crime agency: Cybergames, https://cybergamesuk.com/cybergames
7. Brooke, J.: Sus: A quick and dirty usability scale. Usability Eval. Ind. **189** (11 1995)
8. Garzotto: Investigating the educational effectiveness of multiplayer online games for children. Proceedings of the 6th international conference on Interaction design and children p. 29–36 (2007). https://doi.org/10.1145/1297277.1297284, https://doi.org/10.1145/1297277.1297284
9. Kordaki, M., Gousiou, A.: Digital card games in education: A ten year systematic review. Computers Education **109**, 122–161 (2017). https://doi.org/https://doi.org/10.1016/j.compedu.2017.02.011, https://www.sciencedirect.com/science/article/pii/S036013151730043X
10. Laal, M., Ghodsi, S.M.: Benefits of collaborative learning. Procedia - Social and Behavioral Sciences **31**, 486–490 (2012). https://doi.org/https://doi.org/10.1016/j.sbspro.2011.12.091, https://www.sciencedirect.com/science/article/pii/S1877042811030205, world Conference on Learning, Teaching Administration - 2011
11. Lo, J.J., Kuo, T.Y.: A study of parent-child play in a multiplayer competitive educational game. 2013 IEEE 13th International Conference on Advanced Learning Technologies pp. 43–47 (2013)
12. Putz, L.M., Hofbauer, F., Treiblmaier, H.: Can gamification help to improve education? findings from a longitudinal study. Computers in Human Behavior **110**, 106392 (2020). https://doi.org/https://doi.org/10.1016/j.chb.2020.106392, https://www.sciencedirect.com/science/article/pii/S074756322030145X
13. Seah, E.T.W., Kaufman, D., Sauvé, L., Zhang, F.: Play, learn, connect. Journal of Educational Computing Research **56**, 675–700 (2018)
14. Shi, L., Cristea, A.I.: Motivational gamification strategies rooted in self-determination theory for social adaptive e-learning. In: International Conference on Intelligent Tutoring Systems. pp. 294–300. Springer (2016)
15. Storm: 90% of security incidents trace back to pebkac and id10t errors (2015), https://www.computerworld.com/article/2910316/90-of-security-incidents-trace-back-to-pebkac-and-id10t-errors.html
16. Toda, A.M., Oliveira, W., Klock, A.C., Palomino, P.T., Pimenta, M., Gasparini, I., Shi, L., Bittencourt, I., Isotani, S., Cristea, A.I.: A taxonomy of game elements for gamification in educational contexts: Proposal and evaluation. In: 2019 IEEE 19th International Conference on Advanced Learning Technologies (ICALT). vol. 2161, pp. 84–88. IEEE (2019)
17. Wendel, V., Gutjahr, M., Göbel, S., Steinmetz, R.: Designing collaborative multiplayer serious games: Escape from wilson island—a multiplayer 3d serious game for collaborative learning in teams. Education and Information Technologies **18** (2013). https://doi.org/10.1007/s10639-012-9244-6

18. Wendel, V., Konert, J.: Multiplayer Serious Games, pp. 211–241. Springer International Publishing, Cham (2016). https://doi.org/10.1007/978-3-319-40612-1_8, https://doi.org/10.1007/978-3-319-40612-1_8