Cyber-Detective - A Game for Cyber Crime Prevention

Inês G. F. Lopes[1] , Yuliya Morenets[3], Pedro R. M. Inácio[1,2], Frutuoso G. M. Silva[1,2]

[1]Universidade da Beira Interior,
[2]Instituto de Telecomunicações,
[3]TaC- Together Against Cybercrime

ABSTRACT

Technologies are increasingly becoming a part of the daily lives of younger generations and with no supervised usage of these technologies, teenagers are exposed to various threats. To raise the awareness of teenagers in ages between 14 and 17 years old, and to provide a methodological tool for educational professionals working with the young and even for enforcement professionals investigating the cyber cases, an educational game about cyber security was designed and prototyped.

A detective game was devised, where the player takes the role of a detective to investigate a cyber crime. To solve the case, the player must play several mini-games, where each one explores a specific thematic about cyber security. For example, in the prototype, the situation that the detective needs to solve is a ransomware case. The situations are introduced by a tridimensional animation, which appears as a cutscene introducing the game scene. It is an animation where one can see a teen trying to buy a pair of sneakers online and after downloading an application suggested in the website, his mobile phone is locked. Thus, he decides to search help from the police, where the detective will try to solve the problem. For that, the player has to solve several mini-games about sharing information in social networks, phishing and the importance of creating strong passwords. In these mini-games the player makes decisions and learns based on that, i.e., at the end of each mini-game each decision is explained to the player regardless of the choice being correct or incorrect. This way, the player is always informed of the various situations that can occur based on their behavior/decisions online.

The prototype was developed for mobile devices and some preliminary tests were performed with teenagers. The tests showed that the teenagers improved their cyber security knowledge after playing the game.

A cyber security educational game can be used as a tool for younger generations because it uses the technologies that are part of their daily lives and can contribute to the growing of their cyber security awareness.

In the future, we hope to develop the full game, where other thematic will be included, namely, talking with strangers in social networks, dangers related with the webcam and microphone, online piracy and cyber bullying.

Introduction

Nowadays, technologies are increasingly becoming a part of the daily lives of younger generations of our society. Since a young age, children have contact with devices such as smartphones or tablets and the virtual world, namely the Internet. When they reach adolescence, these young people have an active virtual life through their computers and mobile phones, and this is often not accompanied by their parents (sometimes because many of them do not keep up with technological advances). As such, these teens are exposed to various threats through their devices. However, the teenagers also learn a lot in the Internet, for example when playing some video games. While most of the games have the goal of amusing their players, Serious Games have a major purpose besides the entertainment - transmit knowledge. According to the Discovery Learning Theory of Jerome Bruner, students who engage on play-based learning activities (such as video games) experience increased motivation, enhanced problem-solving skills and a greater sense of personal responsibility, among other benefits (David L., 2017). While playing a Serious Game, these benefits can increase the learning ability of the player. As stated by Michael & Chen (2006), serious games allow "the player to not only learn, but to demonstrate and apply what he or she has learned", and this is one of the goals of our game.

A good game should lead the player to reaches the mental state of flow, i.e., when a person performing an activity is immersed with focus, involvement and enjoyment in the process of that activity, losing sense of space and time (Csikszentmihalyi, 1990). Reaching the state of flow in a certain activity makes it an "optimal experience", since the user gets a high gratification from it. In order to keep a person in the state of flow, the activity needs to reach a balance between the challenges of the activity and the abilities of the user. If the challenge is higher than the skills of the user, the activity becomes overwhelming and creates frustration in the user because it is too hard; if the challenge is lower than the ability of the user, the user gets bored because the activity is too easy (Nakamura & Csikszentmihalyi, 2002). A game that can maintain the flow experience in its players is a game that is more likely to succeed because it retains the players, something that our project wishes to achieve.

To educate the young and create awareness of the risks of using the Internet, there are several organizations and projects that focus on cyber security and create awareness between parents and educators. Together against Cybercrime International (TaC, 2016) is an example of one of these cyber crime fighting organizations. In the context of a collaboration protocol between TaC and the *Universidade da Beira Interior* (UBI) and to support the pedagogical actions on cyber security taken by this type of organizations or by educators, there was the intention to design and develop a smartphone video game addressing threats to which teenagers are exposed and to encourage a better online behavior.

The project main goal was to design and develop a video game prototype that reinforces the cyber security culture among young people and make them more aware of the risks and responsibilities online, eventually by turning them into active actors in the process. This prototype will serve as support for a complete game that will allow youngsters to take responsible actions on the Internet autonomously. A secondary goal was to define and apply a testing protocol to evaluate and fine-tune the game during field trials.

Related Work

Nowadays there is a considerable amount of video games on the cyber security subject. However, most of these games have a completely academic nature (for example, quizzes) and, from those that are not like that, there are several games that use cyber security as the theme but do not provide any kind of knowledge as collateral, being merely playful. In addition to these points, there is also the fact that most of these games target young children. The target audience of the current project is teenagers. Therefore, the way that the topics are addressed in some of these games is childish and demotivates older players.

Of the existing games on cyber security, there are several that can be taken as examples in the scope of our project. Three games that stand out from the others are presented in the following paragraphs.

The first game, Digital Compass (Common Sense Education, 2015), is a digital citizenship game devised for children from 9 to 12 years old. This game allows

players to impersonate young characters with computer problems. The player can guide each character through a story related to a theme of digital citizenship, making decisions that will influence the outcome of the story. At the end of each story there are mini games related to each theme. This game, although it is not addressed to the target audience of this project, should be considered as it allows the player to educate itself about digital citizenship through a real application of the theme and gives the player the possibility of taking its own safety choices digitally.

The second game, Digizen (Childnet International, 2016), is a game focused on cyber bullying, and unlike the game presented above, it targets teenagers. The player impersonates a character who attends a school where it is taught notions about online safety. In addition to some quizzes about the digital world, made to the player in the classroom, the main narrative of the game involves the friend of the main character, who suffers from cyber bullying. It is up to the player to make decisions in the game narrative, considering the problem of his friend. This game, as mentioned above, should be considered as it introduces good practices in proximity of a cyber bullying case through an interactive narrative, where the player learns from its actions.

Lastly, Cybersecurity Lab (WGBH Educational Foundation, 2014), is a game whose goal is to educate teenagers on the cyber security issue, giving the player the possibility to assume the role of a newly created social network worker, supervising its security. From the games presented, this is the game that best combines the theoretical part with the playful part of the game and that is more suitable for a teen audience. It consists of four mini games:

- Server Protection against Cyber Attack Game: when an attack of a certain type occurs, the player must protect the network of the company using the coins earned in other mini games. Each coin protects one of the 6 network ports. Each attack strikes the network in 3 aspects, each of them has two respective ports. The player must choose, using cyber security knowledge, the ports that he must protect to lose the minimum number of users. This game aims to test the knowledge of the player regarding cyber security flaws in computer networks;

- Programming Challenge: with the help of code blocks, the player must create a program that allows a figure to cross a map. This game aims to introduce programming logic in the player;
- Decipher Passwords Challenge: the player is challenged by a spy from within the company to a password battle, in each chooses a password and then tries to unravel the password of the opponent, following certain methods used by hackers (for example, using the list of the 10 most used passwords to try to compromise the password). This game instills in the player better practices in choosing a safe keyword;
- Social Engineering Challenge: in a game similar to a discover the differences one, the player must find the differences between e-mails, websites, etc. and phishing attempts. This game educates the player regarding phishing signals that may be found in suspicious e-mails, websites, etc.

This game should be taken as a reference for our game because, by placing the player in an active position of the cyber security department of a company, he tests his knowledge and learns about the subject. As mentioned before, it has a good playful component that takes this educational game to an exciting level for the player.

With the evaluation of some existing related games, it was possible to establish some guidelines for design and development of our game.

Cyber-Detective Game

The game devised aims to innovate in the cyber security area, as it will not merely be an educational game that focuses on testing the knowledge of the player through questions, like most games on the subject. It is envisioned the development of a game that, with an immersive narrative, makes the player an active character in decisions on the cyber security reality, using previously acquired knowledge and learning new things with the outcome caused by its decisions in the game. The game is committed to address the issue of cyber security applying it to real examples, so that the player can see himself in the situations and thus know the best practices to have. The game also wants to demonstrate to the young player that cyber crime is punished and that it is possible to punish cyber criminals.

The main audience of the game is teenagers, particularly young between the ages of 14 and 17. Considering this audience, the top games on platforms like Play-Store, Steam and Twitch were analyzed, as well as the paper that analyzed the most played games by students (Carvalho et al., 2014), to understand the gaming habits of the audience age group. Based on the results presented in the paper, it is possible to conclude that over 80% of surveyed secondary school students (ages 14 to 17 years old) would like to use games in school activities. It is also possible to analyze values from a survey about the preferred type of games for teaching subjects content. It was concluded that the favored three types of game that youngsters in this age group would most like to see in an educational game would be Strategy, Action and Adventure.

By investigating the target audience and its gaming habits, it was easier to pick the right direction to follow regarding the game type to develop.

"If we want to increase the appeal of our games, it is necessary to understand what makes an experience entertaining, and how such an experience can be created. The discipline that tries to answer these questions is called game design." (Jurie, 2007).

The main objective for our game was to offer the player an exciting experience while learning didactic content.

Bearing in mind the conclusions drawn from the analysis of the target audience about the preferred game types of teenagers for educational games, the three game types (Strategy, Action and Adventure) were combined, conceiving the idea for an investigation game, that would well fit in the cyber security theme. This investigation game will connect some cyber security issues and present them as a cyber crime. The player then assumes the role of a cyber-detective and, to help the victim of the crime should solve the case, winning some mini games related to some cyber security subjects. This strategy of using mini games to learn subjects was proposed by Barbosa et al. (2014), when they presented the learning mechanisms in the design and development of Serious Games. The full version of the game should contain numerous levels, each one representing a case. The full game should approach the many subjects of cyber security. The prototype developed represents one level of this complete game and should serve as a model for the development of other levels.

With the detective game concept mentioned, it was drawn the following list of stages for the unfolding of each case:

3. Introduction – animated cutscene illustrating the actions that led to a cyber crime;
4. Case Acceptance – in the cyber security department, the player, in the role of detective, accepts the case and objectives to accomplish (mini games);
5. Case Solving (mini games) – the player must solve some mini games to progress in the case solving;
6. Case Conclusion – Once all the objectives of the game are completed, a cutscene is presented, illustrating the resolution of the case.

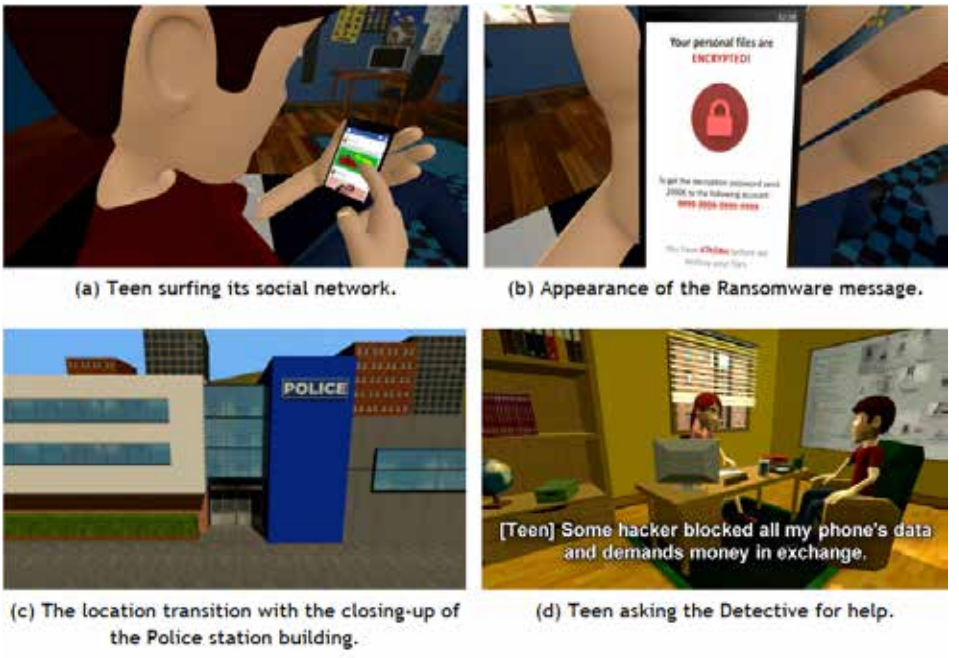

Figure 1 – Introduction of the case and case acceptance.

So, the game is an investigation/detective game that aims to educate teenagers about cyber security and it takes place at a police station, specifically in the cyber

security department. This department contains a waiting room, a common office, the office of the cyber-detective and a laboratory with some research rooms. Figure 1 a) and b) show the introduction of the case and Figure 1 c) and d) show the case acceptance by the detective.

Figure 2 – Layout of the cyber security department.

The game purpose is to solve cyber crimes resorting to cyber security themed mini games, available in the laboratory rooms (see Figure 2). To successfully solve the mini games, the player must use his knowledge about the themes. For the developed prototype, the main theme chosen for the cyber crime was ransomware. A storyline was then created up to connect crime with the stages of its resolution, then producing a story with logic. The plot is divided in two parts: the crime occurrence, at the house of the victim (a teenager), and its resolution, at the cyber security department. It was decided that the victim of the crime would be a teenager, so that the audience target of the game could relate to the character. The storyline of the crime occurrence, presented to the player as an animated cutscene, goes as follows:

1. A teenager boy surfs his social networks on his smartphone;
2. In the social network feed, he finds an ad for a website claiming to sell branded shoes at an incredibly low price;
3. The adolescent check the website and then decides to buy a pair of sneakers;
4. Before letting the teen advance with the purchase, the website proposes him to download an application in exchange of a 10% discount on the purchase;

5. Without suspecting, the teen continues with the download and installation of the application;
6. The teenager is surprised with a ransomware message;
7. The ransomware message claims to have encrypted all the device files and demands a large amount payment in exchange of the decryption password;
8. Frightened, the teenager decides to seek police help;
9. The teen goes to the cyber security department of a police station, explains the situation to the cyber-detective and asks for help and the detective accepts.

The storyline of the resolution of the crime has the following order of events:

1. The detective decides to analyze the social network of the adolescent to find the ad that led him to the malicious website; to achieve this, the player must complete the Social Network mini game, that tests the knowledge of the player on making secure choices in Social Networks (see Figure 4);
2. The detective then decides to investigate the suspicious website and its phishing signs to find out who might have created it; for that, the player must solve the Phishing Detector mini game, where the ability of the player to identify phishing signs on the Internet is tested;
3. With the suspect website creators and their info, the detective tries to discover the decryption passwords of the files; to achieve this, the player must complete the Password Decoder mini game, that allows the player to come across with weak elements commonly used in passwords;
4. After solving the three mini games, the detective manages to clear the ransomware off the device and decrypt the files; the smartphone is returned to the teen (displayed to the player through an animated cutscene).

With the game design defined, it was possible to develop the prototype of this level of the game, as shows Figure 3.

Figure 3 – Interface of the game.

Figure 4 – Layout of the Social Network mini game.

Tests and Results

To evaluate the quality of the prototype developed, some tests were implemented with the target audience of the game. The tests were applied in *Escola Secundária do Fundão*, to a 9th grade class, with 14 students with ages between 14 and 17 years old, where 6 of them were boys and 8 were girls. The students were submitted to a knowledge quiz twice: once before playing the game (pre-quiz) and once after playing it (post-quiz). The students were observed while playing the game and making some comments about their experience. After playing, the students also answered a questionnaire to evaluate the game and their usability experience. With the results from the knowledge quizzes, it was possible to analyze the improvement made by the students after playing the prototype.

Usability Tests

The questionnaire answered by the students approached four different subjects: the flow of the game, the thematic of the game, graphics and mini games, and didactic. The teenagers evaluated the game on these topics answering questions based on a Likert Scale.

Analyzing the evaluations made to the flow of the game, as seen in Table 1, it is noted that the students had some difficulties in understanding which were the correct actions to complete the tasks. This may have happened due to the language of the prototype, because not all the students were comfortable with the English Language.

Table 1 - Flow of the Game Evaluation

Flow of the Game	Disagree	I do not agree or disagree	Agree
I always understood what the task was.	0	5	**9**
I have always found the right action to take, effortlessly.	3	**6**	5
I always realized that performing certain action would complete the corresponding task.	1	5	**8**
I was always aware of the progress made when completing tasks.	0	3	**11**

About the evaluations made to the Thematic of the Game, summarized in Table 2, it can be concluded that almost a third of the students seems to have no awareness of all the dangers they face online every day, since they stated that they did not deal with the themes of the game on their daily life, although the answers to the questions "I use a smartphone/the Internet/social networks everyday" were so positive. The results also show that the students are concerned about cyber security and the dangers of the Internet. With these results, it can be concluded that, even with lack of knowledge, this age segment is worried and interested in cyber security, making it the perfect audience target for the current game.

Table ***2*** - Thematic of the Game Evaluation

Thematic of the Game	Disagree	I do not agree or disagree	Agree
I use a smartphone every day.	0	1	**13**
I use the Internet every day.	0	1	**13**
I use social networks every day.	0	2	**12**
I was always aware of the progress made when completing tasks.	1	2	11
The themes of the game are something that I deal with in my daily life.	1	5	**8**
Cyber security and the dangers of the Internet are something that worries me.	0	2	12

Analyzing the evaluations made to the Graphics and Mini Games, as seen in Table 3, it is possible to observe that the students were pleased with the game graphics and mobility. The mini games evaluation results show that the mini games of the prototype were not too difficult nor too easy. With these values, it can be concluded that overall the difficulty of the mini games is well-balanced.

Table 3 - Graphics and Mini Games Evaluation

Graphics and Mini Games	Disagree	I do not agree or disagree	Agree
The game graphics were adequate.	1	1	**12**
I understood the plot of the game.	1	2	**11**
The mobility in the game was good.	2	3	**9**
The social networks mini game was difficult.	5	**7**	2
The phishing mini game was difficult.	5	**8**	1
The passwords mini game was difficult.	3	**6**	5

About the evaluations made to the Didactic of the Game, summarized in Table 4, it is possible to conclude that overall the students learned about cyber security with the game and would willingly play a full version of the game conceptualized. It is also possible to observe that the students think that learning about cyber security with a video game is appealing, comparing to the typical teaching methods.

Table 4 - Didactic Evaluation

Didactic	Disagree	I do not agree or disagree	Agree
This game taught me about the topics approached in the game.	0	3	**11**
I think this type of game suits the theme.	0	1	**13**
I would like to play a full version of this game to learn more about cyber security.	0	2	**12**
I would rather learn about cyber security with a video game than with lectures/videos/classes.	0	2	12

Lastly, the questionnaire had two open questions, "Have you found any problem in the game?" and "Which improvements would you propose for the game?". Regarding the problems found, two students found a bug that allowed the detective character to walk through a wall. This bug was identified and corrected. Regarding the second question, the students pointed some improvements that could be implemented in the prototype, such as that the detective character could walk faster, that the buttons of the game could be bigger, an improvement of the camera movement near walls or the addition of a "Skip Intro" button, for example.

Education Efficiency Tests

Since the game of this project is an educational game (i.e. a Serious Game), it was imperative to evaluate the efficiency of its educational component. The students answered a knowledge quiz with questions about ransomware, phishing signs, passwords and social network security, themes approached by the game. To evaluate the growth of the knowledge of the students, the students were asked to take this quiz twice, once before playing the game and once after playing, and the results of both quizzes were compared. Regarding the comparison of the results for each question, as seen on Table 5, the two questions that got the worst results in the second round of the quiz were a question to evaluate if a screen was a phishing attempt and a question asking if it was safe to post a picture of a football player in a social network. In the question to evaluate if a screen was a phishing attempt, the screen presented was not a phishing attempt, just a simple bank account e-mail. Although that, the students were more hesitant regarding this question in the second take of the quiz. The question asking if it was safe to

post a picture of a football player in a social network had a positive answer, it is safe to post a simple picture of a football player. In spite of that answer, in the second take of the quiz, the students seemed more unsure of the safety of the post.

Opposing the results of the phishing question above, the question that had the better improvement rate was a similar phishing question, in which the screen presented is an e-mail with a phishing attempt. The combination of the results of these two questions conclude that the students were more aware of phishing attempts through e-mails after playing the prototype and were overly cautious about them.

The second question with better improvement asked the student to pick the safest password of a list. The improvement of the score of this question shows that the students improved their capacity of identifying a safe password.

Table 5 - Quiz Scores Improvement per Question

	Quiz Questions							
	1	2	3a	3b	3c	4a	4b	4c
Pre-Quiz Results	21%	50%	100%	64%	100%	64%	100%	100%
Post-Quiz Results	36%	71%	100%	79%	100%	79%	100%	100%
Improvement	15%	21%	0%	15%	0%	15%	0%	0%
	5a	5b	5c	6a	6b	6c	7	8
Pre-Quiz Results	50%	64%	86%	50%	100%	79%	28%	11%
Post-Quiz Results	64%	64%	71%	93%	100%	57%	33%	32%
Improvement	14%	0%	-15%	43%	0%	-22%	5%	21%

Overall, it was possible to verify an improvement of the quiz scores, as seen in Table 6, where each row of the table represents a student of the class. The scores of the quiz improved on average nearly 7%. With these results, it is possible to conclude that the education component is efficient, since the students improved their knowledge on the subject. Although the language of the game, i.e. English Language, may not helped to achieve better results for some students.

With the results from the tests implemented with the target audience, it was possible to conclude that teenagers are sometimes unaware of the cybernetic

dangers that they might encounter in their daily life. However, these young students showed interest in learning about the subject to be safer, supporting the purpose of this game. It was also possible to verify an improvement of cyber security knowledge on the teenagers after playing the created game, confirming that this game can be used not only as a game, but also as a learning tool.

Table 6 - Ordered Quiz Scores Improvement

Pre-Quiz	Post-Quiz	Improvement of each student (Ordered from low to high)
68,8%	67,7%	-1,0%
83,3%	83,3%	0,0%
58,3%	58,3%	0,0%
58,3%	59,4%	1,0%
78,1%	80,2%	2,1%
77,1%	83,3%	6,2%
71,9%	78,1%	6,3%
51,6%	58,2%	6,6%
68,8%	76,0%	7,3%
56,3%	63,5%	7,3%
71,9%	83,3%	11,5%
60,4%	71,9%	11,5%
52,1%	70,8%	18,8%
78,1%	96,9%	18,8%
66,8%	73,7%	**6,9**%

Students Results

Average

Conclusions and Future Work

It was possible to conceptualize the idea for a cyber security detective game for teenagers and to develop a prototype of a level of that game, in the English language. The prototype was developed in Unity 4.2.2 to be available for different platforms. The prototype was tested with a group of teenagers (representing

the target audience) and was proven to improve the cyber security knowledge of teens, making it a suitable base for a full game of the conceptualized idea.

Although the main goal of the project was achieved, the developing of a prototype, there are some improvements that can be applied to the prototype. Following are some proposed improvements for the prototype, such as the addition of sound and music to the cut scenes and game, a better flow of the game for the understanding of the player and the addition of multiple languages, for example. The support for other languages, as for example the Portuguese and French languages, is an important aspect, because some students in the tests showed some difficulties with the English language.

In the future, we hope to develop the full game, where other thematic will be included, namely, talking with strangers in social networks, dangers related with the webcam and microphone, online piracy and cyber bullying.

Acknowledgment

This study was carried out within the scope of R&D Unit 50008, financed by UID/EEA/50008/2013.

References

Barbosa, A. F., Pereira, P. N., Dias, J. A., & Silva, F. G. (2014). A New Methodology of Design and Development of Serious Games. International Journal of Computer Games Technology. Retrieved September 24, 2017, from http://www.hindawi.com/journals/ijcgt/2014/817167/

Carvalho, A. A., Araújo, I. C., Zagalo, N., Gomes, T., Barros, C., & Cruz, S. (2014). Os jogos mais jogados pelos alunos do Ensino Básico ao Ensino Superior. Retrieved January 14, 2017, from http://jml.fpce.uc.pt/pub/2014_Os_jogos_mais_jogados_2C EB_ES_ejml.pdf

Childnet International. (2016). Are you a responsible digital citizen? Retrieved January 6, 2017, from http://www.digizen.org/resources/cyberbullying/interactive/

Common Sense Education. (2015). Digital Compass. Retrieved January 6, 2017, from https://www.brainpop.com/games/digitalcompass/

Csikszentmihalyi, M. (1990). Flow: The Psychology of Optimal Experience. Harper and Row.

Jurie. (2007). Why Game Design Is Important. Retrieved August 21, 2017, from http://www.intelligent-artifice.com/2007/10/why-game-design-is-important.html

L., David (2017). Discovery Learning (Bruner), in Learning Theories, February 2. Retrieved October 1, 2017, from https://www.learning-theories.com/discovery-learning-bruner.html

Michael, D., & Chen, S. (2006). Serious Games: Games That Educate, Train, and Inform. Thomson Course Technology PTR.

Nakamura, J., & Csikszentmihalyi, M. (2002). The concept of flow. Oxford University Press.

TaC. (2016). *TaC Together against Cybercrime International*. Retrieved January 14, 2017, from https://againstcybercrime.org/

WGBH Educational Foundation. (2014). Cyber Lab. Retrieved January 6, 2017, from http://www.pbs.org/wgbh/nova/labs/lab/cyber/research#/newuser