International Journal of Security and Its Applications
Vol. 10, No. 5 (2016) pp.165-180
http://dx.doi.org/10.14257/ijsia.2016.10.5.16

A Cybercrime Prevention Program based on Simulation and Quiz Game: Applying Item Response Theory for Effective Information Security Learning

Su Ryeon Kim[1], Ji Hyeon Yang[1] and Seong Baeg Kim[1,1],

[1] *Dept. of Computer Education, Jeju National University, Jeju-do, Republic of Korea*
rus1031@gmail.com, llyyyy@hanmail.net, sbkim@jejunu.ac.kr

Abstract

Recently, as utilization rate of the Internet gets higher, cybercrime rates are growing up. In order not to be damaged from such cybercrimes, the importance of an education for protection from them is increasingly critical. However, the existing information security educations have not been enough to deal effectively with rising cybercrimes. To tackle the problems of the existing educations, in this paper, we examine a way to prevent cybercrimes using learning contents related to a real life, help learners to improve awareness of cybercrimes and realize their seriousness through an indirect experience of them. We develop a program with learning contents based on a simulation for preventing cybercrimes. Furthermore, we provide a quiz game to enhance the understanding of the cybercrimes. After learning through the quiz game, the learners can check and extend their knowledge of preventing the cybercrimes. Specifically, each learner can identify vulnerable cybercrime types and get the proper feedbacks for preventing them through the analysis of learner's own correct/wrong answers.

Keywords*: Simulation, Information Security, Item Response Theory, Quiz Game, Feedback, Academic Achievement*

1. Introduction

Nowadays, the Internet has a large impact in every field. As time passes, the influence of the Internet is growing up because people are using more and more a banking service based on the Internet for financial transactions. In proportion to the growth of Internet usage, the cybercrime rate related to the Internet is also increasing. Particularly, according to 2013 Norton Report of Symantec, it was found that the monetary damages per each person caused by cybercrimes have increased about 50 percent from 197 dollars to 298 dollars, with cybercrimes rising up across the world [1].

The importance of information security education is growing in response to the increase of cybercrimes. However, the existing information security educations in schools has not been effectively provided with appropriate learning materials enough to make learners prevent cybercrimes and realize their seriousness. In case of South Korea, a close look at the contents of the information security section of the textbooks published reveals that most of them put emphasis on viruses and hardly include information protection or hacking. So, they are inappropriate to provide a balanced education to students. Therefore, to carry out the systematic information security education in schools is not plausible [2].

However, if the secondary school students, who are exposed to various cybercrimes, want to be protected from security threats, they must get the precise information for

[1] Seong Baeg Kim (sbkim@jejunu.ac.kr) is the corresponding author of this paper.

ISSN: 2005-4262 IJGDC

cybercrimes and handle properly them. The information security education in schools, which play the role of providing accurate information, must inform learners of a method to prevent the cybercrimes related to real life.

Therefore, in this study, by targeting the secondary students, we aim to develop an effective program of providing accurate security information and increasing the security awareness through indirect experience activities related to the cybercrimes. We revised and extended our existing research related to information security [17].

After learning, by practicing a quiz game in cooperation with other learners, they can check and extend the knowledge that they have learned. After finishing the whole process of learning activities including the quiz game, learners are able to check the weak security types by themselves through the analysis results of correct/wrong answers of the quiz game, and get a proper feedback to make up for the weakness.

2. Theoretical Background

2.1. Case-based Learning

Case-based learning is a teaching method to make students solve a new problem, based on the successful experiences that have been used to solve a problem from the past.

Let's look at previous studies about an effectiveness of case-based leaning as in the following. There have been researches on the effectiveness of the case-based learning [3][4][5]. The features of the case-based learning are as follows. First, it can be easily applied to a similar situation. Second, during the learning process, it can bring the continuous participation of learners and draw their motivation in solving problems. Third, it can make learners learn by placing them in specific situation occurred actually in the past and letting them experience it and then make them construct a new knowledge in relation with the valuable information of the previous cases.

Finally, it can be called ‘Actionable Learning’, which helps learners to enhance problem solving abilities and collaborative skills. Therefore, in this study, we exploit the primary advantages of the case-based learning for the purpose of preventing cybercrimes. We will propose the learning to let learners experience cybercrime cases that occurred in the past and prevent a new cybercrime through the learning of the similar incidents.

2.2. Simulation

Generally, a simulation is intended to let us manipulate and experience a situation that we can’t face with under a real world. In an educational perspective, the simulation is a tool that provides a situation similar to the real world to achieve an educational goal [6].

Through such simulation, actual dangerous situations can be learned in a safe way and the controlled experiments like selecting and repeating the necessary portion, which are impossible in a real world, can be provided [7].

Depending on learning objectives, types of simulation can be classified. Alessi and Trollip(2001) categorized them into four types: physical, procedural, situational, and process simulation[16]. Chul Il Im and Yeun Kyung Yeon described the four simulation types and the situational simulation among them is as follows: Situational simulation is a program that students can learn an attitude or behavior change. Through this program, they are able to solve problems given in the contexts of social relations by making them experience various roles based on the role-playing scenarios [7].

In this study, learners who become the main character of a learning scenario, experience the previous cybercrimes indirectly under the scenario reflecting those cases that occurred in real life and resolve a new cybercrime given.

2.3. Edutainment

Edutainment is a concept commonly called software and web site that can learn with fun. There is a typical example of edutainment such as learning a math formula through a game or simulating a scientific experiment on a game web site [8].

Especially, an educational game based on a simulation is possible to highlight an association with real life to learner and enhance learning motivation [9]. Therefore, we assumed that learning could be effective if a learner solves problems given through edutainment.

2.4. Item Analysis

Item response theory is a theory that analyzes the feature of each item rather than estimates a capacity of a learner by analyzing the total score of the items [10]. The item response theory has a unique characteristic curve per each item. Although each item has a different level, it is possible to identify consistently a learner's ability regardless of the difficulty degree of an item using the theory. In the program we developed in this study, according to the item response theory, when evaluating a learner, we put more credit to a learner who replies correctly to more difficult item.

3. Related Research

3.1. Research Trends

A survey on researches related to existing information security educations is as follows.

Table 1. Research and Development Trends

Title	Learner	Learning contents
Design and implementation of a courseware for database security learning[11]	Vocational high school student	• The concept of object • The concept of rights • Authorization method • Rights termination method • Understanding the playing role
Design and implementation of a situational simulation learning model for information security training in secondary schools[12]	Middle school student	• The basic concept of information security • The concept of virus • The concept of network security • The concept of copyright
Design and implementation of web-based educational contents for information security using XML[13]	Secondary school student	• The basic concept of information security • Virus and vaccine • Using Internet safely • Cyber ethics
Design of an information security simulator for educating encryption principles [14]	Middle school student	• Understanding encryption principles

Development of a procedural simulation-type courseware for information security education in secondary curriculum[15]	Middle school student	• Password security • Handling malwares • Handling e-commerce frauds

In case of the design and implementation of a courseware for database security learning by targeting vocational high school students, the courseware was developed to enable learners to visually learn a portion that is difficult to understand with only theory.

In case of the design and implementation of a situational simulation learning model for information security training in secondary schools, the learning proceeds to show learning contents with Flash.

In the case of web-based educational content of youth information security design and implementation, targeting youth, by using XML, depending on the individual's abilities, this educational content enables learners to study step by step using videos. During practice, learners can directly experience situations related to learning contents.

In the case of Information Security simulator designed for a encryption principle education, targeting middle school student, by using a simulator, it is possible to understand the principles of each encryption method. Solving problems proceeds by method of inputting commands and then the commands are stored in a record so that a professor can check later.

In the case of procedural simulation type courseware development for information security education in secondary education, students can learn how to prevent against security attacks by experiencing what kinds of damages occur from each of them through simulation-based training that targets middle school students.

3.2. The Problem of the Existing Information Security Learning Researches

Existing information security learning researches were classified into case-based learning content, learning method, evaluation method, and with or without a feedback.

Table 2. Characteristics of Previous Information Security Researches

Title	Case-based learning content	Learning method	Evaluation method	Feedback (achievement degree)
Design and implementation of a courseware for database security learning[11]	X	O	X	X
Design and implementation of a situational simulation learning model for information security training in secondary schools[12]	X	△	X	X
Design and implementation of web-based educational contents for information security using XML[13]	X	O	X	△

Design of an information security simulator for educating encryption principles [14]	X	O	Δ	X
Development of a procedural simulation-type courseware for information security education in secondary curriculum[15]	O	O	X	X

In the previous information security learning research, there were little learning cases with an example of showing an actual incident that occurred in a specific accident and there didn't exist learning the principles of why the damage occurs either. It is inappropriate for learners to prevent incidents that can provoke damage in real life, because learning contents are biased to the definition of words and consist of a high-quality technology suitable for practitioners.

Learning content and assessment also is not interrelated and thus it is not enough to attract the interest of learners. Furthermore, there are many cases that an evaluation method is not provided. In addition, it is difficult to identify learners' achievement due to the absence of storing their information and later they have trouble in reviewing what they have learned.

Therefore, in this study, based on damage cases of cybercrimes, we describe the principles of bringing the damage and methods of preventing it, and we let learners naturally participate in an evaluation process of being assessed by a game. After learners do the evaluation game, we intend to make them identify their vulnerable points by analyzing their item responses.

4. Design

4.1. Game Scenarios & Story Composition

When the program starts, a learner hears a story of a postman owl in the game. The postman owl must deliver mails related with learning contents, which are selected by the learner, to the village. But, villains as a character who symbolize cyber-crimes appear on the way to the village. Because the villains hinder the postman owl from entering into the village, he must defeat them in order to safely deliver the mails. He asked the learner to deliver the mails, because he can't deliver them due to an injury of his wing. The learner promises to help him and hears from him about how to beat the villains. The learner can naturally learn a defensive method against the villains because the way to beat the villains corresponds to preventing cybercrimes. After listening to the postman owl about how to defeat the villains, the learner starts to go to the village. The learner meets a captain villain who plays a role of a cybercrime type and his subordinates on the street under way and the learner should reach to the captain villain by avoiding safely the subordinates. If the learner eventually reaches to him by passing successfully through them, the learner must solve all problems asked by the captain villain. After the learner defeats him by answering correctly them, the learner can deliver the mails to the village safely.

A. Flowchart of the Overall System

The overall system flowchart of the program is as follows:

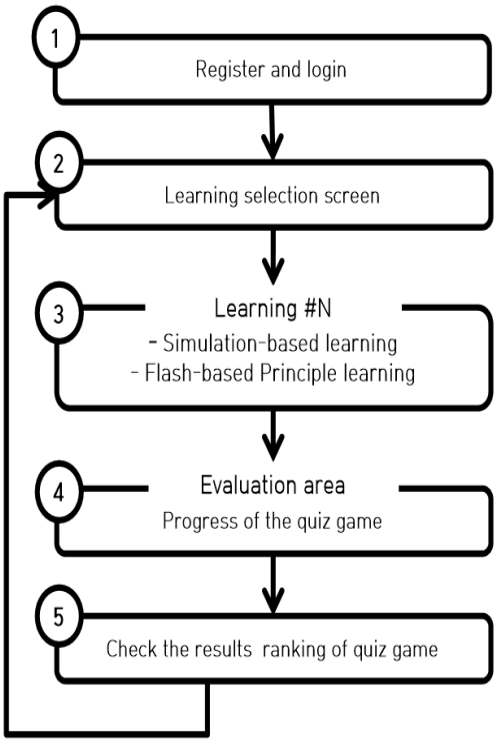


Figure 1. Learning Flowchart

4.1.1. Register and Login

To continue the learning in succession and store a learner's achievement, a learner has to log in and connect to the program.

4.1.2. Learning Selection

A learner selects the learning content that the learner wants to study.

4.1.3. Learning

After a learner, who selects learning contents, experiences the damage cases of indirectly corresponding to them, the learner becomes to learn the principles that result in the damages and a preventive method using a Flash animation.

4.1.4. Evaluation Area

A learner would be tested through a quiz game made with the related learning contents, after the study is finished.

4.1.5. Quiz Game Results

A learner can check his/her own ranking by scoring the correct answers to items after the quiz game is over. Types of quiz games are as follows.

- Determining true or false
- Choosing an option only stated correctly among multiple options
- Putting together in order

- Finding out words related
- Answering shortly

The items of a type of determining true or false present a statement that can be identified into true or false. The items of a type of choosing an option only stated correctly among multiple options consists of mixture of one true and three false statements and a learner should select the true one. The items of a type of putting together in order are to re-arrange principles of causing damage correctly step by step. A learner should always put them carefully in sequence because the sequence can be changed each time. The items of a type of finding out words related questions are to draw a common concept from the words presented. The items of a type of answering shortly are to submit the answer of a short form to an item given.

We set an evaluation method for scoring a quiz game of being tested during learning, based on 'item response theory'. In our evaluation method, we put more weight through item response theory as the percentage of the correct answer is lower. As a result, a learner who answers correctly to an item that the correct answer rate becomes low, can obtain a higher score using the following formula:

$$\left(\frac{Time\ Limit}{Time\ limit - Remaining\ time} + Weighted\ Difficulty\ Degree\right) \times 10$$

The formula for calculating a score for each item, is given as above. To obtain high scores, a learner must solve items as quickly as possible within limited time and answer correctly to more difficult items.

To determine the percentage of correct answers that represents the degree of difficulty, we put a weighted credit to more recent correct answer than older one. The formula is as follows.

$$\text{Correct answer rate} = (1-\alpha) \times \frac{No.of\ the\ correct\ answer\ out\ of\ the\ past\ items\ +\ \alpha \cdot \beta}{(1-\alpha) \times No.of\ items\ tested\ in\ the\ past\ +\ \alpha \cdot 1})$$

, where $\alpha = 0.2$ and $\beta =$ Answer or not of the corresponding item

We put proper values about the weight of the degree of item difficulty on the basis of Sungtaeje's item classification method as Table 3 shows.

Table 3. The Weights of the Degree of Difficulty according to the Correct Answer Rate

Correct answer rate x	Difficulty weights
$x < 0.3$	5
$0.3 \leq x < 0.8$	3
$0.8 \leq x$	1

Depending on the percentage of correct answers x, items are classified into difficult one if x is less than 0.3, intermediate one if x is ranged from 0.3 to 0.8, and easy one if x is more than 0.8 [10].

Accordingly, we set the weighted value 5 in case of difficult one, 3 in case of

intermediate one, and 1 in case of easy one.

B. Detailed design

The detailed design of a learning part is as follow.

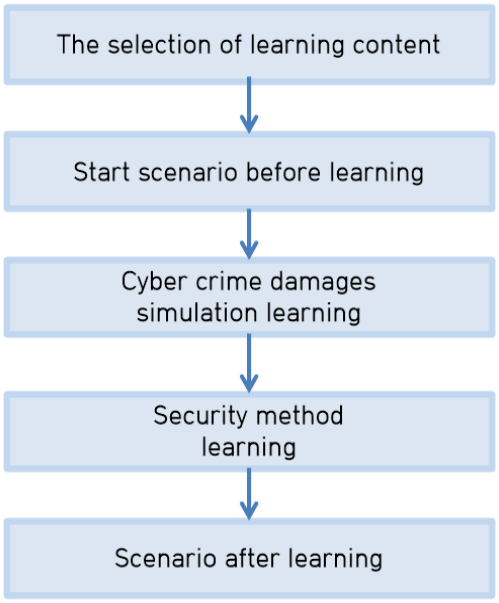


Figure 2. A Detailed Design of a Learning Part

If a learner logs in after user registration, the learner can see a screen to select learning contents. Thus, in the screen, the learner can choose the learning contents that he/she wants to learn.

Then, along the learning scenario, the learner accepts the owl's request and starts learning with listening to the owl's explanation. The learner experiences cybercrime cases indirectly through simulation and gets to know preventive methods of the cybercrime cases.

The detailed design of a game part is shown in Figure 3. Based on the scenario, the learner who finished the learning part explained by the owl, meets the captain villain and his subordinates who play roles of types of cybercrimes and then starts a mini-game that reaches the captain by passing though his subordinates without damages. If the learner fails to pass through the subordinates in the mini-game, a HP (health point) of the learner is diminished. If the HP becomes 0, the learner must determine whether he/she tries again or not. If the learner reaches safely the captain villain, he/she must solve a quiz asked by the captain villain. A series of process is repeated until the learner solves all the given items, If the learner have solved all of them, it is possible to see his/her ranking and to return to the main screen.

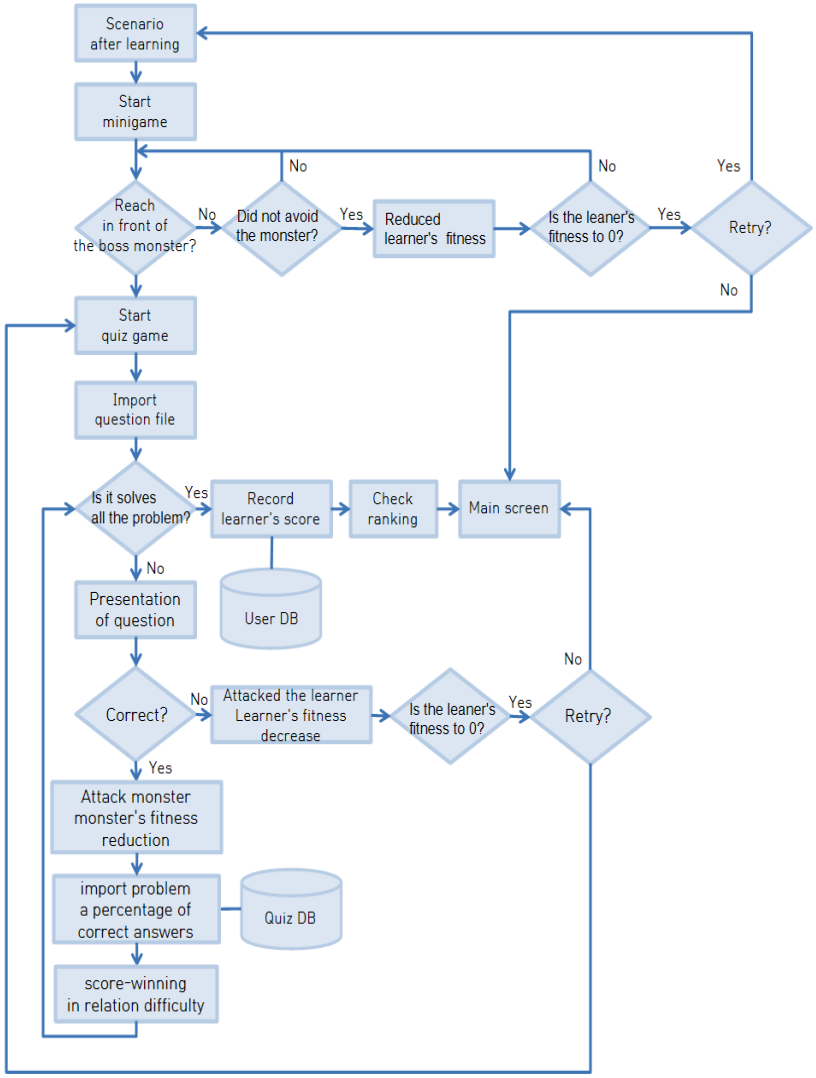


Figure 3. The Detailed Design of a Game Part

5. Implementation

5.1. Implementation Environment and Contents

The program was implemented using Visual Studio 2013, Adobe Flash Professional CC 2014, and Microsoft SQL Server 2012. The basic program operates based on a form of C# and Flash is used for showing graphical elements like the effect of simulation and quiz game. User information, quiz information, and item analysis information are managed by Microsoft SQL Server.

5.2. Implementation Results

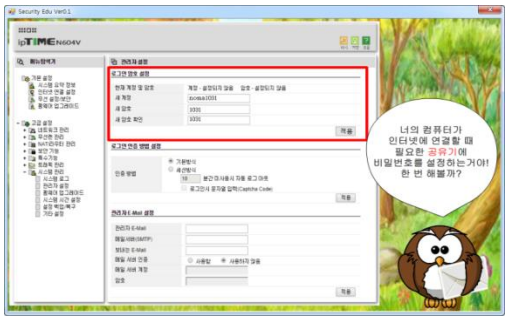
The primary screenshots of the program are shown in Figure 4. Each screenshot represents a primary stage to come up when a learner executes the program.

A learner, depending on learning contents, must go to the village to deliver mails in place of the owl.

The owl tells a learner the reason why he has injured his wing and asks the learner to deliver the mails to the village. But, in addition, he cautiously tells the learner that villains, who play roles of various cybercrimes, will appear during the period going to the village.

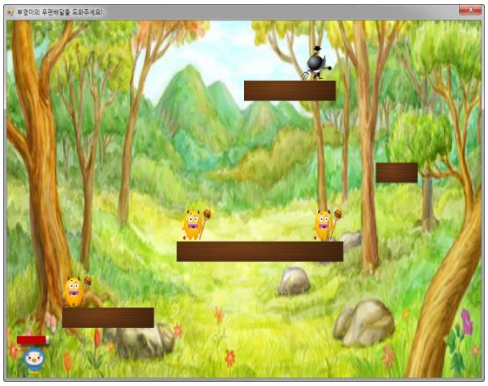
A learner learns a way to defeat the villains who characterize cybercrimes, and deliver mails safely.

A learner learns the principle of incurring a cybercrime damage using a learner-friendly and easy expression.

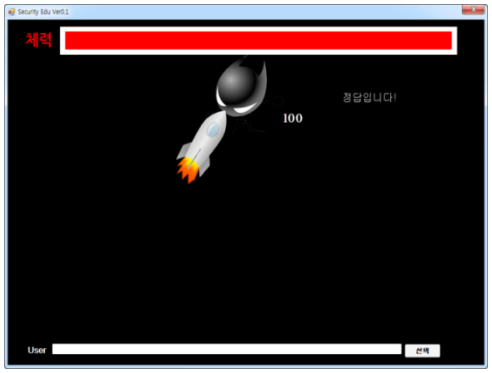


A learner learns how to prevent cybercrime damages. At this time, the learner participates in learning by clicking the screen interactively following a guide.

A learner meets subordinate villains of the captain villain on the way to the village for mail delivery.



A learner should approach a captain villain passing evasively through his subordinates.



A learner solves a series of quizzes and eventually defeats the villains who characterize a type of cybercrimes.

After defeating villains, a learner finally reaches the destination village along the scenario described above.

After finishing the game successfully, a learner gets the score reflecting item response theory and then the learner can check it.

Figure 4. The Primary Screenshots

6. Analysis

6.1. The Outline of the Survey

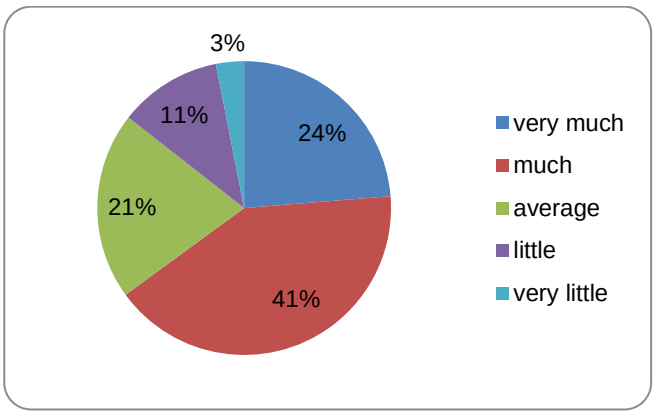
We surveyed a group of students who range largely from primary students to undergraduate students. The group size was 34 and we selected the students randomly.

6.2. Analysis Result after using the Program

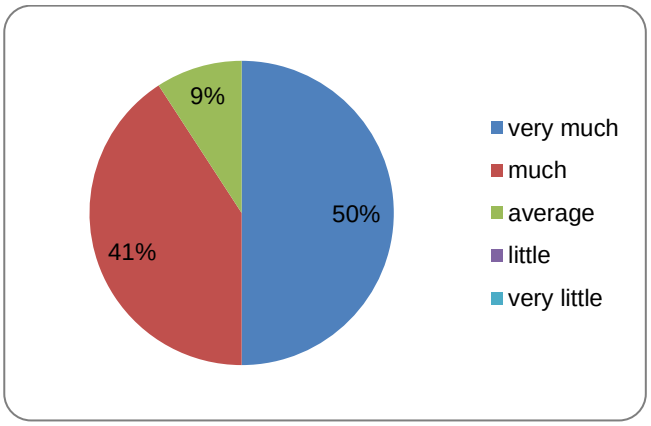
The questionnaire consists of three parts: items to compare before and after learning in order to find the learning effect, items to ask about learning content and game difficulty, and an item to ask whether a learner becomes to show into action to prevent a cybercrime in cyber activities in the future after the learning.

As the first part, the questionnaire items and the survey results are at the following.

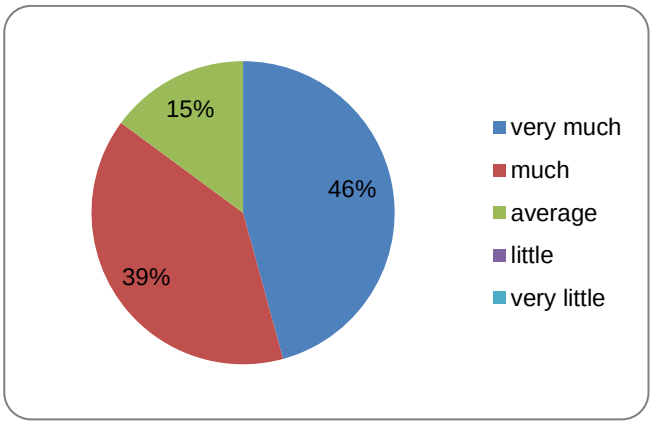
1) Before knowing this program, have you ever heard of cases of the cybercrimes appearing in the learning contents of the program?



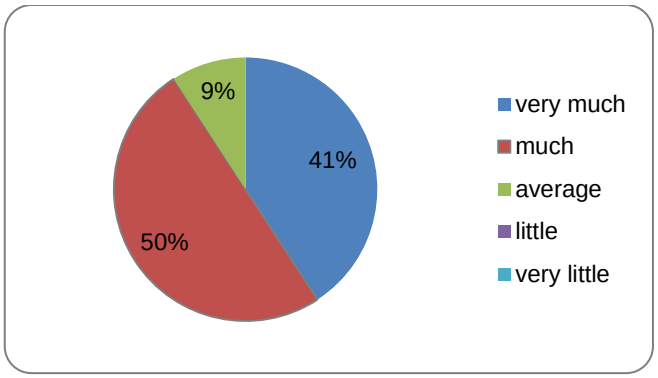
2) After using this program, did you easily understand a damage case by a cybercrime and how to prevent it?



3) After the learning, did you recognize seriousness of cybercrimes?



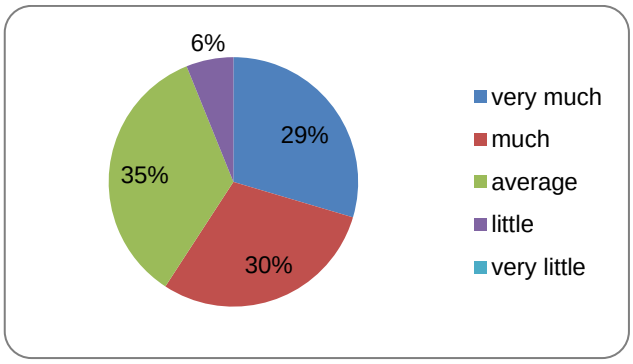
4) Did you have supplementary lessons through this game?



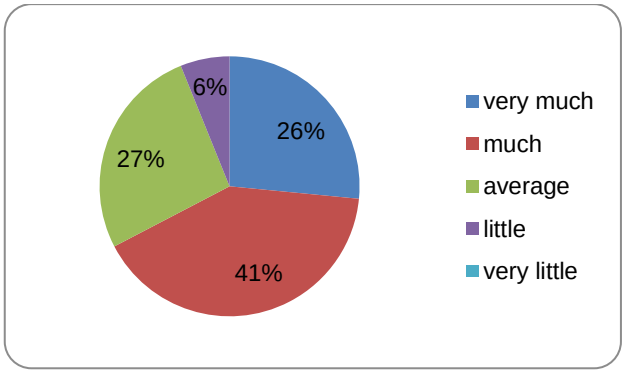
Before the learning, when it comes to awareness of cybercrimes, 34 percent of the students have heard of only types of cybercrimes and the rest of them have understood roughly about cybercrimes. After learning the definitions and damage cases of cybercrimes, the 86~91 percent of the students got to know the seriousness of cybercrimes. Also, the 91 percent of the students answered that they have extended their knowledge lacking in the learning contents through the game. As a result, we find that the students learned exactly the definition of a cybercrime, the principle of incurring a damage of a cybercrime, and how to prevent it, and they have gotten to realize the seriousness of a cybercrime.

As the second part, the items about difficulty of learning and the survey results are at the following.

5) Is the level of the learning contents appropriate for middle school students?



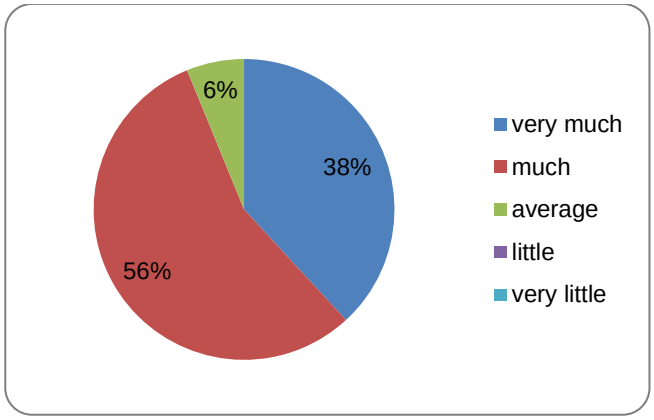
6) Is the degree of difficulty of the quiz game appropriate?



The 58 percentage of the students answered that the degree of difficulty of this program is appropriate at middle schools. The 66 percentage of the students answered that the degree of difficulty of the quiz games is appropriate. Because an adequacy of the difficulty appeared slightly more than 50%, it is necessary to lower a bit the difficulty of learning contents and quiz games.

Finally, an item to ask whether a learner becomes to show into action to prevent a cybercrime in cyber activities in the future after the learning and the surveyed analysis are at the following.

7) Are you going to show into action a security method based on what you've learned so far?



All of the students answered that based on what they have learned, they will show in a manner to prevent a cybercrime. This is because students recognize seriousness of cybercrimes and consider that the cybercrimes should be prevented. Therefore, we find that learners obtained positive effects through this learning program.

7. Conclusion

Learners are able to learn about information security effectively through this program. Analyzing the questionnaire, learners who select learning types that they want to learn, were aware of the seriousness of actual cybercrimes by experiencing them indirectly. After the learning, they would apply information security measures to real life, based on the learning contents. In order to adjust a difficulty level of learning contents to middle school students who use this program, we made the story in a way of helping the mail delivery of the 'postman owl'. Also, we let the students solve problems of the quiz games in order to defeat the villains that characterize types of the cybercrimes. Therefore, the degree of understanding is adequate for the students and they can expand further the contents that they have learned, through the quiz games. However, there were still many answers that it is necessary to adjust the difficulty of learning contents and items of the quiz games. Later, we have to lower the degree of difficulty of terms shown in learning the principle of incurring a damage and how to prevent it in accordance with the story.

After the learning and solving the quiz games, a score is calculated by applying the weight to the items in proportion with the degree of difficulty of the quiz games. The calculated score is displayed to a learner by types of learning and the learner can compare the rank with those of the other students. Through the learning achievement, the learner can get a feedback about the vulnerable types and the learner can study again.

Because of noticeable positive effects that students show in a manner information security methods based on what they have learned, after using this program, the program can be used when a class associated with information security learning is planned in schools and educational institutions. In particular, the information teachers can use this program as a supplementary learning tool for teaching an information security section.

Acknowledgements

This work was supported by the research grant of Jeju National University in 2015.

References

[1] Symantec, 2013 Norton Report **(2013)**, http://www.symantec.com/ko/kr/about/news/resources/press_kits/detail.jsp?pkid=norton-report-2013.
[2] M. Y. Kyoung, "The Current Staus and Teaching Plans of Computer Security Education for Middle School Students", Master's Degree Thesis, Graduate Dongguk University, **(2009)**.
[3] R. C. Schank, "Inside Case-Based Reasoning", Lawrence Erlbaum Associates**, (1989)**.
[4] E. Yeon, "Development of Case Design Principles for Case-based Learning", Doctoral Dissertation, Graduate Seoul National University, **(2013)**.
[5] T. Morrison, "Actionable Learning", Tokyo: Asian Development Bank Institute, **(2001)**.
[6] M. H. Kang, H. S. Kim and J. M. Lee, "The Effects of Flow and Cognitive Presence on Learning Outcomes in a Middle School Class using Web-based Simulation", Korean Association for Educational Information and Media, vol. 17, no. 1, **(2011)**, pp. 39-61.
[7] C. I. Im and Y. K. Yeon, "Formation Research about Case-based Design Principles for Simulation", Institute for Educational Technology, vol. 25, no. 2, **(2009)**, pp. 117-149.
[8] H. S. Kim, "Research about Composition of Web-edutainment Contents using a Game", Essays in Industrial Technology Research, vol. 4, no. 2, **(2002)**, pp. 223-232.
[9] S. K. Kim, "Gamification of Learning", Seoul: Hongrung Publishing Company, **(2014)**.
[10] T. J. Sung, "Educational Evaluation", Seoul: Hakjisa**, (2012)**.
[11] K. B. Lee, "Design and Implementation of Courseware for Database Security Education", Master's Degree Thesis , Graduate Dankook University, **(2003).**
[12] C. H. Lee, "Design and Implementation of a Situational Simulation Study Model for Information Security Education of Middle and High Schools", Master's Degree Thesis, Graduate Catholic University of Daegue, **(2004)**.
[13] M. S. Lee, "Design and Implementation of Web-Based Information Security Education Contents for the Youth Using XML", Master's Degree Thesis, Graduate Catholic University of Daegue, **(2006)**.
[14] K. J. Kim, H. S. Kim and J. H. Kim, "Designing a New Teaching Tool using Cryptography Principle in Secondary Schools", The Journal of Creative Informatics & Computing Education, vol. 1, no. 1, **(2007)**, pp. 1-11.
[15] S. Yoo, "Procedural-simulation Type Courseware Development for Information Security Learning in Secondary School", Master's Degree Thesis, Graduate Korea University, **(2010)**.
[16] S. M. Alessi and S. R. Trollip, "Multimedia for Learning: Methods and Development (3rd ed.)", Boston, MA:Allyn & Bacon, Inc., **(2001)**.
[17] S. R. Kim, J. H. Yang and S. B. Kim, "A Study on a Security Education and Quiz Game", Proceedings of The 10th International Conference on Information Security and Assurance (ISA 2016), **(2016)**.

Authors

Su Ryun Kim, She is currently working for Neople Corporation. She received the B.S. in Computer Science Education from Jeju National University, Korea, in 2015. Her research interests include computer science education and computer security.

Ji Hyeon Yang, She received the B.S. in Computer Science Education from Jeju National University, Korea, in 2015. Her research interests include computer science education and computer security education.

Seong Baeg Kim, He received the B.S., M.S., and Ph.D. in Computer Engineering from Seoul National University, Korea, in 1989, 1991, and 1995 respectively. He is currently a professor of the Dept. of Computer Education at Jeju National University, where he has been since 1996. He was a visiting scholar at Dept. of Computer Science, Montana State University from 2001 to 2002 and Dept. of Electrical & Computer Engineering, University of Cincinnati from 2008 to 2009. His research interests include computer science education, IT-fusion education, global education, computer system architecture, and computer security education.