



Ondokuz Mayıs Üniversitesi Eğitim Fakültesi Dergisi,
Ondokuz Mayıs University Journal of Faculty of Education

e-ISSN: 2548-0278 OMU EFD, December 2021, 40(2): 901-962

The Effects of an Online Environment Developed for Online Safety and Risk Education on the Knowledge Levels of Secondary School Students

Çevrimiçi Güvenlik ve Risk ile İlgili Eğitime Yönelik
Geliştirilmiş Bir Çevrimiçi Ortamın Ortaokul
Öğrencilerinin Bilgi Düzeylerine Etkileri

Doktora Öğr. Fatma GÖLPEK SARI¹, Prof. Dr. Süleyman Sadi SEFEROĞLU²

¹ Milli Eğitim Bakanlığı

• fatmagolpek@gmail.com • ORCID > 0000-0003-4960-3681

² Hacettepe Üniversitesi Eğitim Fakültesi

• sadi@hacettepe.edu.tr • ORCID > 0000-0002-5010-484X

Makale Bilgisi / Article Information

Makale Türü / Article Types: Araştırma Makalesi / Research Article

Geliş Tarihi / Received: 5 Mayıs / May 2021

Kabul Tarihi / Accepted: 03 Aralık / December 2021

Yıl / Year: 2021 | **Cilt – Volume:** 40 | **Sayı – Issue:** 2 | **Sayfa / Pages:** 901-962

Atıf/Cite as: Gölpek Sarı, F. ve Seferoğlu S. S., "The Effects of an Online Environment Developed for Online Safety and Risk Education on the Knowledge Levels of Secondary School Students - Çevrimiçi Güvenlik ve Risk ile İlgili Eğitime Yönelik Geliştirilmiş Bir Çevrimiçi Ortamın Ortaokul Öğrencilerinin Bilgi Düzeylerine Etkileri". Ondokuz Mayıs Üniversitesi Eğitim Fakültesi Dergisi- Ondokuz Mayıs University Journal of Faculty of Education 40 (2), Aralık 2021 901-962. <https://doi.org/933480>

Copyright © Published by Ondokuz Mayıs Üniversitesi, Eğitim Fakültesi – Ondokuz Mayıs University, Faculty of Education, Samsun, Turkey. All rights reserved.



<https://doi.org/10.7822/omuefd.933480>



THE EFFECTS OF AN ONLINE ENVIRONMENT DEVELOPED FOR ONLINE SAFETY AND RISK EDUCATION ON THE KNOWLEDGE LEVELS OF SECONDARY SCHOOL STUDENTS^[1]

ABSTRACT:

The purpose of this research is to examine the effects of trainings conducted in an online environment designed for online security and risk education on secondary school students' knowledge levels regarding online security and risk. At the stage of collecting quantitative data in the research, a single-group pre-test post-test design, which is one of the weak experimental designs, was used, and the findings of the research were supported by using the qualitative data collected with an open-ended questionnaire. The study group of the research consists of students studying in a central secondary school in Ankara. In the data collection process, a personal information form, Online Safety and Risk Level Determination Tool, and an open-ended questionnaire form were used. In order to determine the statistical methods to be used, it was tested whether the study groups showed a normal distribution. A computer-based statistical program was used for the analysis of quantitative data, and descriptive analysis and content analysis methods were used for the analysis of qualitative data. In the study, regarding the students' online safety and risk knowledge levels, it was concluded that it does not change depending on the time they allocate daily for their purpose of using the internet and whether they have received training on online security before. The results of the research showed that the trainings given in the online environment contributed to the students' online safety and risk knowledge levels. In addition, it has been concluded that the trainings given in the environment are not effective enough to ensure the permanence of the learned knowledge.

Keywords: *Online security, internet security, information security, cyber security, online learning, distance education.*

INTRODUCTION

Online environments affect our lives due to the global pandemic conditions we are in. In order to control the pandemic, face-to-face education in schools in many countries around the world has had to be replaced by distance education. Although the damages caused by COVID-19 cannot be calculated, it can be said that this global crisis offers an opportunity to rethink education (Zhao, 2020). The events experienced during the COVID-19 pandemic disrupted the functioning of millions of schools around the world and led to the decision to close schools to a large

[1] Bu çalışma, birinci yazar tarafından ikinci yazarın danışmanlığında hazırlanan doktora tezinden türetilmiştir.

extent. Zhao argues that the education redesign process should be about creating the best educational opportunities for all children.

Comparisons between distance education and face-to-face education have been frequently encountered during the global pandemic process. Moore et al. (2011) state that the design of different learning environments may depend on the learning goal, target audience, access (physical, virtual and/or both), and content type, and it is important to know how to use the learning environment. Bozkurt (2020) also states that the quality of educational materials is a subject open to discussion and that the focus is on quality assurance in the delivery of education and content, whether in distance education or face-to-face education.

Sağıroğlu and Alkan (2018) define information security as “the attempt to prevent information from being obtained by unwanted persons in all kinds of environments by using the right technology for the right purpose and in the right way in order to protect it from threats or dangers”. Safa et al. (2016) state that anti-virus, firewall, authentication and intrusion detection systems are technological measures that address information security, but they cannot guarantee information security. Kearney and Kruger (2016) also indicate the fact that information security awareness trainings should be managed continuously in order to follow the changes in risk profiles due to the constantly changing risks in online environments.

The study was conducted on the issue of security for online environments as a sub-dimension of information security. The concept of “online security” was used within the scope of the research. Hartikainen et al. (2019) defined online security as the protection of a person’s property, including hardware, software, information, and intellectual property. One of the most important factors in online security or internet security problem is the individual. In this regard, Shillair et al. (2015) stated that developing a user’s sense of personal responsibility is a necessary precursor to effective online safety interventions. In the same study, it is emphasized that users need training to increase their knowledge and self-confidence in order to make the internet a safer place. Çelen, Çelik, and Seferoğlu (2011) also state that the widespread use of computer and internet technologies contributes to our daily lives in many ways such as obtaining information and communication but also poses a threat to children and young people.

The widespread use of social media and other technologies raises concerns about the threats children to face online (Boyd & Hargittai, 2013). When a literature review on online safety is conducted, it is noteworthy that parents and peers are stated as important actors in children’s online safety (Hasebrink et al., 2011). It is emphasized that especially as the use of digital technologies in schools increases, teachers are faced with the question of how to encourage their use while protecting

children (Ahn et al., 2011). Many countries have different policies and educational practices aimed at promoting digital learning, digital participation, and digital literacy in schools (Ólafsson et al., 2013).

Within the scope of the European Children Online (EU Kids Online) Project (2010), research was conducted on digital literacy and safety skills, excessive use of the internet, frequency of online activity, quality of online content, children's use of social networks and risk experiences in the online environment. In the research report, it was stated that most of the children were not disturbed by the negative things they experienced on the internet and the risks were not perceived as distressing or harmful by the children (Livingstone et al., 2011). This result can be interpreted as children do not care about security problems in the online environment and do not feel the need to take any measures to solve these problems. According to a current report published within the scope of the European Children Online Project, in some countries, the amount of time that children spend online every day is almost double compared to 2010 (Smahel et al., 2020). It has been stated that children's negative experiences in the online environment increase with age, and most of them do not receive any online safety advice on online safety from their parents, teachers, or friends. Also, it has been reported that children who encounter negative experiences online display behaviors such as closing the window or application, ignoring the problem, and blocking the person, in addition to sharing the issue with someone (Smahel et al., 2020).

Considering the fact that the individual has the greatest responsibility for online safety and security on the Internet, and children frequently use online environments, it is thought that it is important for children to gain awareness in this regard and to reflect this awareness to their behaviors. Mihçı and Kılıç-Çakmak (2017) also draw attention to the importance of providing education to students in order to display responsible and safe behaviors on the internet. On the other hand, Padlipsky (2018) investigated whether an online course in cybersecurity could be developed with offline and face-to-face activities that reflect traditional classroom methods. The research findings showed that the group participating in both the online and offline activities of the course had a more positive awareness of cybersecurity.

To be able to reach more individuals from time to time in cases where face-to-face education cannot be applied, online education can provide an opportunity to provide flexibility in terms of space and time. In these days of the global pandemic, online education has provided many opportunities to students and teachers, and made online education be considered from different perspectives. Especially online environments, which are prepared by considering the target audience and achievements, can play a key role in the education of children. In this

sense, it is thought that the training to be held in an online environment designed for online security and risk issues is important in terms of the knowledge levels of secondary school students about online security and risk.

Purpose of the Research

This research aims to examine the effects of training conducted in an online environment designed for online security and risk education on secondary school students' knowledge levels regarding online security and risk. In the process of achieving this aim, answers to the following research questions were sought.

How does the students' knowledge of online safety and risk differ according to the daily allocated time for the purposes of using the internet and the previous training on online security, information security, or internet security?

What is the impact of training conducted in an environment designed for online safety and risk education on the change in students' knowledge of online safety and risk?

What are the effects of online safety and risk training conducted in the online environment on the permanence of what is learned?

What are the students' views on the developed online environment?

METHOD

Research Model

In this study, at the stage of collecting quantitative data, a single-group pre-test post-test design, which is one of the weak experimental designs, was used.

It was aimed to support the quantitative findings of the research with the qualitative data collected through an open-ended questionnaire. The experimental design and process for the study group of the research are given in Table 1.

Table 1. Experimental Design and Process for the Study Group of the Research

| Processes Before Experimental Process | Study Group | Method | Operations After the Experimental Process |
|--|-------------|------------------|---|
| Implementation of the personal information form | Students | Online Education | Implementation of the Online Security and Risk Leveling tool |
| Implementation of the Online Security and Risk Leveling tool | | | Implementation of the open-ended questionnaire form |
| | | | Implementation of the persistence test 4 weeks after the experimental procedure (Online safety and risk level determination tool) |

Study Group

The study group of the research consisted of students studying at a central secondary school in Ankara and attending the Information Technologies and Software course.

Demographic Information About Participants

The profile of the participants varies in terms of the time allocated per day for the purposes of using the Internet, and whether they have received previous training on online security, information security or internet security. A total of 30 sixth-grade students participated in the experimental application process of the research, and the data obtained from the students through the personal information form were presented in sub-titles.

Distribution of Participants by the Time Spent Daily in Using the Internet for Reading News and Following the Media

A total of 40% (12) of the students in the study group used the internet less than

15 minutes; 23.3% (7) of the students used the internet less than one hour; 6.7% (2) of them have daily internet use for 1-3 hours to read news and follow the media; It was observed that 30% (9) of the students never used the internet for reading news and following the media (See Table 2).

Table 2. Distribution of Participants by the Time Spent Daily for Reading News and Following the Media

| Daily Mean Time Spent | f | % |
|-----------------------|----|------|
| 1-3 hour | 2 | 6,7 |
| Less than 1 hour | 7 | 23,3 |
| Less than 15 minutes | 12 | 40 |
| Never | 9 | 30 |
| Total | 30 | 100 |

Distribution of the Participants according to the Time Spent Daily for Recreational Use of the Internet

A total of 56.7% (17) of the students in the study group took 1-3 hours; 20% (6) less than 1 hour; 13.3% (4) 4-6 hours; 6.7% (2) less than 15 minutes; It was observed that 3.3% (1) of them used the internet for 7 hours or more per day for entertainment purposes (See Table 3).

Table 3. Distribution of the Participants according to the Time Spent Daily for Recreational Use of the Internet

| Daily Mean Time Spent | f | % |
|-----------------------|----|------|
| 7 hours and more | 1 | 3,3 |
| 4-6 hours | 4 | 13,3 |
| 1-3 hours | 17 | 56,7 |
| Less than 1 hour | 6 | 20 |
| Less than 15 minutes | 2 | 6,7 |
| Total | 30 | 100 |

The Distribution of the Participants by the Time Spent Daily for Using the Internet for Educational Purposes

When the distribution of the participants according to the time they spend daily for educational purposes (doing research, doing homework, continuing distan-

ce education) is examined, it is seen that the majority of the students in the study group (76.7%) use the Internet 1-3 times a day for educational purposes (doing research, doing homework, continuing distance education) (see Table 4).

Table 4. Distribution of Participants by the Time Spent Daily in Educational Use of the Internet

| Daily Mean Time Spent | n | % |
|-----------------------|----|------|
| 4-6 hour | 3 | 10 |
| 1-3 hour | 23 | 76,7 |
| Less than 1 hour | 4 | 13,3 |
| Total | 30 | 100 |

Distribution of Participants by Receiving Any Previous Training on Online Security, Information Security, Cyber Security, or Internet Security

When the distribution of the participants according to their previous education on online security, information security, cyber security or internet security is examined, it is seen that the majority of the students in the study group (76.7%) have had no previous experience in online security, information security, cyber security or internet security (See Table 5).

Table 5. Distribution of Participants by Receiving Any Previous Training on Online Security, Information Security, Cyber Security, or Internet Security

| Educational Status | n | % |
|--------------------|----|------|
| Yes | 7 | 23,3 |
| No | 23 | 76,7 |
| Total | 30 | 100 |

Research Process

Experimental implementations of the research were carried out in the first semester of the 2020-2021 academic year with the implementation of the personal information form and pre-test (Online Security and Risk Level determination tool) and continued with the implementation of the post-test (Online Security and Risk Level determination tool) and open-ended questionnaire form. Finally, to test the permanence of the learning, the content in the online system was closed four weeks after the training was completed and the previously applied Online Security and Risk Level determination tool was reapplied. The procedures performed during the experimental implementation of the research are shown in Table 6.

Table 6. Transactions Performed in the Experimental Implementation Process

| Weeks | Activities |
|------------------------|---|
| 1. Week | Informing the participants about the process, examining the online environment of the participants, applying the personal information form and pre-test (Online safety and risk level determination tool) |
| 2. Week-5. Week | Online learning activities |
| 6. Week | Implementing of open-ended questionnaire and post-test (Online safety and risk and leveling tool) |
| 10. Week | Implementing of the permanency test (Online safety and risk level determination tool) to test the permanence of learning |

Within the scope of learning activities in the online environment, weekly tasks were given to the students every week in the form of synchronous lessons held with the students via video conferencing tool, independently of the online environment. Table 7 shows the topics that the students followed each week.

Table 7. Distribution of Topics Followed by Students

| Weeks | Activities |
|----------------|---|
| 1. Week | Conscious Use of the Internet Unit - Protection of Personal Data Conscious Use of the Internet Unit - The Subject of Social Networks Synchronous participation with video conferencing tool |
| 2. Week | Conscious Use of the Internet Unit – The Subject of Internet Literacy Conscious Use of the Internet Unit – The Subject of Cyberbullying Conscious Use of the Internet Unit – The Subject of Online Risks End of Unit Events Page Synchronous participation with video conferencing tool |

| | |
|---------------|--|
| 3.Week | Internet and Network Security Unit - Password Security Issue Internet and Network Security Unit - Malware Subject Synchronous participation with video conferencing tool |
| 4.Week | Internet and Network Security Unit -The Subject of Web Security Precautions Internet and Network Security Unit - The Subject of Unsecured Communication Ways End of Unit Events Page Synchronous participation with video conferencing tool |

Online Environment Design Process

In order to develop the online learning environment, a detailed literature review was conducted and the characteristics that an effective online learning environment should have were determined. Although there are different design suggestions in the literature for the design process of online learning environments, a design model similar to Tüzün's (2011) nine-stage design proposal was prepared for the environment to be used in the study (See Table 8).

Table 8.Design Process of Online Learning Environment

| | Design Phases | Executed Transactions |
|---|--|--|
| 1 | Pre-Design Processes | Determination of gains |
| 2 | Performing the analysis work | Determining the characteristics of the target audience, determining the physical possibilities |
| 3 | Determination of Personnel | Determining the personnel who will be in charge of the online environment development process, realizing the distribution of tasks |
| 4 | Doing the Design/Development work | Carrying out the design work by considering the determined gains, methods and techniques and physical possibilities |

| | | |
|---|--|---|
| 5 | Experts' assessment | Evaluation of the environment by the experts in line with the criteria presented to them, taking their opinions |
| 6 | Troubleshooting the environment | Elimination of problems in the environment in line with expert feedback, realization of suggestions |
| 7 | Piloting | Conducting the usability study of the environment with a pilot group |

A literature review was conducted in order to determine the criteria taken into account in the evaluation of the environment. In order to determine the features that the environment should have in the online environment design process, the items of the scale titled "Online Environments Scale for Gaining Self Protection Awareness to Children" developed by Eren and Erdem (2020) were accepted as criteria. In this context, the dimension of access to the environment, motivation dimension, learning dimension, content dimension, active support system dimension, which are among the scale criteria, were taken into consideration. The criteria for evaluating the educational content prepared by the researcher were used to determine the problems in the environment. Opinions were received from eight field experts within the scope of the determined criteria, and some arrangements were made in the environment in line with the suggestions received.

Data Collection Tools

During the research process, data collection was carried out before and after the experimental procedure. In order to collect data, "Personal Information Form, Online Environment Expert Opinion Form, Online Safety and Risk Level Determination Tool and an Open-Ended Questionnaire Form" were used. In the personal information form developed by the researchers, there are questions about the daily allocated time for the purposes of using the internet and the status of having received previous training on online security, information security or internet security. A measurement tool titled "Online Security and Risk Level Determination Tool" developed by the researchers was used to measure the knowledge levels of secondary school students about online safety and risk. The Online Safety and Risk Level Determination Tool consists of 16 open-ended questions developed by determining the themes that should be included in the scope of the literature review. The measurement tool, which was prepared in order to reveal the intelligibility of the questions and their suitability for the level of the student, was applied to nine sixth-grade students. In this process, two questions that were thought to be inappropriate for the level of the students were removed from the test. The 14-question test was evaluated by 10 field experts. In line with expert opinions, three questions

that were thought to measure similar gains and had a low content validity ratio were excluded from the test, and some adjustments were made to some questions. The scope validity index of the measurement tool, which was reduced to 11 questions, was determined as 0.94. Since the number of experts consulted was 10, the scope validity criterion was accepted as 0.62, since the scope validity index > coverage validity rate, the content validity of the developed tool was determined to be statistically significant (Veneziano & Hooper, 1997). On the other hand, the final arrangements of the tool were made based on the opinions of two grammar experts. In order to determine the reliability of the online safety and risk level determination tool, the pre-test results were coded by two different coders, Kappa statistics were used for each question, and encoder fit values were calculated.

An expert opinion form titled “Online Environment Expert Opinion Form” was developed in order to determine the features that the environment should have during the online environment design process. While preparing this form, the list of criteria developed by Eren and Erdem (2020) was used. Necessary permissions were obtained for the use of the criteria in the scale titled “Online Environments Scale for Raising Self-protection Awareness to Children” developed by Eren and Erdem (2020). In the environment design process, in order to determine the problems in the environment, opinions were taken from eight field experts within the scope of the determined criteria, and some arrangements were made in the environment in line with the suggestions received.

Within the scope of the research, an open-ended questionnaire form was developed by the researchers in order to determine the effectiveness of the online learning environment. In this form, “Is the content on the site up-to-date? How long do you think the videos and narratives should be (longer-short)?” questions are included.

Ethics Committee Approval

Ethical permissions were obtained from the relevant institutions to carry out the study. The data collection process and participation in online training were carried out on a voluntary basis, and the necessary permissions were obtained from the parents of the students through an online form.

The Title of the Ethics Committee: Hacettepe University Rectorate

Ethics Document's Number: 35853172-300

Approval Date: 12.11.2019

The Title of the Ethics Committee: Ankara Governor's Office of National Education

Ethics Document's Number: 14588481-605.99-E. 24100798

Approval Date: 04.12.2019.

Online Security and Risk Level Determination Tool Coder Compliance Analysis

In order to determine the reliability of the Online Safety and Risk Level determination tool developed by the researcher, the pre-test results were coded by two separate coders, Kappa statistics were used for each question, and encoder fit values were calculated. In order to interpret the Kappa values of the questions in the measurement tool, the table suggested by Landis and Koch (1977) was taken into account (see Table 9).

Table 9. Kappa Statistics Value and Compliance Interpretation

| Kappa Value Range | Compliance Strength |
|-------------------|---------------------|
| <0.00 | Weak-bad |
| 0.00-0.20 | Small |
| 0.21-0.40 | Acceptable |
| 0.41-0.60 | Medium |
| 0.61-0.80 | Important, strong |
| 0.81-1.00 | Excellent |

The encoder fit values calculated using the Kappa statistic are presented in Table 10:

Table 10. Distribution of Kappa Statistics Results for Pre-test

| Questions | Cohen Kappa Count | Spearman Correlation Value |
|-----------|-------------------|----------------------------|
| 1 | 1,000 | 1,000 |
| 2 | ,923 | ,911 |
| 3 | ,712 | ,760 |
| 4 | ,660 | ,873 |
| 5 | ,779 | ,790 |
| 6 | ,737 | ,942 |
| 7 | ,722 | ,843 |
| 8 | ,720 | ,799 |
| 9 | ,685 | ,753 |
| 10 | ,705 | ,708 |
| 11 | ,671 | ,723 |

As seen in Table 10, considering the values suggested by Landis and Koch (1977) (See Table 9), the consistency level of the 3rd, 4th, 5th, 6th, 7th, 8th, 9th, 10th, and 11th questions in the measurement tool was strong, the compatibility level of the 1st and 2nd questions was excellent, and it can be said that the measurement tool is reliable in line with these data.

Analysis of Data

While determining the statistical methods to be used for the analysis of the quantitative data of the study, since the sample size was less than 50, the assumption of normality was tested with the Shapiro-Wilks test. For the analysis of the open-ended questionnaire, which was used to collect qualitative data, descriptive analysis and content analysis methods were used.

The research process, which includes the data sources of the research, data collection and data analysis, is presented in Table 11.

Table 11. Outline of Research for the Study Group

| Research Problem | Data Source | Data Collection | Data Analysis |
|---|-------------|---|--|
| How does the students' knowledge of online safety and risk differ according to the daily allocated time for the purposes of using the internet and the previous training on online security, information security or internet security? | Students | Personal Information Form Online security and risk leveling tool | Descriptive Statistics Independent Groups T-Test One-Factor Analysis of Variance |
| What is the impact of training conducted in an environment designed for online safety and risk education on the change in students' knowledge of online safety and risk? | Students | Online security and risk leveling tool | Dependent Groups T-Test |
| What are the effects of online safety and risk training conducted in the online environment on the permanence of what is learned? | Students | Online security and risk leveling tool | Dependent Groups T-Test |
| What are the students' views on the developed online environment? | Students | Open-ended questionnaire form | Descriptive and content analysis |

FINDINGS

This section includes the findings of the encoder fit analysis for the pre-test and the findings for the research questions. The findings are presented in a way that the research questions determined in line with the purpose of this research can be answered separately.

Change of Students' Online Safety and Risk-Related Knowledge Levels Based on Daily Allotted Time for Internet Use Purposes and Receiving Previous Training on Online Security, Information Security, or Internet Security

The first research question of this study is “*Students' knowledge levels about online safety and risk; How does the amount of time allocated per day for the purposes of using the Internet differ according to previous training in online security, information security or internet security?*” The results of the Shapiro-Wilks test applied to the pre-test and post-test data in order to determine whether the data show a normal distribution for the knowledge levels of the study group about online safety and risk are given in Table 12.

Table 12. Distribution of Shapiro-Wilks Normality Test Results Regarding Pre-Test and Post-Test Results

| Test | N | X | S | Sd | t | P |
|-----------|----|-------|-------|----|-------|-------|
| Pre-test | 30 | 64,70 | 18,15 | 29 | -8,50 | 0,000 |
| Post-test | 30 | 91,80 | 14,92 | | | |

As can be seen in Table 12, since $p > .05$ according to the Shapiro-Wilks test analysis results applied for the pre-test and post-test results, it was decided that the group participating in the study showed a normal distribution. In this direction, one-way analysis of variance and independent groups were used to determine how students' knowledge levels about online security and risk change depending on the daily allocated time for their purpose of using the internet and their previous training on online security, information security or internet security.

Findings on How Students' Online Safety and Risk Levels Change Depending on the Time Allotted Daily for Internet Use Purposes

Findings on how the online safety and risk level of the participants change depending on the daily allocated time for reading news and following the media, for entertainment and educational purposes (research, doing homework, continuing distance education) are presented under separate headings.

Findings on How Students' Online Safety and Risk Levels Change Depending on the Time They Allocate Daily for Using the Internet for Reading News and Following the Media

A single-factor analysis of variance was used to determine how the online safety and risk level of the participants changed depending on the time they spent daily reading news and following the media. The results of this analysis are given

in Table 13.

Table 13. The Distribution of the Results of the Single Factor Analysis of Variance by the Time Spent Daily on Using the Internet for the Purpose of Reading News and Following the Media and by the Level of Knowledge of Online Safety and Risk of the Participants

| Source of Variance | Sum of Squares | sd | Mean Squares | F | p | Significant Difference |
|--------------------|----------------|----|--------------|-----|-----|------------------------|
| Intergroup | 987,06 | 3 | 329.02 | .99 | .40 | |
| Ingroups | 8573,23 | 26 | 329.74 | | | - |
| Total | 9560.30 | 29 | | | | |

The results of the single-factor analysis of variance showed that students' knowledge levels about online safety and risk; It shows that the use of the internet for reading news and following the media does not change depending on the time spent daily, $F(3, 26) = .99, p > .05$.

Findings on How Students' Online Safety and Risk Levels Change Depending on the Time They Allocate Daily for Recreational Use of the Internet

A single factor analysis of variance was used to determine whether the level of knowledge about online safety and risk differed according to the daily time spent by the participants for entertainment purposes. The results of this analysis are given in Table 14.

Table 14. Distribution of Single-Factor Analysis of Variance Results by Time Spent Daily on Recreational Use of the Internet and Level of Knowledge of Online Safety and Risk of Participants

| Source of Variance | Sum of Squares | sd | Mean Squares | F | p | Significant Difference |
|--------------------|----------------|----|--------------|------|-----|------------------------|
| Intergroup | 2765,19 | 4 | 691.30 | 2.54 | .06 | |
| Ingroups | 6795,11 | 25 | 271.80 | | | - |
| Total | 9560,30 | 29 | | | | |

The results of the single-factor analysis of variance showed that students' knowledge levels about online safety and risk; shows that it does not change depending

on the time spent daily for entertainment purposes [$F(4, 25) = 2.54, p >.05$].

Findings on How Students' Online Safety and Risk Level Changes Depending on the Time They Allocate Daily for Using the Internet for Educational Purposes (Research, Homework, Continuing Distance Education)

A single-factor analysis of variance was used to determine the relationship between the daily time spent by the participants using the Internet for educational purposes (research, homework, continuing distance education) and their level of knowledge about online safety and risk. The results of this analysis are given in Table 15.

Table 15. The Distribution of the Results of Single Factor Analysis of Variance by the Time Spent Daily by the Participants for Using the Internet for Educational Purposes (Doing Research, Doing Homework, Continuing Distance Education) and their Knowledge Levels on Online Safety and Risk

| Source of Variance | Sum of Squares | sd | Mean Squares | F | P | Significant Difference |
|--------------------|----------------|----|--------------|------|-----|------------------------|
| Intergroup | 1199,92 | 2 | 599,96 | 1.93 | .16 | |
| Ingroups | 8360,37 | 27 | 309,64 | | | - |
| Total | 9560,30 | 29 | | | | |

The results of the single-factor analysis of variance showed that students' knowledge levels about online safety and risk; shows that it does not change depending on the daily time spent using the internet for educational purposes (research, homework, continuing distance education), $F(2, 27) = 1.93, p >.05$.

The Relationship between Participants' Level of Knowledge About Online Security, Information Security, Cyber Security, or Internet Security and Their Level of Prior Education about Online Security and Risk

Since it was determined that the pre-test results of the group participating in the study were normally distributed (See Table 12), the difference between the participants' previous training on online security, information security, cyber security or internet security and their level of knowledge about online security and risk. Independent groups t-test analysis was used to determine the relationship. The results of this analysis are given in Table 16:

Table 16. Distribution of Independent Groups T-Test Results by Participants' Level of Knowledge About Online Security, Information Security, Cyber Security, or Internet Security and Their Level of Knowledge About Online Security and Risk

| Education Status | N | X | S | sd | t | p |
|------------------|----|-------|-------|----|-----|-----|
| Yes | 7 | 62,85 | 27,05 | 28 | .30 | .76 |
| No | 23 | 65,26 | 15,27 | | .22 | |

According to independent groups t-test results, students' knowledge levels about online safety and risk; online security, information security, cyber security or internet security does not change according to any previous training, $t(28)=.30$, $p>.05$.

Findings on the Effect of Online Training on the Change in Students' Knowledge of Online Safety and Risk

The second research question of this study is "What is the effect of training conducted in an environment designed for online security and risk-related education on the change in students' knowledge of online security and risk?" The Shapiro-Wilks test was used for the pre-test and post-test data to determine whether the data showed a normal distribution for the online safety and risk knowledge levels of the study group. Since $p>.05$ for both tests, it was decided that the group had a normal distribution. The pre-test and post-test scores were compared in order to test the effectiveness of the experimental application on the students' knowledge levels about online safety and risk. The dependent groups t-test results for the comparison of the results are given in Table 17.

Table 17. Distribution of Dependent Groups T-Test Results Regarding the Comparison of Pre-test and Post-test Results of the Study Group

| Test | N | X | S | Sd | t | p |
|-----------|----|-------|-------|----|------|-----|
| Pre-test | 30 | 64,70 | 18,15 | 29 | 8.50 | .00 |
| Post-test | 30 | 91,80 | 14,92 | | | |

As seen in Table 17, it was determined that there was a significant increase in the knowledge levels of students about online safety and risk after the online training, $t(29)=-8.50$, $p<.05$. While the average of the Online Security and Risk Level scores of the students before the education was $X= 64.70$, the average of the Online Security and Risk Level scores after the education was determined as $X= 91.80$.

This finding can be interpreted as the fact that online security and risk-related trainings conducted in the online environment have a significant effect on increasing students' level of knowledge about online security and risk.

Findings on the Effect of Online Safety and Risk-Related Trainings Conducted in the Online Environment on the Permanence of Learned

The third research question of this study is “*What are the effects of online safety and risk training on the permanence of what has been learned?*” The Shapiro-Wilks test was used for the retention test data to determine whether the data showed a normal distribution for the online safety and risk knowledge levels of the study group, and since the analysis results were $p > .05$ (Table 18), it was decided that the group had a normal distribution.

Table 18. Distribution of Shapiro-Wilks Normality Test Results Regarding Permanency Test Results

| Test | df | P |
|-----------------|----|-----|
| Permanency Test | 30 | .38 |

The post-test and retention test scores of the study group were compared in order to evaluate the experimental application in terms of the permanence of what was learned. The dependent groups t-test results regarding the comparison of the post-test and retention test results of the study group are given in Table 19.

Table 19. Dependent Groups T-Test Results Regarding the Comparison of the Study Group's Post-test and Permanency Test Results

| Test | N | X | S | Sd | t | P |
|-----------------|----|-------|-------|----|------|-----|
| Post-Test | 30 | 91.80 | 14.92 | 29 | 2.10 | .04 |
| Permanency Test | 30 | 87.26 | 14.26 | | | |

As seen in Table 19, it was determined that there was a significant difference in students' knowledge levels about online safety and risk, $t(29)=2.10$, $p < .05$. While the average of the Online Safety and Risk Level scores of the students from the post-test was $X=91.80$, it was seen that the average of the online safety and risk level scores was $X=87.26$ in the permanence test performed four weeks after the completion of the training. These data show that the training conducted in the online environment is not sufficient to ensure the permanence of the learned information.

Students' Views on the Functionality of the Developed Online Environment

The fourth and final research question of this study is “*What are the students' views on the functionality of the developed online environment?*”. In order to determine the usability problems and functionality of the environment developed within the scope of the research, an open-ended questionnaire was developed by the researcher, taking into account the expert opinions. The opinions of the students who participated in the online training on the functionality of the developed environment were obtained through an open-ended questionnaire. The data obtained with an open-ended questionnaire form are presented under sub-headings:

Findings Regarding the Appropriateness of the Name of the Site

All of the students in the study group (30) stated that they found the name of the developed online environment appropriate.

Findings Regarding the Up-to-Dateness of Content on the Site

All of the students (30) in the study group stated that they thought that the content available online was up-to-date.

Findings Regarding How Long (Longer-Shorter) Videos and Narratives Should Be

Regarding the duration of the videos and narratives in the developed online environment; 12 students stated that the durations were ideal; seven students said that the duration should be shorter, six students said that the duration should be longer; five students stated that the duration should be changed according to the content of the subject.

Findings Regarding What You Think About “Let’s Test Ourselves” Episodes

Regarding the “Let’s Test Ourselves” sections in the developed online environment, 25 students stated that the “let’s test ourselves” sections helped them to reinforce the topics, they understood the topic better with the examples given, and they found this section effective and enjoyable. Five students stated that the number of questions in the “Let’s Test Ourselves” section is low.

Findings Regarding What You Think About the Activities in the “Events” Section

Regarding the “Events” section in the developed online environment, 26 students stated that all of the activities attracted their attention, four students stated

that they had problems while implementing the activities via mobile technologies; two students stated that the activities did not attract their attention, two students stated that some activities attracted their attention, and one student stated that she did not like the “Sample Case Analysis” activity.

Findings Regarding Which Aspect of the Online Environment Is Most Liked

Regarding which aspect of the developed online environment is most liked; eight students stated that the games section; eight students stated that the contents are useful, educational, clear, and understandable; six students ensure that the environment is pleasant and fun; six students stated that the activities; four students stated that the videos; two students stated that “ask questions”; two students said that they liked all sections on the site; one student said that she liked the “friends” section; one student stated that the teacher’s development of the environment attracted their attention.

Findings Regarding Which Aspect of the Online Environment Is Least Liked

Regarding which aspect of the developed online environment they liked the least, 11 students stated that there was no aspect they did not like in the developed online environment; four students stated that there were occasional mistakes in the games; two students stated that they had problems in viewing whether the activities were done or not, and two students stated that the texts were too long. The sentences about the aspects of the site that 11 students did not like are as follows:

“The puzzle in the activities section is confusing.” (Student 9)

“Words are difficult to write in the word puzzle.” (Student 22)

“I didn’t like that the events were not done from the phone.” (Student 20)

“I didn’t like the activities.” (Student 24)

“It would be better if there were more questions in the ‘Let’s test ourselves’ section.” (Student 18)

“I didn’t like the ‘Sample Case Analysis’ event and the length of the articles.” (Student 19)

“There could be more video tutorials.” (Student 23)

“I don’t like that the videos are not full screen.” (Student 25)

“I didn’t like the videos.” (Student 2)

“I didn’t have any dissatisfaction with anything other than the annoyance that the site sometimes crashed.” (Student 2)

“When I want to repeat the past topics, I don’t like the fact that the previous week’s topic is not reopened.” (Student 10)

Findings on What Contributions the Online Environment Contributes to Online Security and Risk Level

Regarding how the online environment contributes to information about online safety and risk, 13 students stated that they learned the subjects they did not know through the online environment; 13 students stated that they learned the importance of being more careful on the Internet. The sentences of four students about how the online environment contributes to knowledge about online safety and risk are as follows:

“The online environment showed me how not to trust people on social media, how to set passwords now.” (Student 20)

“I learned about password security and personal data protection, what to do when faced with cyberbullying, and much more.” (Student 4)

“The online environment taught me how to protect myself in the virtual environment, how to behave, how to protect my information.” (Student 10)

“I started to set my passwords properly.” (Student 15)

Findings Regarding What Kinds of Difficulties Encountered in Using the Online Environment

Regarding the difficulties encountered in the use of the online environment, 14 students stated that they did not encounter any difficulties while using the online environment; three students had problems doing activities over the phone; two students stated that they could encounter advertisements in the video section, two students stated that they had problems in recording the sections they completed, and two students stated that there were occasional errors in the games. The views of seven students on the difficulties they encountered in the process of using the online environment are as follows:

“Video freezing forced me.” (Student 9)

“Sometimes I have difficulties opening videos.” (Student 14)

“I had a little difficulty opening the site.” (Student 12)

“I had a hard time typing letters in the word search activity.” (Student 19)

“I had difficulty in the puzzle part of the activities.” (Student 15)

“I couldn’t find the site search. It should be visible though.” (Student 22)

“Sometimes, even though I marked the questions, they showed up as blank.” (Student 18)

Findings on Which Topics Should Be Included in an Online Safety and Risk Education for Students

Regarding which topics should be included in an online safety and risk education for students, 10 students stated that the online topics were sufficient and seven students stated that they had no idea about the topic proposal. The statements of 13 students about what other topics should be included in an online safety and risk education for students are as follows:

“Videos should be shared periodically about what we can do when we encounter cyberbullying.” (Student 4)

“What more can we do about these issues, how should we learn to limit ourselves in the virtual environment, etc. topics should be included.” (Student 10)

“It may be an issue with the settings section in Google.” (Student 19)

“We should be told how to use social media more securely.” (Student 2)

“Ways of protection from viruses should be explained more.” (Student 1)

“What should I do in the face of hackers?” (Student 25)

“In my opinion, information about applications should also be given.” (Student 18)

“Separate sections should be included in each unit.” (Student 28)

“Include interesting content and even more fun activities.” (Student 23)

“The puzzle should be added.” (Student 13)

“Photoshop applications should be added.” (Student 7)

“The word derivation activity should be added.” (Student 14)

“The topics should be included in the order in which the course topics go.” (Student 20)

Findings Regarding the Contribution of Communication with Other Users in the “Add New Comment” Section

Regarding the contribution of the communication with other users in the “Add New Comment” section, 21 students stated that the “Add New Comment” section enabled them to exchange ideas with their friends, provided the opportunity to learn different information, eight students stated that they did not use this section and did not find it necessary. One student stated that this section helped to consolidate their knowledge.

Recommendations About the Online Environment

22 students stated that they do not have any suggestions for the online environment. Eight students’ suggestions for the online environment are as follows:

“Videos may be a little slower” (Student 8)

“More different events (puzzle, fill in the blanks, True False questions) can be added.” (Student 9)

“Errors in mobile technologies should be fixed.” (Student 16)

“Online safety hazards must be repeated often.” (Student 10)

“Continued’ text should be bigger and more games and activities should be added.” (Student 29)

“It should be a topic that teaches how to protect ourselves from hackers.” (Student 25)

“True/false activities can be added.” (Student 22)

RESULT AND DISCUSSION

In these days when the global pandemic has affected our lives in many areas, serious transformations have occurred in the field of education, and it has become important to evaluate distance education in terms of opportunities. With distance education activities, the time spent on the Internet in daily life has increased, and it has become necessary to be informed about some security risks that the Internet can bring as well as the opportunities it provides. Within the scope of this study, the effectiveness of the training conducted in the online environment developed for training on online safety and risk was tested in terms of students' knowledge levels about online security and risk.

The first research question of the study was *“Students' knowledge levels about online safety and risk; How does the amount of time allocated per day for the purposes of using the Internet differ according to previous training in online security, information security or internet security?”*. A single-factor analysis of variance was used to determine how students' knowledge levels about online safety and risk change depending on the time they spend daily using the internet for reading news and following the media. According to the results obtained, the level of knowledge about online safety and risk of the students who compose the study group of the research; it is possible to say that it does not change depending on the time they allocate daily to use the internet. In a study carried out to determine teachers' thoughts about cyberbullying; It has been determined that as the duration of internet use increases, the thoughts of the participants that cyberbullying will only be done by adults decrease (Yenilmez & Seferoğlu, 2013). It is stated that as children's internet use increases, the probability of being exposed to unwanted risks also increases (Livingstone et al., 2011).

Within the scope of the study, there is no significant relationship between the participants' previous training on online security, information security, cyber security or internet security and their knowledge levels about online security and risk. It can be thought that this result is due to the fact that the scope of the training that the students have attended before is more limited compared to the subjects in the developed environment. In the study carried out within the scope of the European Children Online (2020) project, it was stated that feeling safe online is an important factor for participation in many online activities (Smahel et al., 2020). In this study, considering the students' participation in training on online security and risk before, it was determined that the students were at the same level in terms of online security and risk knowledge levels, and the training was carried out.

The second research question of the study is *“What is the effect of training conducted in an environment designed for online security and risk-related education on*

the change in students' knowledge of online security and risk?" In order to test the effectiveness of the experimental application on the students' knowledge levels of online safety and risk, pre-test and post-test scores were compared with dependent groups t-test, and it was determined that there was a significant increase in students' knowledge levels about online safety and risk after the training. This can be thought of as the fact that the online security and risk-related training conducted in the online environment within the scope of the research have a significant impact on improving the knowledge levels of students about online security and risk. It is possible to say that this result obtained from the research coincides with the results of some studies in the literature. E.g; In a study in which children aged 9-13 were given online privacy-privacy literacy education; It has been examined that education can affect children's online privacy literacy. Research results have shown that education improves children's understanding of online privacy (Desimpelaere et al., 2020). In another study examining the effect of digital footprint course design on students' academic achievement in digital citizenship, it was determined that the design of the digital footprint course had a positive effect on academic success in digital citizenship (Kuh Karyeli & Dağhan, 2019).

The third research question of the study is *"What are the effects of online safety and risk training on the permanence of what has been learned?"* The post-test and retention test scores of the study group were compared with the dependent groups' t-test in order to evaluate the learning in terms of permanence. Within the scope of the research, it was concluded that there was a significant difference in the students' knowledge levels about online safety and risk in terms of post-test and permanency test scores. This finding can be interpreted as the training conducted in the online environment within the scope of the research is not sufficient to ensure the permanence of what has been learned. It can be thought that this result is due to the fact that the students did not participate in the lessons adequately.

The fourth and final research question of the study; *"What are the students' views on the developed online environment?"* Through this research question, the usability problems of the environment were determined and the arrangements that could be made in the environment were determined. Findings such as the low number of questions in the "Let's Test Ourselves" section in the environment developed in this direction, the problems in the implementation of the "Events" section through mobile technologies, the long texts on some pages, and the advertisements on the videos page draw attention. Considering these findings, it was thought that it would be appropriate to make arrangements such as increasing the number of questions in the "let's test ourselves" section in the environment developed, eliminating the problems experienced in mobile technologies for events, shortening the texts and presenting the videos directly on the developed system without advertisements.

To summarize the results obtained within the scope of the study, it can be said that online environments developed in accordance with the targeted achievements and student level and the training carried out by the planning of the teacher through these environments will contribute to student success. Nowadays, when the time spent online is quite high, it is important for students to be informed about the security problems and risks they may encounter in online environments. For future studies, it may be recommended to conduct experimental studies in which different learning techniques are used for the use of online environments.

REFERENCES

- Ahn, J., Bivona, L. K., & Discala, J. (2011). Social media access in K12 schools: Intractable policy controversies in an evolving world. *Proceedings of the American Society for Information Science and Technology*, 48(1), 1-10.
- Boyd, D., & Hargittai, E. (2013). Connected and concerned: Variation in parents' online safety concerns. *Policy & Internet*, 5(3), 245-269.
- Bozkurt, A. (2020). Koronavirüs (Covid-19) pandemi süreci ve pandemi sonrası dünyada eğitime yönelik değerlendirmeler: Yeni normal ve yeni eğitim paradigması. *Açıköğretim Uygulamaları ve Araştırmaları Dergisi*, 6(3), 112-142.
- Çelen, F. K., Çelik, A., & Seferoğlu, S. S. (2011). Çocukların İnternet kullanımları ve onları bekleyen çevrim-içi riskler. XIII. *Akademik Bilişim Konferansı (AB11) Bildirileri*, 645-652. İnönü Üniversitesi, Malatya. [Çevrimiçi: http://ab.org.tr/ab11/kitap/celen_celik_Riskler_AB11.pdf, Erişim Tarihi: 15.02.2021]
- Cresswell, J. W. (2017). *Araştırma deseni nitel, nicel ve karma yöntem yaklaşımları* (4. Baskıdan çeviri, S. B. Demir). Ankara: Eğiten Kitap.
- Desimpelaere, L., Hudders, L., & Van de Sompel, D. (2020). Knowledge as a strategy for privacy protection: How a privacy literacy training affects children's online disclosure behavior. *Computers in Human Behavior*, 110, 106382.
- Eren, S., & Erdem, M. (2013). The examination of online kids' sites with the purpose of raising kids' self-protection awareness. *Procedia-Social and Behavioral Sciences*, 83, 611-614.
- Hartikainen, H., Livari, N., & Kinnula, M. (2019). Children's design recommendations for online safety education. *International Journal of Child-Computer Interaction*, 22, 100-146.
- Hasebrink, U., Görzig, A., Haddon, L., Kalmus, V., & Livingstone, S. (2011). *Patterns of risk and safety online. In-depth analyses from the EU Kids Online survey of 9-16-year-olds and their parents in 25 countries*. LSE, London: EU Kids Online.
- Kearney, W. D., & Kruger, H. A. (2016). Can perceptual differences account for enigmatic information security behaviour in an organisation? *Computers & Security*, 61, 46-58.
- Kuh Karyeli, G., & Dağhan, G. (2019). Sayısal ayak izi ders tasarımının öğrencilerin sayısal vatandaşlık konusundaki akademik başarılarına etkisi. *Erzincan Üniversitesi Eğitim Fakültesi Dergisi*, 22(1), 256-275.
- Landis, J. R., & Koch, G. G. (1977). The measurement of observer agreement for categorical data. *Biometrics*, 33, 159-174.
- Livingstone, S., Haddon, L., Görzig, A., & Ólafsson, K. (2011). *Technical report and user guide: The 2010 EU Kids Online Survey*. LSE, London: EU Kids Online.
- Mihçı, P., & Kılıç-Çakmak, E. (2017). Öğrenci siber sağlık ölççekleri geliştirme çalışması. *Gazi Üniversitesi Gazi Eğitim Fakültesi Dergisi*, 37(2), 457-491.
- Moore, J. L., Dickson-Deane, C., & Galyen, K. (2011). e-Learning, online learning, and distance learning environments: Are they the same? *The Internet and Higher Education*, 14(2), 129-135.
- Ólafsson, K., Livingstone, S., & Haddon, L. (2013). *Children's use of online technologies in Europe: A review of the European evidence base*. EU Kids Online. London, UK.
- Padlipsky, S. (2018). *Using offline activities to enhance online cybersecurity education*. Yayınlanmamış yüksek lisans tezi. California Polytechnic State University, California.
- Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security*, 56, 70-82.

- Sağıroğlu, Ş., & Alkan, M. (2018). *Siber güvenlik ve savunma farkındalık ve caydırıcılık*. BGD Siber Güvenlik ve Savunma Kitap Serisi. s. 26. Grafiker Yayınları. Ankara.
- Shillair, R., Cotten, S. R., Tsai, H. Y. S., Alhabash, S., LaRose, R., & Rifon, N. J. (2015). Online safety begins with you and me: Convincing Internet users to protect themselves. *Computers in Human Behavior*, 48, 199-207.
- Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K., Livingstone, S., & Hasebrink, U. (2020). EU Kids Online 2020: Survey results from 19 countries. *EU Kids Online. London School of Economics and Political Science*, London, UK.
- Tüzün, H., Bilgiç, H. G., Kalaycı, E., Çınar, M., Akıncı, A., Denizler, Y., & Yüksel, Y. (2011). Yerleşik bir dersin web tabanlı uzaktan eğitim için yeniden tasarımı. Demirci, B.B., Telli-Yamamoto, G. & Demiray, U., *Türkiye’de e-öğrenme: Gelişmeler ve uygulamalar II* (ss.175-199). Anadolu Üniversitesi Yayınları: Eskişehir.
- Veneziano L., & Hooper J. (1997). A method for quantifying content validity of health-related questionnaires. *American Journal of Health Behavior*, 21(1), 67-70.
- Yenilmez, Y., & Seferoğlu, S. S. (2013). Sanal zorbalık ve öğretmenlerin farkındalık durumlarına bir bakış. *Education & Science/Eğitim ve Bilim*, 38(169).
- Zhao, Y. (2020). COVID-19 as a catalyst for educational change. *Prospects*, 49(1), 29-33.

THE EFFECTS OF AN ONLINE ENVIRONMENT DEVELOPED FOR ONLINE SAFETY AND RISK EDUCATION ON THE KNOWLEDGE LEVELS OF SECONDARY SCHOOL STUDENTS

EXTENDED ABSTRACT:

Distance education and online education can provide an opportunity to provide flexibility in terms of space and time. Online environments are prepared especially by considering the target and achievements; they can play a key role in the education of children. This study aims to examine the effects of trainings conducted in an online environment that designed for online security and risk education on secondary school students’ knowledge levels about online security and risk. In the research, at the stage of collecting quantitative data, one group pre-test post-test design, which is one of the weak experimental designs, was used. The findings of the research were supported by using qualitative data collected with an open-ended questionnaire. The study group of the research consists of students studying at a central secondary school in Ankara. In the data collection process; personal information form, online media expert opinion form, online safety and risk knowledge level determination tool and open-ended questionnaire were used. In the personal information form developed by the researchers; there are questions about the daily allocated time for the purposes of using the internet and the status of having previously received training on online security, information security or internet security. A measurement tool titled “Online Safety and Risk-Related Knowledge Level Determination Tool” developed by the researchers was used to measure the level of knowledge about online safety and risk for secondary school students. This measurement tool consists of 16 open-ended questions developed by determining the themes that should be included in the scope of the literature review. Within the scope of the study, an expert opinion form titled “Online Media Expert Opinion Form” was developed to evaluate the online environment develo-

ped by the researchers. Within the scope of the research, a semi-structured interview form was developed by the researchers in order to determine the effectiveness of the online learning environment. In order to determine the statistical methods to be used, it was tested whether the study groups showed a normal distribution or not. A computer-based statistics program was used for the analysis of quantitative data. Descriptive analysis and content analysis methods were used for the analysis of qualitative data.

The first research question of this study is “The level of knowledge of students about online safety and risk; how does the daily allotted time for the purposes of using the internet and online security change according to a previous training on information security or internet security? “. One-way ANOVA and independent groups t-test method were used to find an answer to this question. One-way ANOVA was used to determine the relationship between the daily time spent by the participants using the internet to read news and to follow the media, and their level of knowledge about online safety and risk. One-way ANOVA results showed that students’ knowledge levels about online safety and risk does not change depending on the amount of time spent per day using the internet to read news and to follow the media. One-way ANOVA was used to determine the relationship between the daily time spent by the participants for recreational use of the internet and their level of knowledge about online safety and risk. One-way ANOVA results showed that students’ knowledge levels about online safety and risk does not change depending on the amount of time spent on entertainment purposes. One-way ANOVA was used to determine the relationship between the daily time spent by the participants for using the internet for educational purposes (doing research, doing homework, continuing distance education) and their level of knowledge about online safety and risk. One-way ANOVA results showed that students’ knowledge levels about online safety and risk does not change depending on the amount of time spent daily using the internet for educational purposes (doing research, doing homework, continuing distance education). Independent groups t-test analysis was applied to determine the relationship between the participants’ status of having received any previous training on online security or information security and their knowledge level about online security and risk. According to the results of independent groups t-test analysis, students’ level of knowledge about online safety and risk does not change according to previous training on online security, information security, cyber security or internet security.

The second research question of the study is “What are the students’ views on the online environment developed?” in the form. All of the students (30) stated that the name of the online environment developed was appropriate and that the content available online was up-to-date.

The third research question of the research is “What is the effect of the environment designed for online security and risk-related education on the change in students’ knowledge about online security and risk?”. In order to test the effectiveness of the experimental practice conducted on students’ online safety and risk-related knowledge levels, pre-test and post-test scores were compared with dependent groups t-test, and it was determined that there was a significant increase in students’ knowledge levels about online safety and risk after the trainings.

The fourth and final research question of the research is “What is the effect of online safety and risk trainings on the retention of learning?”. In order to evaluate the experimental practice in terms of the retention of the learning, the posttest and permanence test scores of the study group were compared with the dependent groups’ t-test. It was concluded that there was a significant difference in the posttest and retention test scores of students’ knowledge levels about online safety and risk. This finding was interpreted as the training conducted in the online environment was not sufficient to ensure the permanence of the learned information.

To summarize the results obtained within the scope of the study, the online environments developed in accordance with the targeted achievements and the student level and the trainings carried out in accordance with the teacher’s planning through these environments; it can be said that it will contribute to student success. Nowadays, when the time spent in online environments is quite high, it is important for students to be informed about the security problems and risks they may encounter in online environments. For future studies, it can be suggested to conduct experimental studies in which different learning techniques are used for the use of online environments for control and experimental groups.

Keywords: *Online security, internet security, information security, cyber security, online learning, distance education.*

ÇEVİRİMİÇİ GÜVENLİK VE RISK İLE İLGİLİ EĞİTİME YÖNELİK GELİŞTİRİLMİŞ BİR ÇEVİRİMİÇİ ORTAMIN ORTAOKUL ÖĞRENCİLERİNİN BİLGİ DÜZEYLERİNE ETKİLERİ

ÖZ:

Bu araştırmanın amacı, çevrimiçi güvenlik ve risk ile ilgili eğitime yönelik tasarlanan bir çevrimiçi ortamda gerçekleştirilen eğitimlerin ortaokul öğrencilerinin çevrimiçi güvenlik ve risk ile ilgili bilgi düzeylerine etkisinin incelenmesidir. Araştırmada nicel verilerin toplandığı aşamada zayıf deneysel desenlerden tek grup ön test son test deseninden faydalanılmış, açık uçlu bir anket formu ile toplanan nitel veriler kullanılarak araştırmanın bulguları desteklenmiştir. Araştırmanın çalışma grubunu Ankara'da merkezi bir ortaokulda öğrenim görmekte olan öğrenciler oluşturmaktadır. Veri toplama sürecinde; kişisel bilgi formu, Çevrimiçi Güvenlik ve Risk Düzeyi belirleme aracı ve açık uçlu bir anket formu kullanılmıştır. Kullanılacak olan istatistiksel yöntemlerin belirlenmesi amacıyla, çalışma gruplarının normal dağılım gösterip göstermedikleri test edilmiştir. Nicel verilerin analizi için bilgisayar tabanlı bir istatistik programından yararlanılmıştır. Nitel verilerin analizi için ise betimsel analiz ve içerik analizi yöntemlerine başvurulmuştur. Çalışmada; öğrencilerin çevrimiçi güvenlik ve risk bilgi düzeylerinin; interneti kullanım amaçlarına yönelik günlük ayırdıkları süreye ve daha önce çevrimiçi güvenlik hakkında bir eğitim alma durumlarına bağlı olarak değişmediği sonucuna ulaşılmıştır. Araştırma sonuçları çevrimiçi ortamda verilen eğitimlerin öğrencilerin çevrimiçi güvenlik ve risk bilgi düzeyleri açısından katkı sağladığını göstermiştir. Ayrıca, ortamda verilen eğitimlerin öğrenilenlerin kalıcılığını sağlama konusunda yeteri kadar etkili olmadığı sonucuna ulaşılmıştır.

Anahtar Sözcükler: Çevrimiçi güvenlik, internet güvenliği, bilgi güvenliği, siber güvenlik, çevrimiçi öğrenme, uzaktan eğitim.

GİRİŞ

Çevrimiçi ortamlar içinde bulunduğumuz küresel salgın koşulları sebebiyle hayatımızı daha fazla etkiler hale gelmiştir. Salgının kontrolünü sağlayabilmek amacıyla, dünyada pek çok ülkede okullardaki yüz yüze eğitimler yerini uzaktan eğitime bırakmak durumunda kalmıştır.

COVID-19'un getireceği hasarlar hesaplanamamakla birlikte bu küresel krizin, eğitimi yeniden düşünmek için bir fırsat sunduğu söylenebilir (Zhao, 2020). COVID-19 salgını sürecinde yaşananlar, dünyada milyonlarca okulun işleyişini aksatmış ve okulların büyük ölçüde kapatılması kararının alınmasına yol açmıştır. Yine Zhao eğitimi yeniden tasarlama sürecinin, okulları iyileştirmek yerine tüm çocuklar için en iyi eğitim fırsatlarını yaratmakla ilgili olması gerektiğini savunmaktadır.

Küresel salgın sürecinde uzaktan eğitim ve yüz yüze eğitim arasında yapılan karşılaştırmalara sıkça rastlanmıştır. Moore vd. (2011) farklı öğrenme ortamlarının tasarımının, öğrenme hedefine, hedef kitleye, erişime (fiziksel, sanal ve/veya her ikisi) ve içerik türüne bağlı olabileceğini, öğrenme ortamının nasıl kullanılacağını bilmenin önemli olduğunu belirtmektedir. Bozkurt (2020) da eğitsel materyallerin kalitesinin tartışmaya açık bir konu olduğunu, ister uzaktan eğitimde ister yüz yüze eğitimde odak noktasının eğitimin sunumunda ve içeriklerde kalite güvencesinin sağlanması olduğunu belirtmektedir.

Sağiroğlu ve Alkan (2018) bilgi güvenliğini “bilginin, tehditlerden veya tehlikelerden korunması için doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılarak, her türlü ortamda istenmeyen kişiler tarafından elde edilmesini önleme girişi” olarak tanımlamışlardır. Safa vd. (2016) anti-virüs, güvenlik duvarı, kimlik doğrulama ve izinsiz giriş tespit sistemlerinin bilgi güvenliğini ele alan teknolojik önlemler olduğunu, ancak bu önlemlerin bilgi güvenliğini garanti edemediklerini belirtmektedirler. Kearney ve Kruger (2016) de çevrimiçi ortamlardaki risklerin sürekli değişmesi sebebiyle bilgi güvenliği farkındalık eğitimlerinin, risk profillerindeki değişiklikleri takip etmek amacıyla sürekli olarak yönetilmesi gerektiğine dikkat çekmektedir.

Bu çalışma kapsamında bilgi güvenliğinin bir alt boyutu olarak internete yani çevrimiçi ortamlara yönelik güvenlik konusuna yönelik bir çalışma gerçekleştirilmiştir. Bu doğrultuda, araştırma kapsamında “çevrimiçi güvenlik” kavramı kullanılmıştır. Hartikainen vd. (2019) çevrimiçi güvenliği, bir kişinin donanım, yazılım, bilgi ve fikri mülkiyet de dâhil olmak üzere mülkünün korunması olarak tanımlamıştır. Çevrimiçi güvenlik veya internet güvenliği sorununda en önemli faktörlerden birisi bireydir. Bu hususta Shillair vd. (2015) bir kullanıcının kişisel sorumluluk duygusunu geliştirmesinin, etkili çevrimiçi güvenlik müdahalelerinin gerekli öncüsü olduğunu belirtmiştir. Yine aynı çalışmada, interneti daha güvenli bir alan haline getirmek için, kullanıcıların bilgilerini ve özgüvenlerini artırmaya yönelik eğitime ihtiyaç duydukları vurgulanmaktadır. Çelen, Çelik ve Seferoğlu (2011) da bilgisayar ve internet teknolojilerinin yaygınlaşmasının bilgi edinme, iletişim gibi birçok yönden günlük hayatımıza katkı sağlarken çocuklar ve gençler için tehdit de oluşturmaya başladığını belirtmektedirler.

Sosyal medyanın ve diğer teknolojilerinin yaygın olarak kullanımı, çocukların çevrimiçi ortamlarda karşılaştıkları tehditler hakkında endişelere sebep olmaktadır (Boyd & Hargittai, 2013). Çevrimiçi güvenliğe yönelik bir alanyazın taraması yapıldığında ebeveynlerin ve akranların çocukların çevrimiçi güvenliğinde önemli aktörler olarak belirtilmesi dikkat çekmektedir (Hasebrink vd., 2011). Özellikle okullarda dijital teknolojilerin kullanımı arttıkça, öğretmenlerin de çocukları korurken kullanımlarını nasıl teşvik edecekleri sorusuyla karşı karşıya oldukları

vurgulanmaktadır (Ahn vd., 2011). Birçok ülkede okullarda dijital öğrenme, dijital katılım ve dijital okuryazarlığı teşvik etmeye yönelik farklı politikalar ve eğitim uygulamaları yer almaktadır (Ólafsson vd., 2013).

Avrupa Çevrimiçi Çocuklar (EU Kids Online) Projesi (2010) kapsamında 9-16 yaş aralığındaki çocukların dijital okuryazarlık ve güvenlik becerileri, interneti aşırı kullanımları, çevrimiçi aktivite sıklıkları, çevrimiçi içeriğin kalitesi, çocukların sosyal ağ kullanımları ve çevrimiçi ortamdaki risk deneyimlerine yönelik bir araştırma yapılmıştır. Araştırma raporunda, çocukların çoğunun, internette yaşadıkları olumsuz şeylerden rahatsız olmadıkları ve risklerin çocuklar tarafından üzücü ya da zararlı olarak algılanmadığı belirtilmiştir (Livingstone vd., 2011). Bu sonuç, çocukların çevrimiçi ortamdaki güvenlik sorunlarını önemsemedikleri ve bu sorunların çözümüne yönelik herhangi bir önlem alma ihtiyacı hissetmedikleri şeklinde yorumlanabilir. Avrupa Çevrimiçi Çocuklar Projesi kapsamında yayınlanan güncel rapora göre ise, bazı ülkelerde çocukların her gün çevrimiçi olarak geçirdiği sürenin 2010 yılına kıyasla neredeyse iki katı olarak belirlenmiştir (Smahel vd., 2020). Çocukların çevrimiçi ortamdaki olumsuz deneyimlerinin yaşla birlikte arttığı, çoğunun ebeveynlerinden, öğretmenlerinden veya arkadaşlarından çevrimiçi güvenlik konusuna yönelik herhangi bir çevrimiçi güvenlik tavsiyesi almadığı belirtilmiştir. Yine, çevrimiçi ortamda olumsuz deneyimle karşılaşan çocukların bu konu ile ilgili olarak, konuyu birisi ile paylaşmanın yanı sıra, pencereyi veya uygulamayı kapatmak, sorunu görmezden gelmek, kişiyi engellemek gibi davranışlar sergilediği raporlanmıştır (Smahel vd., 2020).

Çevrimiçi güvenlik ve internette güvenlik konusunda büyük sorumluluğun bireyde olduğu ve çocukların da çevrimiçi ortamları sıklıkla kullandıkları gerçeğinden hareketle; çocukların bu hususta farkındalık kazanmaları ve bu farkındalığı davranışlarına yansıtma olmasının önemli olduğu düşünülmektedir. Mıhçı ve Kılıç-Çakmak (2017) da internette sorumlu ve güvenli davranışların sergilenmesi için öğrencilere eğitim verilmesinin önemine dikkat çekmektedirler. Öte yandan Padlipsky (2018) yapmış olduğu bir çalışmada, siber güvenlik alanındaki çevrimiçi bir kursun, geleneksel sınıf yöntemlerini yansıtan çevrimdışı ve yüz yüze gerçekleştirilen etkinliklerle geliştirilip geliştirilemeyeceğini araştırmıştır. Araştırma bulguları, kursun hem çevrimiçi hem de çevrimdışı etkinliklerine katılan grubun siber güvenliğe karşı daha olumlu bir farkındalığa sahip olduğunu göstermiştir.

Yüz yüze eğitimin uygulanmadığı durumlarda, zaman zaman daha fazla bireye erişebilmek; mekân ve zaman açısından esneklik sağlayabilmek için uzaktan eğitim ve çevrimiçi eğitim bir fırsat sağlayabilmektedir. Küresel salgının yaşandığı şu günlerde çevrimiçi eğitim öğrencilere ve öğretmenlere pek çok fırsat sağlamış, çevrimiçi eğitimin farklı açılardan düşünülmesini sağlamıştır. Özellikle hedef kitle ve kazanımlar dikkate alınarak hazırlanmış çevrimiçi ortamlar çocukların

eğitiminde kilit rol oynayabilmektedir. Bu anlamda çevrimiçi güvenlik ve risk konularına yönelik tasarlanan bir çevrimiçi ortamda gerçekleştirilecek eğitimlerin ortaokul öğrencilerinin çevrimiçi güvenlik ve risk ile ilgili bilgi düzeyleri açısından önemli olduğu düşünülmektedir.

Araştırmanın Amacı

Bu araştırmanın amacı, çevrimiçi güvenlik ve risk ile ilgili eğitime yönelik tasarlanan bir çevrimiçi ortamda gerçekleştirilen eğitimlerin ortaokul öğrencilerinin çevrimiçi güvenlik ve risk ile ilgili bilgi düzeylerine etkisinin incelenmesidir. Bu amaca ulaşma sürecinde aşağıdaki araştırma sorularına yanıt aranmıştır.

- Öğrencilerin çevrimiçi güvenlik ve risk ile ilgili bilgi düzeyleri; interneti kullanım amaçlarına yönelik günlük ayrılan süre ve çevrimiçi güvenlik, bilgi güvenliği veya internet güvenliği hakkında daha önce bir eğitim alma durumuna göre nasıl değişmektedir?
- Çevrimiçi güvenlik ve risk ile ilgili eğitime yönelik tasarlanan ortamda yürütülen eğitimlerin öğrencilerin çevrimiçi güvenlik ve risk ile ilgili bilgi düzeylerindeki değişime etkisi nedir?
- Çevrimiçi ortamda yürütülen çevrimiçi güvenlik ve risk ile ilgili eğitimlerin öğrenilenlerin kalıcılığına etkisi nedir?
- Öğrencilerin geliştirilen çevrimiçi ortamın işlevselliğine yönelik görüşleri nelerdir?

YÖNTEM

Araştırma Modeli

Bu çalışmada nicel verilerin toplandığı aşamada zayıf deneysel desenlerden tek grup ön test son test deseninden faydalanılmıştır. Açık uçlu anket formu ile toplanan nitel verilerle ise araştırmanın nicel bulgularının desteklenmesi amaçlanmıştır. Araştırmanın çalışma grubu için deneysel desen ve süreç Tablo 1'de verilmiştir.

Tablo 1. Araştırmanın Çalışma Grubu İçin Deneysel Desen ve Süreç

| DeneySEL Süreçten Önceki İşlemler | Çalışma Grubu | Yöntem | DeneySEL Süreçten Sonraki İşlemler |
|--|---------------|--------------------------|--|
| Kişisel bilgi formunun uygulanması Çevrimiçi Güvenlik ve Risk Düzeyi belirleme aracının uygulanması | Öğrenciler | Çevrimiçi Ortamda Eğitim | Çevrimiçi güvenlik ve risk düzeyi belirleme aracının uygulanması Açık uçlu anket formunun uygulanması DeneySEL işlemden 4 hafta sonra kalıcılık testinin uygulanması (Çevrimiçi güvenlik ve risk düzeyi belirleme aracı) |

Çalışma Grubu

Araştırmanın çalışma grubunu, Ankara'da merkezi bir ortaokulda öğrenim görmekte olan ve Bilişim Teknolojileri ve Yazılım dersine katılan öğrenciler oluşturmuştur.

Katılımcılarla İlgili Demografik Bilgiler

Katılımcıların profili, interneti kullanım amaçlarına yönelik günlük ayrılan süre, çevrimiçi güvenlik, bilgi güvenliği veya internet güvenliği hakkında daha önce bir eğitim alma durumu açısından çeşitlilik göstermektedir. Araştırmanın deneysel uygulama sürecine 30 altıncı sınıf öğrencisi katılmış olup, öğrencilerden kişisel bilgi formu aracılığıyla elde edilen veriler alt başlıklar halinde sunulmuştur.

Katılımcıların İnterneti Haber Okumak- Medyayı Takip Etmek Amaçlı Kullanımda Günlük Harcadığı Süreye Göre Dağılımları

Çalışma grubundaki öğrencilerin %40'ının (12) 15 dk'dan az; %23,3'ünün (7) bir saatten az; %6,7'sinin (2) 1-3 saat haber okumak-medyayı takip etmek amaçlı günlük internet kullanımlarının olduğu; %30'unun (9) ise hiçbir zaman interneti haber okumak-medyayı takip etmek amaçlı kullanmadıkları görülmüştür (Bkz. Tablo 2).

Tablo 2. Katılımcıların Haber Okumak- Medyayı Takip Etmek Amaçlı Günlük Harcadığı Süreye Göre Dağılımları

| Günlük ortalama harcanılan zaman aralığı | f | % |
|--|-----------|------------|
| 1-3 saat | 2 | 6,7 |
| 1 saatten az | 7 | 23,3 |
| 15 dk'dan az | 12 | 40 |
| Hiçbir zaman | 9 | 30 |
| Toplam | 30 | 100 |

Katılımcıların İnterneti Eğlence Amaçlı Kullanımda Günlük Harcadığı Süreye Göre Dağılımları

Çalışma grubundaki öğrencilerin %56,7'sinin (17) 1-3 saat; %20'sinin (6) 1 saatten az; %13,3'ünün (4) 4-6 saat; %6,7'sinin (2) 15 dk'dan az; %3,3'ünün (1) günlük 7 saat ve üzeri interneti eğlence amaçlı kullanımlarının olduğu görülmüştür (Bkz. Tablo 3).

Tablo 3. Katılımcıların İnterneti Eğlence Amaçlı Kullanımda Günlük Harcadığı Süreye Göre Dağılımları

| Günlük Ortalama Harcanan Süre | f | % |
|-------------------------------|-----------|------------|
| 7 saat ve üzeri | 1 | 3,3 |
| 4-6 saat | 4 | 13,3 |
| 1-3 saat | 17 | 56,7 |
| 1 saatten az | 6 | 20 |
| 15 dk'dan az | 2 | 6,7 |
| Toplam | 30 | 100 |

Katılımcıların İnterneti Eğitim Amaçlı Kullanımda Günlük Harcadığı Süreye Göre Dağılımları

Katılımcıların, interneti eğitim amacıyla kullanmak (araştırma yapmak, ödev yapmak, uzaktan eğitime devam etmek) için günlük harcadığı süreye göre dağılımlarına bakıldığında, çalışma grubundaki öğrencilerden büyük çoğunluğunun (%76,7) interneti eğitim amacıyla kullanmak (araştırma yapmak, ödev yapmak, uzaktan eğitime devam etmek) için günlük 1-3 zaman ayırdıkları görülmüştür (Bkz. Tablo 4).

Tablo 4. Katılımcıların İnterneti Eğitim Amaçlı Kullanımda Günlük Harcadığı Süreye Göre Dağılımları

| Günlük Ortalama Harcanan Süre | n | % |
|-------------------------------|-----------|------------|
| 4-6 saat | 3 | 10 |
| 1-3 saat | 23 | 76,7 |
| 1 saatten az | 4 | 13,3 |
| Toplam | 30 | 100 |

Katılımcıların Çevrim İçi Güvenlik, Bilgi Güvenliği, Siber Güvenlik veya İnternet Güvenliği Hakkında Daha Önce Herhangi Bir Eğitim Alma Durumuna Göre Dağılımları

Katılımcıların çevrimiçi güvenlik, bilgi güvenliği, siber güvenlik veya internet güvenliği hakkında daha önce herhangi bir eğitim alma durumuna göre dağılımları incelendiğinde, çalışma grubundaki öğrencilerden büyük çoğunluğunun (%76,7) çevrimiçi güvenlik, bilgi güvenliği, siber güvenlik veya internet güvenliği hakkında daha önce herhangi bir eğitim almadığı görülmüştür (Bkz. Tablo 5).

Tablo 5. Katılımcıların Çevrim İçi Güvenlik, Bilgi Güvenliği, Siber Güvenlik veya İnternet Güvenliği Hakkında Daha Önce Herhangi Bir Eğitim Alma Durumuna Göre Dağılımları

| Eğitim Alma Durumu | n | % |
|--------------------|-----------|------------|
| Evet | 7 | 23,3 |
| Hayır | 23 | 76,7 |
| Toplam | 30 | 100 |

Araştırma Süreci

Araştırmanın deneysel uygulamaları 2020-2021 Eğitim-Öğretim yılı 1. yarısında gerçekleştirilmiştir. Deneysel uygulamalar, kişisel bilgi formu ve ön-testin (Çevrimiçi Güvenlik ve Risk Düzeyi belirleme aracı) uygulanması ile başlatılmış olup, son-test (Çevrimiçi Güvenlik ve Risk Düzeyi belirleme aracı) ve açık uçlu anket formunun uygulanması ile sürdürülmüştür. Son olarak ise, öğrenmenin kalıcılığının sınanabilmesi amacıyla, eğitimler tamamlandıktan dört hafta sonra çevrimiçi sistemdeki içerikler erişime kapatılarak daha önce uygulanmış olan Çevrimiçi Güvenlik ve Risk Düzeyi belirleme aracı tekrar uygulanmıştır. Araştırmanın deneysel uygulama sürecinde yapılan işlemler Tablo 6'da gösterilmiştir.

Tablo 6. Deneysel Uygulama Sürecinde Yapılan İşlemler

| Haftalar | Etkinlikler |
|------------------------|---|
| Hafta 1 | Katılımcıların süreç hakkında bilgilendirilmesi, katılımcıların çevrimiçi ortamı incelemesi, kişisel bilgi formu ve ön-testin (Çevrimiçi güvenlik ve risk düzeyi belirleme aracı) uygulanması |
| Hafta 2-Hafta 5 | Çevrimiçi ortamda öğrenme etkinlikleri |
| Hafta 6 | Açık uçlu anket formu ve son-testin (Çevrimiçi güvenlik ve risk ile düzeyi belirleme aracı) uygulanması |
| Hafta 10 | Öğrenmenin kalıcılığının sınanması amacıyla kalıcılık testinin (Çevrimiçi güvenlik ve risk düzeyi belirleme aracı) uygulanması |

Çevrimiçi ortamdaki öğrenme etkinlikleri kapsamında her hafta öğrencilere haftalık görevler verilmiştir. Her hafta çevrimiçi ortamdan bağımsız olarak video konferans aracı ile öğrencilerle eş zamanlı ders gerçekleştirilmiştir. Tablo 7’de öğrencilerin her hafta takip etmiş oldukları konular yer almaktadır.

Tablo 7. Öğrencilerin Takip Ettikleri Konuların Dağılımı

| Haftalar | Etkinlikler |
|----------------|--|
| Hafta 1 | İnternetin Bilinçli Kullanımı Ünitesi - Kişisel Verilerin Korunması Konusu İnternetin Bilinçli Kullanımı Ünitesi - Sosyal Ağlar Konusu Video konferans aracı ile eş zamanlı derse katılım |
| Hafta 2 | İnternetin Bilinçli Kullanımı Ünitesi – İnternet Okuryazarlığı Konusu İnternetin Bilinçli Kullanımı Ünitesi – Siber Zorbalık Konusu İnternetin Bilinçli Kullanımı Ünitesi – Çevrimiçi Riskler Konusu Ünite Sonu Etkinlikler Sayfası Video konferans aracı ile eş zamanlı derse katılım |
| Hafta 3 | İnternet ve Ağ Güvenliği Ünitesi -Şifre Güvenliği Konusu İnternet ve Ağ Güvenliği Ünitesi -Zararlı Yazılımlar Konusu Video konferans aracı ile eş zamanlı derse katılım |

| | |
|----------------|---|
| Hafta 4 | İnternet ve Ağ Güvenliği Ünitesi -Web Güvenlik Önlemleri Konusu |
| | İnternet ve Ağ Güvenliği Ünitesi -Güvenli Olmayan İletişim Yolları Konusu |
| | Ünite Sonu Etkinlikler Sayfası |
| | Video konferans aracı ile eş zamanlı derse katılım |

Çevrimiçi Ortamın Tasarımı Süreci

Çevrimiçi öğrenme ortamının geliştirilmesi amacıyla ayrıntılı bir alanyazın taraması yapılmış ve etkili bir çevrimiçi öğrenme ortamının sahip olması gereken özellikler belirlenmiştir. Çevrimiçi öğrenme ortamlarının tasarım sürecine yönelik alanyazında farklı tasarım önerileri yer almakla birlikte çalışmada kullanılacak ortam için Tüzün'ün (2011) dokuz aşamalı tasarım önerisine benzer bir tasarım modeli hazırlanmıştır (Bkz. Tablo 8).

Tablo 8. Çevrimiçi Öğrenme Ortamının Tasarım Süreci

| | Tasarım Aşaması | Yürütülen İşlemler |
|---|--|---|
| 1 | Tasarım Öncesi İşlemler | Kazanımların belirlenmesi |
| 2 | Analiz işinin yapılması | Hedef kitlenin özelliklerinin belirlenmesi, fiziksel imkânların tespiti |
| 3 | Personelin Belirlenmesi | Çevrimiçi ortam geliştirmesi sürecinde görevli olacak personelin belirlenmesi, görev dağılımının gerçekleştirilmesi |
| 4 | Tasarım/Geliştirme işinin yapılması | Belirlenen kazanımlar, yöntem ve teknikler ile fiziksel imkânlar göz önünde bulundurularak tasarım işinin yapılması |
| 5 | Uzmanların değerlendirilmesi | Uzmanların, kendilerine sunulan ölçütler doğrultusunda ortamı değerlendirmesi, görüş alınması |
| 6 | Ortamdaki sorunların giderilmesi | Uzman geribildirimleri doğrultusunda ortamdaki sorunların giderilmesi, önerilerin gerçekleştirilmesi |
| 7 | Pilot uygulama | Pilot bir grupla ortamın kullanılabilirlik çalışmasının yapılması |

Ortamın değerlendirilmesinde dikkate alınan ölçütlerin belirlenebilmesi ama-

cıyla bir alanyazın taraması yapılmıştır. Çevrimiçi ortam tasarımı sürecinde ortamın sahip olması gereken özelliklerin belirlenmesi amacıyla ise, Eren ve Erdem'in (2020) geliştirdiği "Çocuğa Kendini Koruma Bilinci Kazandırma Amaçlı Çevrimiçi Ortamlar Ölçeği" başlıklı ölçeğin maddeleri ölçüt olarak kabul edilmiştir. Bu bağlamda ölçek ölçütlerinden ortama erişim boyutu, motivasyon boyutu, öğrenme boyutu, içerik boyutu, aktif destek sistemi boyutu dikkate alınmıştır. Araştırmacının hazırladığı eğitim içeriğini değerlendirme ölçütleri ortamdaki sorunların belirlenmesi amacıyla kullanılmıştır. Sekiz alan uzmanından belirlenen ölçütler kapsamında görüşler alınmış, gelen öneriler doğrultusunda ortamda birtakım düzenlemeler yapılmıştır.

Veri Toplama Araçları

Araştırma sürecinde deneysel işlemin öncesinde ve sonrasında veri toplama işlemi gerçekleştirilmiştir. Veri toplamak amacıyla, "Kişisel Bilgi Formu, Çevrimiçi Ortam Uzman Görüş Formu, Çevrimiçi Güvenlik ve Risk Düzeyi Belirleme Aracı ve Açık Uçlu Anket Formu" kullanılmıştır. Araştırmacılar tarafından geliştirilen kişisel bilgi formunda; interneti kullanım amaçlarına yönelik günlük ayrılan süre ve çevrimiçi güvenlik, bilgi güvenliği veya internet güvenliği hakkında daha önce bir eğitim alma durumuna yönelik sorular yer almaktadır.

Ortaokul öğrencilerine yönelik çevrimiçi güvenlik ve risk ile ilgili bilgi düzeylerini ölçmek amacıyla araştırmacılar tarafından geliştirilen "Çevrimiçi Güvenlik ve Risk Düzeyi Belirleme Aracı" başlıklı bir ölçme aracı kullanılmıştır. Çevrimiçi Güvenlik ve Risk Düzeyi Belirleme Aracı, alanyazın taraması doğrultusunda kapsama dâhil edilmesi gereken temalar belirlenerek geliştirilen 16 açık uçlu sorudan oluşmaktadır. Soruların anlaşılabilirliği ve öğrenci seviyesine uygunluğunu ortaya çıkarabilmek amacıyla hazırlanan ölçme aracı dokuz altıncı sınıf öğrencisine uygulanmıştır. Bu süreçte öğrencilerin seviyesine uygun olmadığı düşünülen iki soru testten çıkartılmıştır. 14 soruluk testin değerlendirmesi ise 10 alan uzmanınca yapılmıştır. Uzman görüşleri doğrultusunda; benzer kazanımları ölçtüğü düşünülen ve kapsam geçerlik oranının düşük olduğu belirlenen üç soru testten çıkartılmış, bazı sorularda ise birtakım düzenlemeler gerçekleştirilmiştir. 11 soruya indirgenen ölçme aracının KGİ 0.94 olarak belirlenmiştir. Başvurulan uzman sayısı 10 olduğu için, kapsam geçerlik ölçütü 0,62 olarak kabul edilmiş; KGİ > KGÖ olduğundan, geliştirilen aracın kapsam geçerliğinin istatistiksel olarak anlamlı olduğuna karar verilmiştir (Veneziano & Hooper, 1997). Öte yandan iki dil bilgisi uzmanının görüşlerine dayanarak aracın son düzenlemeleri yapılmıştır. Çevrimiçi güvenlik ve risk düzeyi belirleme aracının güvenilirliğini belirleyebilmek amacıyla, ön-test sonuçları iki ayrı kodlayıcı tarafından kodlanmış, her soru için Kappa istatistiği kullanılmış ve kodlayıcı uyum değerleri hesaplanmıştır.

Çevrimiçi ortam tasarımı sürecinde ortamın sahip olması gereken özelliklerin belirlenmesi amacıyla “Çevrimiçi Ortam Uzman Görüş Formu” başlıklı bir uzman görüş formu geliştirilmiştir. Bu form hazırlanırken Eren ve Erdem’in (2020) geliştirmiş oldukları ölçütler listesinden faydalanılmıştır. Eren ve Erdem’in (2020) geliştirdiği “Çocuğa Kendini Koruma Bilinci Kazandırma Amaçlı Çevrimiçi Ortamlar Ölçeği” başlıklı ölçekte yer alan ölçütlerin kullanımı için gerekli izinler alınmıştır. Ortam tasarımı sürecinde, ortamdaki sorunların belirlenmesi amacıyla, sekiz alan uzmanından belirlenen ölçütler kapsamında görüşler alınmış, gelen öneriler doğrultusunda ortamda birtakım düzenlemeler yapılmıştır.

Araştırma kapsamında çevrimiçi öğrenme ortamının etkililiğinin belirlenebilmesi amacıyla araştırmacılar tarafından açık uçlu bir anket formu geliştirilmiştir. Bu formda “Sitede bulunan içerikler güncel midir? Video ve anlatıların süresi sizce ne kadar olmalıdır (daha uzun-kısa)?” şeklinde sorular yer almaktadır.

Etik Kurul İzin Bilgileri

Çalışmanın yürütülebilmesi için etik izinler ilgili kurumlardan alınmıştır. Veri toplama süreci ve çevrimiçi ortamdaki eğitimlere katılım süreci gönüllük esasına göre yürütülmüş olup, öğrencilerin velilerinden gerekli izinler çevrimiçi ortamda bir form aracılığıyla alınmıştır.

Etik Değerlendirmeyi Yapan Kurul: Hacettepe Üniversitesi Rektörlük

Evrak No: 35853172-300

Tarih: 12.11.2019

Etik Değerlendirmeyi Yapan Kurul: Ankara Valiliği Milli Eğitim Müdürlüğü

Evrak No: 14588481-605.99-E. 24100798

Tarih: 04.12.2019.

Çevrimiçi Güvenlik ve Risk Düzeyi Belirleme Aracı Kodlayıcı Uyum Analizleri

Araştırmacı tarafından geliştirilmiş olan Çevrimiçi Güvenlik ve Risk Düzeyi belirleme aracının güvenilirliğini belirleyebilmek amacıyla ön-test sonuçları iki ayrı kodlayıcı tarafından kodlanmış, her soru için Kappa istatistiği kullanılmış ve kodlayıcı uyum değerleri hesaplanmıştır. Ölçme aracında yer alan soruların Kappa değerlerinin yorumlanabilmesi amacıyla Landis ve Koch (1977)’in önerdiği tablo dikkate alınmıştır (Bkz. Tablo 9).

Tablo 9. Kappa İstatistiği Değeri ve Uyum Yorumu

| Kappa Değer Aralığı | Uyum Güçlülüğü |
|---------------------|----------------|
| <0.00 | Zayıf-kötü |
| 0.00-0.20 | Hafif |
| 0.21-0.40 | Makul |
| 0.41-0.60 | Orta |
| 0.61-0.80 | Önemli, güçlü |
| 0.81-1.00 | Mükemmel |

Kappa istatistiği kullanılarak hesaplanan kodlayıcı uyum değerleri Tablo 10'da sunulmuştur:

Tablo 10. Ön-teste Yönelik Kappa İstatistiği Sonuçlarının Dağılımı

| Sorular | Cohen Kappa Sayısı | Spearman Korelasyon Değeri |
|---------|--------------------|----------------------------|
| 1 | 1,000 | 1,000 |
| 2 | ,923 | ,911 |
| 3 | ,712 | ,760 |
| 4 | ,660 | ,873 |
| 5 | ,779 | ,790 |
| 6 | ,737 | ,942 |
| 7 | ,722 | ,843 |
| 8 | ,720 | ,799 |
| 9 | ,685 | ,753 |
| 10 | ,705 | ,708 |
| 11 | ,671 | ,723 |

Tablo 10'da görüldüğü üzere; Landis ve Koch (1977)'in önerdiği değerler dik-kate alınarak (Bkz. Tablo 9); ölçme aracında yer alan 3., 4., 5., 6., 7., 8., 9., 10. ve 11. soruların uyum düzeyinin güçlü; 1. ve 2. soruların uyum düzeyinin ise mükemmel olduğu; ölçme aracının bu veriler doğrultusunda güvenilir olduğu söylenebilir.

Verilerin Analizi

Araştırmanın nicel verilerinin analizi için kullanılacak olan istatistik yöntemleri belirlenirken, örneklem büyüklüğünün 50'den az olması sebebiyle Shapiro-Wilks testiyle normallik varsayımı sınanmıştır. Nitel verilerin toplanması amacıyla kullanılmış olan açık uçlu anket formunun analizi için ise içerik sırasıyla betimsel analiz ve içerik analizi yöntemlerine başvurulmuştur.

Araştırmanın veri kaynaklarını, veri toplanması ve veri analizini içeren araştırma süreci Tablo 11'de sunulmuştur.

Tablo 11. Çalışma Grubu için Araştırmanın Anahatları

| Araştırma Problemi | Veri Kaynağı | Verilerin Toplanması | Veri Analizi |
|---|--------------|--|--|
| Çevrimiçi güvenlik ve risk ile ilgili bilgi düzeyleri; interneti kullanım amaçlarına yönelik günlük ayrılan süre ve çevrimiçi güvenlik, bilgi güvenliği veya internet güvenliği hakkında daha önce bir eğitim alma durumuna göre nasıl değişmektedir? | Öğrenciler | Kişisel Bilgi Formu Çevrimiçi güvenlik ve risk düzeyi belirleme aracı | Betimsel İstatistikler Bağımsız Gruplar T-Testi Tek Faktörlü Varyans Analizi |
| Çevrimiçi güvenlik ve risk ile ilgili eğitime yönelik tasarlanan ortamda yürütülen eğitimlerin öğrencilerin çevrimiçi güvenlik ve risk ile ilgili bilgi durumlarındaki değişime etkisi nedir? | Öğrenciler | Çevrimiçi güvenlik ve risk düzeyi belirleme aracı | Bağımlı Gruplar T-Testi |
| Çevrimiçi ortamda yürütülen çevrimiçi güvenlik ve risk ile ilgili eğitimlerinin öğrenilenlerin kalıcılığına etkisi nedir? | Öğrenciler | Çevrimiçi güvenlik ve risk düzeyi belirleme aracı | Bağımlı Gruplar T-Testi |
| Öğrencilerin, geliştirilen çevrimiçi ortama yönelik görüşleri nelerdir? | Öğrenciler | Açık uçlu anket formu | Betimsel analiz ve içerik analizi |

BULGULAR

Bu bölümde ön-teste yönelik kodlayıcı uyum analizleri bulguları ve araştırma sorularına yönelik bulgular yer almaktadır. Bulgular bu araştırmanın amacı doğrultusunda belirlenen araştırma soruları ayrı ayrı cevaplandırılacak şekilde sunulmuştur.

Öğrencilerin Çevrimiçi Güvenlik ve Risk ile İlgili Bilgi Düzeylerinin İnterneti Kullanım Amaçlarına Yönelik Günlük Ayrılan Süre ve Çevrimiçi Güvenlik, Bilgi Güvenliği veya İnternet Güvenliği Hakkında Daha Önce Bir Eğitim Alma Durumuna Bağlı Olarak Değişiklik Durumu

Bu çalışmanın ilk araştırma sorusu “Öğrencilerin çevrimiçi güvenlik ve risk ile ilgili bilgi düzeyleri; interneti kullanım amaçlarına yönelik günlük ayrılan süre ve çevrimiçi güvenlik, bilgi güvenliği veya internet güvenliği hakkında daha önce bir eğitim alma durumuna göre nasıl değişmektedir?” şeklinde belirlenmiştir. Çalışma grubunun çevrimiçi güvenlik ve risk ile ilgili bilgi düzeyleri için verilerin normal dağılım gösterip göstermediğini belirlemek amacıyla ön-test ve son-test verilerine yönelik uygulanan Shapiro-Wilks testinin sonuçları Tablo 12’de verilmiştir.

Tablo 12. Ön-Test ve Son Test Sonuçlarına İlişkin Shapiro-Wilks Normallik Testi Sonuçlarının Dağılımı

| Test | N | X | S | Sd | t | P |
|----------|----|-------|-------|----|-------|-------|
| Ön-test | 30 | 64,70 | 18,15 | 29 | -8,50 | 0,000 |
| Son-test | 30 | 91,80 | 14,92 | | | |

Tablo 12’de görüldüğü üzere, ön-test ve son-test sonuçlarına yönelik uygulanan Shapiro-Wilks testi analiz sonuçlarına göre $p > .05$ olduğundan; çalışmaya katılan grubun normal dağılım gösterdiğine karar verilmiştir. Bu doğrultuda, öğrencilerin çevrimiçi güvenlik ve risk ile ilgili bilgi düzeylerinin interneti kullanım amaçlarına yönelik günlük ayrılan süre ve çevrimiçi güvenlik, bilgi güvenliği veya internet güvenliği hakkında daha önce bir eğitim alma durumuna bağlı olarak nasıl değiştiğini belirlemek amacıyla tek yönlü varyans analizi ve bağımsız gruplar t-testinin kullanılmasının uygun olduğuna karar verilmiştir.

Öğrencilerin Çevrimiçi Güvenlik ve Risk Düzeyinin İnterneti Kullanım Amaçlarına Yönelik Günlük Ayrılan Süreye Bağlı Olarak Nasıl Değiştiğine Yönelik Bulgular

Katılımcıların çevrimiçi güvenlik ve risk düzeyinin interneti haber okumak-medya takip etmek amaçlı, eğlence amaçlı ve eğitim amaçlı kullanıma (araştırma yapmak, ödev yapmak, uzaktan eğitime devam etmek) yönelik günlük ayrılan

süreye bağlı olarak nasıl değiştiğine yönelik bulgular ayrı başlıklar halinde sunulmuştur.

Öğrencilerin Çevrimiçi Güvenlik ve Risk Düzeyinin İnterneti Haber Okumak-Medyayı Takip Etmek Amaçlı Kullanıma Yönelik Günlük Ayırdığı Süreye Bağlı olarak Nasıl Değiştiğine Yönelik Bulgular

Katılımcıların çevrimiçi güvenlik ve risk düzeyinin interneti haber okumak-medyaı takip etmek amaçlı kullanıma yönelik günlük ayırdığı süreye bağlı olarak nasıl değiştiğinin belirlenmesi amacıyla tek faktörlü varyans analizine başvurulmuştur. Bu analizin sonuçları Tablo 13'te verilmiştir.

Tablo 13. Katılımcıların İnterneti Haber Okumak- Medyaı Takip Etmek Amaçlı Kullanıma Yönelik Günlük Harcadığı Süre ile Çevrimiçi Güvenlik ve Risk ile İlgili Bilgi Düzeylerine Göre Tek Faktörlü Varyans Analizi Sonuçlarının Dağılımı

| Varyansın Kaynağı | Kareler Toplamı | sd | Kareler Ortalaması | F | p | Anlamlı Fark |
|-------------------|-----------------|-----------|--------------------|-----|-----|--------------|
| Gruplararası | 987,06 | 3 | 329.02 | .99 | .40 | |
| Gruplarıçi | 8573,23 | 26 | 329.74 | | | - |
| Toplam | 9560.30 | 29 | | | | |

Tek faktörlü varyans analizi sonuçları, öğrencilerin çevrimiçi güvenlik ve risk ile ilgili bilgi düzeylerinin; interneti haber okumak- medyaı takip etmek amaçlı kullanımda günlük harcadığı süreye bağlı olarak değişmediğini göstermektedir, $F(3, 26) = .99, p > .05$.

Öğrencilerin Çevrimiçi Güvenlik ve Risk Düzeyinin İnterneti Eğlence Amaçlı Kullanıma Yönelik Günlük Ayırdığı Süreye Bağlı olarak Nasıl Değiştiğine Yönelik Bulgular

Katılımcıların interneti eğlence amaçlı kullanıma yönelik günlük harcadığı süreye göre çevrimiçi güvenlik ve risk ile ilgili bilgi düzeylerinin farklılaşp farklılaşmadığının belirlenmesi amacıyla tek faktörlü varyans analizine başvurulmuştur. Bu analizin sonuçları Tablo 14'te verilmiştir.

Tablo 14. Katılımcıların İnterneti Eğlence Amaçlı Kullanıma Yönelik Günlük Harcadığı Süre ile Çevrimiçi Güvenlik ve Risk ile İlgili Bilgi Düzeylerine Göre Tek Faktörlü Varyans Analizi Sonuçlarının Dağılımı

| Varyansın Kaynağı | Kareler Toplamı | sd | Kareler Ortalaması | F | p | Anlamlı Fark |
|-------------------|-----------------|----|--------------------|------|-----|--------------|
| Gruplararası | 2765,19 | 4 | 691.30 | 2.54 | .06 | |
| Gruplarıçi | 6795,11 | 25 | 271.80 | | | - |
| Toplam | 9560,30 | 29 | | | | |

Tek faktörlü varyans analizi sonuçları, öğrencilerin çevrimiçi güvenlik ve risk ile ilgili bilgi düzeylerinin; interneti eğlence amaçlı kullanımda günlük harcadığı süreye bağlı olarak değişmediğini göstermektedir [$F(4, 25) = 2,54, p > .05$].

Öğrencilerin Çevrimiçi Güvenlik ve Risk Düzeyinin İnterneti Eğitim Amacıyla (Araştırma Yapmak, Ödev Yapmak, Uzaktan Eğitime Devam Etmek) Kullanmaya Yönelik Günlük Ayırdığı Süreye Bağlı olarak Nasıl Değiştiğine Yönelik Bulgular

Katılımcıların interneti eğitim amacıyla (araştırma yapmak, ödev yapmak, uzaktan eğitime devam etmek) kullanmaya yönelik günlük harcadığı süre ile çevrimiçi güvenlik ve risk ile ilgili bilgi düzeyleri arasındaki ilişkinin belirlenmesi amacıyla tek faktörlü varyans analizine başvurulmuştur. Bu analizin sonuçları Tablo 15'te verilmiştir:

Tablo 15. Katılımcıların İnterneti Eğitim Amacıyla Kullanmak (Araştırma Yapmak, Ödev Yapmak, Uzaktan Eğitime Devam Etmek) için Günlük Harcadığı Süre ile Çevrimiçi Güvenlik ve Risk ile İlgili Bilgi Düzeylerine Göre Tek Faktörlü Varyans Analizi Sonuçlarının Dağılımı

| Varyansın Kaynağı | Kareler Toplamı | sd | Kareler Ortalaması | F | P | Anlamlı Fark |
|-------------------|-----------------|----|--------------------|------|-----|--------------|
| Gruplararası | 1199,92 | 2 | 599,96 | 1.93 | .16 | |
| Gruplarıçi | 8360,37 | 27 | 309,64 | | | - |
| Toplam | 9560,30 | 29 | | | | |

Tek faktörlü varyans analizi sonuçları, öğrencilerin çevrimiçi güvenlik ve risk ile ilgili bilgi düzeylerinin; interneti eğitim amacıyla (araştırma yapmak, ödev yapmak, uzaktan eğitime devam etmek) kullanıma yönelik günlük harcadığı süreye bağlı olarak değişmediğini göstermektedir, $F(2, 27) = 1.93, p > .05$.

Katılımcıların Çevrimiçi Güvenlik, Bilgi Güvenliği, Siber Güvenlik veya İnternet Güvenliği Hakkında Daha Önce Herhangi Bir Eğitim Alma Durumu ile Çevrimiçi Güvenlik ve Risk ile İlgili Bilgi Düzeyleri Arasındaki İlişki

Çalışmaya katılan grubun ön-test sonuçlarının normal dağılım gösterdiğine

karar verilmesi sebebiyle (Bkz. Tablo 12), katılımcıların çevrimiçi güvenlik, bilgi güvenliği, siber güvenlik veya internet güvenliği hakkında daha önce herhangi bir eğitim alma durumu ile çevrimiçi güvenlik ve risk ile ilgili bilgi düzeyleri arasındaki ilişkinin belirlenmesi amacıyla bağımsız gruplar t-testi analizine başvurulmuştur. Bu analizin sonuçları Tablo 16’da verilmiştir:

Tablo 16. Katılımcıların Çevrimiçi Güvenlik, Bilgi Güvenliği, Siber Güvenlik veya İnternet Güvenliği Hakkında Daha Önce Herhangi Bir Eğitim Alma Durumu ve Çevrimiçi Güvenlik ve Risk ile İlgili Bilgi Düzeylerine Göre Bağımsız Gruplar T-Testi Sonuçlarının Dağılımı

| Eğitim Alma Durumu | N | X | S | sd | t | p |
|--------------------|----|-------|-------|----|-----|-----|
| Evet | 7 | 62,85 | 27,05 | 28 | .30 | .76 |
| Hayır | 23 | 65,26 | 15,27 | | .22 | |

Bağımsız gruplar t-testi sonuçlarına göre, öğrencilerin çevrimiçi güvenlik ve risk ile ilgili bilgi düzeyleri; çevrimiçi güvenlik, bilgi güvenliği, siber güvenlik veya internet güvenliği hakkında daha önce herhangi bir eğitim alma durumuna göre değişmemektedir, $t(28)=.30, p>.05$.

Çevrimiçi Ortamda Yürütülen Eğitimlerin Öğrencilerin Çevrimiçi Güvenlik ve Risk ile İlgili Bilgi Durumlarındaki Değişimine Olan Etkisine Yönelik Bulgular

Bu çalışmanın ikinci araştırma sorusu “Çevrimiçi güvenlik ve risk ile ilgili eğitime yönelik tasarlanan ortamda yürütülen eğitimlerin öğrencilerin çevrimiçi güvenlik ve risk ile ilgili bilgi durumlarındaki değişime etkisi nedir?” şeklinde belirlenmiştir. Çalışma grubunun çevrimiçi güvenlik ve risk ile ilgili bilgi düzeyleri için verilerin normal dağılım gösterip göstermediğini belirlemek amacıyla ön-test ve son-test verilerine yönelik Shapiro-Wilks testi kullanılmış, her iki test için $p>.05$ olduğundan; grubun normal dağılım gösterdiğine karar verilmiştir. Yürütülen deneysel uygulamanın öğrencilerin çevrimiçi güvenlik ve risk ile ilgili bilgi düzeyleri üzerindeki etkililiğinin test edilmesi amacıyla ön-test ve son-test puanları karşılaştırılmıştır. Sonuçlarının karşılaştırılmasına ilişkin bağımlı gruplar t-testi sonuçları Tablo 17’de verilmiştir.

Tablo 17.Çalışma Grubunun Ön-test ve Son-test Sonuçlarının Karşılaştırılmasına İlişkin Bağımlı Gruplar T-Testi Sonuçlarının Dağılımı

| Test | N | X | S | Sd | t | p |
|----------|----|-------|-------|----|------|-----|
| Ön-test | 30 | 64,70 | 18,15 | 29 | 8.50 | .00 |
| Son-test | 30 | 91,80 | 14,92 | | | |

Tablo 17’de görüldüğü üzere, çevrimiçi ortamda yapılan eğitimler sonrasında öğrencilerin çevrimiçi güvenlik ve risk ile ilgili bilgi düzeylerinde anlamlı bir artış olduğu belirlenmiştir, $t(29)=-8.50$, $p<.05$. Öğrencilerin eğitim öncesi Çevrimiçi Güvenlik ve Risk Düzeyi puanları ortalaması $X= 64.70$ iken, eğitim sonrasında Çevrimiçi Güvenlik ve Risk Düzeyi puanları ortalaması $X= 91.80$ olarak belirlenmiştir. Bu bulgu, çevrimiçi ortamda yürütülen çevrimiçi güvenlik ve risk ile ilgili eğitimlerin, öğrencilerin çevrimiçi güvenlik ve risk ile ilgili bilgi düzeylerini artırmada önemli bir etkisinin olduğu şeklinde yorumlanabilir.

Çevrimiçi Ortamda Yürütülen Çevrimiçi Güvenlik ve Risk ile İlgili Eğitimlerin Öğrenilenlerin Kalıcılığına Etkisine Yönelik Bulgular

Bu çalışmanın üçüncü araştırma sorusu “Çevrimiçi ortamda yürütülen çevrimiçi güvenlik ve risk ile ilgili eğitimlerin öğrenilenlerin kalıcılığına etkisi nedir?” şeklinde belirlenmiştir. Çalışma grubunun çevrimiçi güvenlik ve risk ile ilgili bilgi düzeyleri için verilerin normal dağılım gösterip göstermediğini belirlemek amacıyla kalıcılık testi verilerine yönelik Shapiro-Wilks testi kullanılmış ve analiz sonuçları $p>.05$ olduğundan (Tablo 18); grubun normal dağılım gösterdiğine karar verilmiştir.

Tablo 18. Kalıcılık Testi Sonuçlarına İlişkin Shapiro-Wilks Normallik Testi Sonuçlarının Dağılımı

| Uygulanan Test | df | P |
|-----------------|----|-----|
| Kalıcılık Testi | 30 | .38 |

Deneyel uygulamanın öğrenilenlerin kalıcılığı açısından değerlendirilebilmesi amacıyla çalışma grubunun son-test ve kalıcılık testi puanları karşılaştırılmıştır. Çalışma grubunun son-test ve kalıcılık testi sonuçlarının karşılaştırılmasına ilişkin bağımlı gruplar t-testi sonuçları Tablo 19’da verilmiştir.

Tablo 19. Çalışma Grubunun Son-test ve Kalıcılık Testi Sonuçlarının Karşılaştırılmasına İlişkin Bağımlı Gruplar T-Testi Sonuçları

| Test | N | X | S | Sd | t | P |
|-----------------|----|-------|-------|----|------|-----|
| Son-Test | 30 | 91.80 | 14.92 | 29 | 2.10 | .04 |
| Kalıcılık Testi | 30 | 87.26 | 14.26 | | | |

Tablo 19’da görüldüğü üzere, öğrencilerin çevrimiçi güvenlik ve risk ile ilgili bilgi düzeylerinde anlamlı farklılık olduğu belirlenmiştir, $t(29)=2.10$, $p<.05$. Öğrencilerin son-testten almış oldukları Çevrimiçi Güvenlik ve Risk Düzeyi puanları ortalaması $X=91.80$ iken, eğitim tamamlandıktan dört hafta sonra yapılan kalıcılık testinde çevrimiçi güvenlik ve risk düzeyi puanları ortalamasının $X=87.26$ olduğu görülmüştür. Bu veriler, çevrimiçi ortamda yürütülen eğitimlerin öğrenilen bilgilerin kalıcılığını sağlama açısından yeterli olmadığını göstermektedir.

Öğrencilerin, Geliştirilen Çevrimiçi Ortamın İşlevselliğine Yönelik Görüşleri

Bu çalışmanın dördüncü ve son araştırma sorusu “Öğrencilerin, geliştirilen çevrimiçi ortamın işlevselliğine yönelik görüşleri nelerdir?” şeklinde belirlenmiştir. Araştırma kapsamında geliştirilen ortamın kullanılabilirlik sorunlarının ve işlevselliğinin belirlenebilmesi amacıyla uzman görüşleri dikkate alınarak araştırmacı tarafından açık uçlu bir anket formu geliştirilmiştir. Çevrimiçi ortamdaki eğitimlere katılan öğrencilerin geliştirilen ortamın işlevselliğine yönelik görüşleri açık uçlu anket formu aracılığıyla elde edilmiştir. Açık uçlu bir anket formu ile elde edilen veriler alt başlıklar halinde sunulmuştur:

Sitenin İsminin Uygunluğuna Yönelik Bulgular

Çalışma grubundaki öğrencilerin tamamı (30) geliştirilen çevrimiçi ortamın ismini uygun bulduklarını belirtmiştir.

Sitede Bulunan İçeriklerin Güncelliğine Yönelik Bulgular

Çalışma grubundaki öğrencilerin tamamı (30) çevrimiçi ortamda bulunan içeriklerin güncel olduğunu düşündüklerini belirtmiştir.

Video ve Anlatıların Süresinin Ne Kadar Olması (Daha Uzun-Kısa) Gerektiğine Yönelik Bulgular

Geliştirilen çevrimiçi ortamda yer alan video ve anlatıların süresi ile ilgili olarak; 12 öğrenci, sürelerin ideal olduğunu; yedi öğrenci sürenin daha kısa olması ge-

rektiğini, altı öğrenci sürenin daha uzun olması gerektiğini; beş öğrenci ise süreleri konu içeriğine göre değişmesi gerektiğini belirtmiştir.

“Kendimizi Sınayalım” Bölümleri Hakkında Ne Düşünüldüğüne Yönelik Bulgular

Geliştirilen çevrimiçi ortamda yer alan “Kendimizi Sınayalım” bölümleri ile ilgili olarak 25 öğrenci; “kendimizi sınavalım” bölümlerinin, konuları pekiştirmeleri için yardımcı olduğunu, verilen örneklerle konuyu daha iyi anladıklarını, bu bölümü etkili ve keyifli bulduklarını belirtmişlerdir. Beş öğrenci ise, “Kendimizi Sınayalım” bölümlerindeki soru sayısının az olduğunu belirtmiştir.

“Etkinlikler” Başlıklı Bölümde Yer Alan Etkinlikler Hakkında Ne Düşünüldüğüne Yönelik Bulgular

Geliştirilen çevrimiçi ortamda yer alan “Etkinlikler” bölümü ile ilgili olarak 26 öğrenci; etkinliklerin tamamının ilgisini çektiğini, dört öğrenci, mobil teknolojiler aracılığıyla etkinlikleri uygularken sorun yaşadıklarını; iki öğrenci etkinliklerin ilgisini çekmediğini, iki öğrenci bazı etkinliklerin ilgisini çektiğini, bir öğrenci ise “Örnek Durum Çözümleme” etkinliğini beğenmediğini belirtmiştir.

Çevrimiçi Ortamın En Çok Hangi Yönünün Beğenildiğine Yönelik Bulgular

Geliştirilen çevrimiçi ortamın en çok hangi yönünün beğenildiğine yönelik; sekiz öğrenci oyunlar bölümünü; sekiz öğrenci içeriklerin faydalı, eğitici, açık ve anlaşılır olmasını; altı öğrenci ortamın keyifli ve eğlenceli olmasını; altı öğrenci etkinlikleri; dört öğrenci videoları; iki öğrenci soru sor bölümünü; iki öğrenci site-deki bütün bölümleri beğendiğini; bir öğrenci “arkadaşlar” bölümünü beğendiğini; bir öğrenci ise ortamı öğretmeninin geliştirmesinin ilgisini çektiğini belirtmiştir.

Çevrimiçi Ortamın En Az Hangi Yönünün Beğenildiğine Yönelik Bulgular

Geliştirilen çevrimiçi ortamın en az hangi yönünün beğenildiğine yönelik 11 öğrenci, geliştirilen çevrimiçi ortamda beğenmediği bir yön olmadığını; dört öğrenci, oyunlarda zaman zaman hatalar oluştuğunu; iki öğrenci, etkinliklerin yapıp yapılmadığını görüntülemekte sorun yaşadıklarını ve iki öğrenci, metinlerin fazla uzun olduğunu belirtmiştir. 11 öğrencinin sitede beğenmedikleri yönlerle ilişkin cümleler ise şu şekildedir:

“Etkinlikler bölümündeki bulmaca kafa karıştırıcı.” (Öğrenci 9)

“Kelime bulmacada, yazılar zor yazılıyor.” (Öğrenci 22)

“Etkinliklerin telefonda yapılmamasını beğenmedim.” (Öğrenci 20)

“Etkinlikleri beğenmedim.” (Öğrenci 24)

“Kendimizi sınavalım bölümündeki sorular fazla olsa daha iyi olabilirdi.” (Öğrenci 18)

“Örnek Durum Çözümleme’ etkinliğini ve yazıların uzun olmasını beğenmedim.” (Öğrenci 19)

“Okumadan çok daha fazla anlatımlı video olabilirdi.” (Öğrenci 23)

“Videolar YouTube’den alındığı için tam ekran yapılmamasını beğenmedim.” (Öğrenci 25)

“Videoları beğenmedim.” (Öğrenci 2)

“Sitenin bazen hata vermesi sıkıntısı dışında başka bir şeyden hoşnutsuzluk yaşamadım.” (Öğrenci 2)

“Geçmiş konuları tekrarlamak istediğimde bir önceki haftaya ait işlediğimiz konunun tekrar açılmamasını beğenmedim.” (Öğrenci 10)

Çevrimiçi Ortamın Çevrimiçi Güvenlik ve Risk Düzeyine Yönelik Ne Gibi Katkılar Sağladığına Yönelik Bulgular

Çevrimiçi ortamın çevrimiçi güvenlik ve risk ile ilgili bilgiye yönelik ne gibi katkılar sağladığına yönelik olarak 13 öğrenci, çevrimiçi ortam aracılığıyla bildikleri konuları öğrendiklerini; 13 öğrenci, internette daha dikkatli ve tedbirli davranılmasının önemini öğrendiklerini belirtmiştir. Dört öğrencinin çevrimiçi ortamın çevrimiçi güvenlik ve risk ile ilgili bilgiye yönelik ne gibi katkılar sağladığına ilişkin cümleleri ise şu şekildedir:

“Bana sosyal medyadaki insanlara güvenmemem gerektiğini, şifreleri artık nasıl koyabileceğimi gösterdi.” (Öğrenci 20)

“Şifre güvenliğini ve kişisel verilerin korunmasını siber zorbalıkla karşılaştığımda ne yapmam gerektiğini ve bunlara benzer birçok şey öğrendim.” (Öğrenci 4)

“Kendimi sanal ortamda nasıl korurum, nasıl davranmalıyım bilgilerimi nasıl korumalıyım, bunları öğretti.” (Öğrenci 10)

“Şifrelerimi düzgün belirlemeye başladım.” (Öğrenci 15)

Çevrimiçi Ortamın Kullanımında Ne Tür Zorluklarla Karşılaşıldığına Yönelik Bulgular

Çevrimiçi ortamın kullanımında ne tür zorluklarla karşılaşıldığına yönelik 14 öğrenci, çevrimiçi ortamı kullanırken herhangi bir zorlukla karşılaşmadıklarını; üç öğrenci etkinlikleri telefonda yapma konusunda sorun yaşadıklarını; iki öğrenci video kısmında reklamlarla karşılaşabildiklerini, iki öğrenci tamamladıkları bölümlerin kaydedilmesinde sorun yaşadıklarını ve iki öğrenci oyunlarda zaman zaman hatalar oluştuğunu belirtmişlerdir. Yedi öğrencinin çevrimiçi ortamı kullandıkları süreçte karşılaştıkları zorluklara yönelik görüşleri ise şu şekildedir:

“Arada videoların donması beni zorladı.” (Öğrenci 9)

“Bazen videoları açmakta zorlanıyorum.” (Öğrenci 14)

“İlk önce siteyi açamadım biraz zorlandım ama sonra her şey yeniden başlamış gibi çok eğlendim.” (Öğrenci 12)

“Kelime arama etkinliğinde harfleri yazarken zorlandım.” (Öğrenci 19)

“Etkinliklerdeki bulmaca kısmında zorlandım.” (Öğrenci 15)

“Site içi aramayı bulamadım. Varsa da görünür olmalı.” (Öğrenci 22)

“Bazen soruları işaretlememe rağmen boş olarak gözükiyordu.” (Öğrenci 18)

Öğrencilere Yönelik Bir Çevrimiçi Güvenlik ve Risk ile İlgili Eğitimde Hangi Konulara Yer Verilmesi Gerektiğine Yönelik Bulgular

Öğrencilere yönelik bir çevrimiçi güvenlik ve risk ile ilgili eğitimde hangi konulara yer verilmesi gerektiğine yönelik olarak 10 öğrenci, çevrimiçi ortamdaki konuların yeterli olduğunu ve yedi öğrenci konu önerisi hakkında bir fikrinin olmadığını belirtmiştir. 13 öğrencinin öğrencilere yönelik bir çevrimiçi güvenlik ve risk ile ilgili eğitimde başka hangi konulara yer verilmesi gerektiğine ilişkin ifadeleri aşağıdaki şekildedir:

“Siber zorbalıkla karşılaştığımızda yapabileceklerimizle ilgili belli aralıklarda videolar paylaşılmalı.” (Öğrenci 4)

“Bu konularda daha fazla ne yapabiliriz, kendimizi sanal ortamda nasıl sınırla-

mayı öğrenmeliyiz, vb. konular yer almalı.” (Öğrenci 10)

“Google’deki ayarlar bölümü ile ilgili bir konu olabilir.” (Öğrenci 19)

“Sosyal medyayı daha güvenli nasıl kullanacağımız anlatılmalı.” (Öğrenci 2)

“Virüslerden korunma yolları daha fazla anlatılmalı.” (Öğrenci 1)

“Hackerlar karşısında ne yapmalıyım konusu olmalı.” (Öğrenci 25)

“Bence uygulamalar hakkında da bilgi verilmeli.” (Öğrenci 18)

“Her üniteye ayrı bölümlere yer verilmelidir.” (Öğrenci 28)

“İlgi çekici içeriklere ve daha da eğlenceli etkinliklere yer verilmeli.” (Öğrenci 23)

“Bulmaca eklenmelidir.” (Öğrenci 13)

“Photoshop uygulamaları eklenmelidir.” (Öğrenci 7)

“Kelime türetmece eklenmelidir.” (Öğrenci 14)

“Ders konuları hangi sırayla gidiyorsa o şekilde konulara yer verilmelidir.” (Öğrenci 20)

“Yeni Yorum Ekle” Bölümünde Diğer Kullanıcılarla Gerçekleştirilen İletişimin Ne Gibi Katkılar Sağladığına Yönelik Bulgular

“Yeni Yorum Ekle” bölümünde diğer kullanıcılarla gerçekleştirilen iletişimin ne gibi katkılar sağladığına yönelik olarak 21 öğrenci “Yeni Yorum Ekle” bölümünün, arkadaşlarıyla fikir alışverişi yapmalarını sağladığını, farklı bilgiler öğrenmelerine fırsat sağladığını, sekiz öğrenci, bu bölümü kullanmadıklarını ve gerekli bulmadıklarını, bir öğrenci ise bu bölümün bilgilerini pekiştirmesine yardımcı olduğunu belirtmiştir.

Çevrimiçi Ortama Yönelik Öneriler

22 öğrenci çevrimiçi ortama yönelik bir önerisinin olmadığını belirtmiştir. Sekiz öğrencinin çevrimiçi ortama yönelik önerileri ise şu şekildedir:

“Videolar biraz daha yavaş olabilir, hızlı geçen yazıları okumak için durdurmak zorunda kalıyorsunuz.” (Öğrenci 8)

“Daha farklı etkinlik bulmaca boşluk doldurma, Doğru Yanlış soruları eklenebilir.” (Öğrenci 9)

“Telefondaki hatalar düzeltilmeli. Yani telefondan da rahat bir şekilde yapılmalı.” (Öğrenci 16)

“İçinde olduğumuz ve olacağımız güvenlik tehlikeleri sık sık tekrarlanmalı bence.” (Öğrenci 10)

“ ‘Devamı’ yazısının daha büyük olması ve daha fazla oyun, etkinlik olması.” (Öğrenci 29)

“Hackerlardan nasıl korunmamız gerektiğini öğreten bir konu.”(Öğrenci 25)

“Etkinlikler bölümüne doğru/yanlış eklenebilir.” (Öğrenci 22)

TARTIŞMA, SONUÇ VE ÖNERİLER

Küresel salgının hayatımızı pek çok alanda etkilediği şu günlerde, eğitim alanında ciddi dönüşümler yaşanmış, uzaktan eğitimin fırsatlar açısından değerlendirilmesi önem kazanmıştır. Uzaktan eğitim faaliyetleri ile, günlük hayatta internette geçirilen zaman daha da artmış, internetin sağladığı fırsatların yanı sıra getirebileceği birtakım güvenlik riskleri hakkında da bilgi sahibi olunması gerekliliği ortaya çıkmıştır.

Bu çalışma kapsamında, çevrimiçi güvenlik ve risk ile ilgili eğitime yönelik geliştirilen çevrimiçi ortamda yürütülen eğitimlerin öğrencilerin çevrimiçi güvenlik ve risk ile ilgili bilgi düzeyleri açısından etkililiği sınanmıştır. Bu doğrultuda öğrencilerden ortamın iyileştirilmesine yönelik veriler de toplanmıştır.

Araştırmanın ilk araştırma sorusu, *“Öğrencilerin çevrimiçi güvenlik ve risk ile ilgili bilgi düzeyleri; interneti kullanım amaçlarına yönelik günlük ayrılan süre ve çevrimiçi güvenlik, bilgi güvenliği veya internet güvenliği hakkında daha önce bir eğitim alma durumuna göre nasıl değişmektedir?”* şeklindedir. Öğrencilerin çevrimiçi güvenlik ve risk ile ilgili bilgi düzeylerinin interneti haber okumak- medyayı takip etmek amaçlı kullanımda günlük ayırdıkları süreye bağlı olarak nasıl değiştiğinin belirlenmesi amacıyla tek faktörlü varyans analizine başvurulmuştur. Elde edilen sonuçlara göre, araştırmanın çalışma grubunu oluşturan öğrencilerin çevrimiçi güvenlik ve risk ile ilgili bilgi düzeylerinin; interneti kullanımda günlük ayırdıkları süreye bağlı olarak değişmediğini söylemek mümkündür. Öğretmenlerin sanal zorbalık hakkındaki düşüncelerini belirlemek amacıyla gerçekleştirilen bir çalışmada; internet kullanım süresi arttıkça katılımcıların sanal zorbalığın yalnız-

ca yetişkinler tarafından yapılacağına ilişkin düşüncelerinin azaldığı belirlenmiştir (Yenilmez & Seferoğlu, 2013). Çocukların internet kullanımı arttıkça, istenmeyen risklere maruz kalma olasılığının da arttığı belirtilmektedir (Livingstone vd., 2011).

Çalışma kapsamında katılımcıların çevrimiçi güvenlik, bilgi güvenliği, siber güvenlik veya internet güvenliği hakkında daha önce herhangi bir eğitim alma durumu ile çevrimiçi güvenlik ve risk ile ilgili bilgi düzeyleri arasında anlamlı bir ilişki bulunmamaktadır. Bu sonucun, öğrencilerin daha önce katıldıklarını belirttikleri eğitimlerin kapsamının, geliştirilen ortamda yer alan konulara kıyasla daha kısıtlı olmasından kaynaklandığı düşünülebilir. Avrupa Çevrimiçi Çocuklar (2020) projesi kapsamında gerçekleştirilen çalışmada; çevrimiçi ortamda kendini güvende hissetmenin, birçok çevrimiçi etkinliğe katılım için önemli bir faktör olduğu belirtilmiştir (Smahel vd., 2020). Bu çalışmada öğrencilerin daha önce çevrimiçi güvenlik ve risk ile ilgili bir eğitime katılma durumu göz önüne alınarak, öğrencilerin çevrimiçi güvenlik ve risk bilgi düzeyleri açısından eşit seviyede oldukları belirlenmiş ve eğitimler gerçekleştirilmiştir.

Araştırmanın ikinci araştırma sorusu “Çevrimiçi güvenlik ve risk ile ilgili eğitime yönelik tasarlanan ortamda yürütülen eğitimlerin öğrencilerin çevrimiçi güvenlik ve risk ile ilgili bilgi durumlarındaki değişimine etkisi nedir?” şeklindedir. Yürütülen deneysel uygulamanın öğrencilerin çevrimiçi güvenlik ve risk ile ilgili bilgi düzeyleri üzerindeki etkililiğinin test edilmesi amacıyla ön-test ve son-test puanları bağımlı gruplar t-testi ile karşılaştırılmış, eğitimler sonrasında öğrencilerin çevrimiçi güvenlik ve risk ile ilgili bilgi düzeylerinde anlamlı bir artış olduğu belirlenmiştir. Bu durum, araştırma kapsamında çevrimiçi ortamda yürütülen çevrimiçi güvenlik ve risk ile ilgili eğitimlerin, öğrencilerin çevrimiçi güvenlik ve risk ile ilgili bilgi düzeylerini geliştirme konusunda önemli bir etkisinin olduğu şeklinde düşünülebilir. Araştırmadan elde edilen bu sonucun alanyazında da bazı çalışmalardaki sonuçlarla örtüştüğünü söylemek mümkündür. Örneğin; 9-13 yaş arası çocuklara çevrimiçi mahremiyet-gizlilik okuryazarlığı eğitiminin verildiği bir çalışmada; eğitimin çocukların çevrimiçi gizlilik okuryazarlığını etkileyebileceği incelenmiştir. Araştırma sonuçları, eğitimin çocukların çevrimiçi gizlilik anlayışını geliştirdiğini göstermiştir (Desimpelaere vd., 2020). Yine, dijital ayak izi ders tasarımının öğrencilerin dijital vatandaşlık konusundaki akademik başarılarına etkisinin incelendiği bir başka çalışmada dijital ayak izi dersinin tasarımının dijital vatandaşlık konusundaki akademik başarı açısından olumlu bir etkisinin olduğu belirtilmiştir belirlenmiştir (Kuh Karyeli & Dağhan, 2019).

Araştırmanın üçüncü araştırma sorusu “Çevrimiçi ortamda yürütülen çevrimiçi güvenlik ve risk ile ilgili eğitimlerin öğrenilenlerin kalıcılığına etkisi nedir?” şeklindedir. Öğrenilenlerin kalıcılığı açısından değerlendirilebilmesi amacıyla çalışma grubunun son-test ve kalıcılık testi puanları bağımlı gruplar t-testi ile karşılaştırıl-

mıştır. Araştırma kapsamında öğrencilerin çevrimiçi güvenlik ve risk ile ilgili bilgi düzeylerinde son test ve kalıcılık testi puanları açısından anlamlı farklılık olduğu sonucuna ulaşılmıştır. Bu sonucun, öğrencilerin çevrimiçi ortamdaki derslere yerli katılım sağlayamamış olmalarından kaynaklandığı düşünülebilir.

Araştırmanın dördüncü ve son araştırma sorusu; “Öğrencilerin, geliştirilen çevrimiçi ortama yönelik görüşleri nelerdir?” şeklindedir. Bu araştırma sorusu aracılığıyla ortamın kullanılabilirlik sorunları belirlenmiş, ortamda yapılabilecek düzenlemeler tespit edilmiştir. Bu doğrultuda geliştirilen ortamda yer alan “Kendimizi Sınayalım” bölümlerinde yer alan soru sayısının az olması, “Etkinlikler” bölümünün mobil teknolojiler aracılığıyla uygulanmasında sorun yaşanması, bazı sayfalarda metinlerin çok uzun olması, videolar sayfasında reklamlarla karşılaşılması gibi tespitler dikkat çekmektedir. Bu tespitler göz önünde bulundurularak geliştirilen ortamda “kendimizi sınavalım” bölümündeki soru sayısının artırılması, etkinliklere yönelik mobil teknolojilerde yaşanan sorunların giderilmesi, metinlerin kısaltılması ve videoların doğrudan geliştirilen sistem üzerinden reklamlar olmaksızın sunulması gibi düzenlemeler yapılmasının uygun olacağı düşünülmüştür.

Çalışma kapsamında elde edilen sonuçları özetlemek gerekirse, hedeflenen kazanımlara ve öğrenci seviyesine uygun olarak geliştirilen çevrimiçi ortamların ve bu ortamlar aracılığıyla öğretmenin planlamasına uygun olarak yürütülen eğitimlerin, öğrenci başarısı açısından katkı sağlayacağı söylenebilir. Çevrimiçi ortamlarda geçirilen sürenin oldukça fazla olduğu şu günlerde, öğrencilerin çevrimiçi ortamlarda karşılaşabilecekleri güvenlik sorunları ve riskler hakkında bilgi sahibi olmaları önemli bir konudur. İleride yapılacak çalışmalar için, çevrimiçi ortamların kullanımına yönelik farklı öğrenme tekniklerinin de işe koşulduğu deneysel çalışmaların yapılması önerilebilir.

KAYNAKLAR

- Ahn, J., Bivona, L. K., & Discala, J. (2011). Social media access in K12 schools: Intractable policy controversies in an evolving world. *Proceedings of the American Society for Information Science and Technology*, 48(1), 1-10.
- Boyd, D., & Hargittai, E. (2013). Connected and concerned: Variation in parents' online safety concerns. *Policy & Internet*, 5(3), 245-269.
- Bozkurt, A. (2020). Koronavirüs (Covid-19) pandemi süreci ve pandemi sonrası dünyada eğitime yönelik değerlendirmeler: Yeni normal ve yeni eğitim paradigması. *Açıköğretim Uygulamaları ve Araştırmaları Dergisi*, 6(3), 112-142.
- Çelen, F. K., Çelik, A., & Seferoğlu, S. S. (2011). Çocukların İnternet kullanımları ve onları bekleyen çevrim-içi riskler. XIII. *Akademik Bilişim Konferansı (AB11) Bildirileri*, 645-652. İnönü Üniversitesi, Malatya. [Çevrimiçi: http://ab.org.tr/ab11/kitap/celen_celik_Riskler_AB11.pdf, Erişim Tarihi: 15.02.2021]
- Cresswell, J. W. (2017). *Araştırma deseni nitel, nicel ve karma yöntem yaklaşımları* (4. Baskıdan çeviri, S. B. Demir). Ankara: Eğiten Kitap.
- Desimpelaere, L., Hudders, L., & Van de Sompel, D. (2020). Knowledge as a strategy for privacy protection: How a privacy literacy training affects children's online disclosure behavior. *Computers in Human Behavior*, 110, 106382.
- Eren, S., & Erdem, M. (2013). The examination of online kids' sites with the purpose of raising kids' self-protection

- awareness. *Procedia-Social and Behavioral Sciences*, 83, 611-614.
- Hartikainen, H., Livari, N., & Kinnula, M. (2019). Children's design recommendations for online safety education. *International Journal of Child-Computer Interaction*, 22, 100-146.
- Hasebrink, U., Görzig, A., Haddon, L., Kalmus, V., & Livingstone, S. (2011). *Patterns of risk and safety online. In-depth analyses from the EU Kids Online survey of 9-16-year-olds and their parents in 25 countries*. LSE, London: EU Kids Online.
- Kearney, W. D., & Kruger, H. A. (2016). Can perceptual differences account for enigmatic information security behaviour in an organisation? *Computers & Security*, 61, 46-58.
- Kuh Karyeli, G., & Dağhan, G. (2019). Sayısal ayak izi ders tasarımının öğrencilerin sayısal vatandaşlık konusundaki akademik başarılarına etkisi. *Erzincan Üniversitesi Eğitim Fakültesi Dergisi*, 22(1), 256-275.
- Landis, J. R., & Koch, G. G. (1977). The measurement of observer agreement for categorical data. *Biometrics*, 33, 159-174.
- Livingstone, S., Haddon, L., Görzig, A., & Ólafsson, K. (2011). *Technical report and user guide: The 2010 EU Kids Online Survey*. LSE, London: EU Kids Online.
- Mıhçı, P., & Kılıç-Çakmak, E. (2017). Öğrenci siber sağlık ölçekleri geliştirme çalışması. *Gazi Üniversitesi Gazi Eğitim Fakültesi Dergisi*, 37(2), 457-491.
- Moore, J. L., Dickson-Deane, C., & Galyen, K. (2011). e-Learning, online learning, and distance learning environments: Are they the same? *The Internet and Higher Education*, 14(2), 129-135.
- Ólafsson, K., Livingstone, S., & Haddon, L. (2013). *Children's use of online technologies in Europe: A review of the European evidence base*. EU Kids Online. London, UK.
- Padlipsky, S. (2018). *Using offline activities to enhance online cybersecurity education*. Yayımlanmamış yüksek lisans tezi. California Polytechnic State University, California.
- Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security*, 56, 70-82.
- Sağiroğlu, Ş., & Alkan, M. (2018). *Siber güvenlik ve savunma farkındalık ve caydırıcılık*. BGD Siber Güvenlik ve Savunma Kitap Serisi. s. 26. Grafiker Yayınları. Ankara.
- Shillair, R., Cotten, S. R., Tsai, H. Y. S., Alhabash, S., LaRose, R., & Rifon, N. J. (2015). Online safety begins with you and me: Convincing Internet users to protect themselves. *Computers in Human Behavior*, 48, 199-207.
- Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K., Livingstone, S., & Hasebrink, U. (2020). EU Kids Online 2020: Survey results from 19 countries. *EU Kids Online. London School of Economics and Political Science*, London, UK.
- Tüzün, H., Bilgiç, H. G., Kalaycı, E., Çınar, M., Akıncı, A., Denizler, Y., & Yüksel, Y. (2011). Yerleşik bir dersin web tabanlı uzaktan eğitim için yeniden tasarımı. Demirci, B.B., Telli-Yamamoto, G. & Demiray, U., *Türkiye'de e-öğrenme: Gelişmeler ve uygulamalar II* (ss.175-199). Anadolu Üniversitesi Yayınları: Eskişehir.
- Veneziano L., & Hooper J. (1997). A method for quantifying content validity of health-related questionnaires. *American Journal of Health Behavior*, 21(1), 67-70.
- Yenilmez, Y., & Seferoğlu, S. S. (2013). Sanal zorbalık ve öğretmenlerin farkındalık durumlarına bir bakış. *Education & Science/Eğitim ve Bilim*, 38(169).
- Zhao, Y. (2020). COVID-19 as a catalyst for educational change. *Prospects*, 49(1), 29-33.

THE EFFECTS OF AN ONLINE ENVIRONMENT DEVELOPED FOR ONLINE SAFETY AND RISK EDUCATION ON THE KNOWLEDGE LEVELS OF SECONDARY SCHOOL STUDENTS

EXTENDED ABSTRACT:

Distance education and online education can provide an opportunity to provide flexibility in terms of space and time. Online environments are prepared especially by considering the target and achievements; they can play a key role in the education of children. This study aims to examine the effects of trainings conducted in an online environment that designed for online security and risk education on secondary school students' knowledge levels about online security and risk. In the research, at the stage of collecting quantitative data, one group pre-test post-test design, which is one of the weak experimental designs, was used. The findings of the research were supported by using qualitative data collected with an open-ended questionnaire. The study group of the research consists of students studying at a central secondary school in Ankara. In the data collection process; personal information form, online media expert opinion form, online safety and risk knowledge level determination tool and open-ended questionnaire were used. In the personal information form developed by the researchers; there are questions about the daily allocated time for the purposes of using the internet and the status of having previously received training on online security, information security or internet security. A measurement tool titled "Online Safety and Risk-Related Knowledge Level Determination Tool" developed by the researchers was used to measure the level of knowledge about online safety and risk for secondary school students. This measurement tool consists of 16 open-ended questions developed by determining the themes that should be included in the scope of the literature review. Within the scope of the study, an expert opinion form titled "Online Media Expert Opinion Form" was developed to evaluate the online environment developed by the researchers. Within the scope of the research, a semi-structured interview form was developed by the researchers in order to determine the effectiveness of the online learning environment. In order to determine the statistical methods to be used, it was tested whether the study groups showed a normal distribution or not. A computer-based statistics program was used for the analysis of quantitative data. Descriptive analysis and content analysis methods were used for the analysis of qualitative data.

The first research question of this study is "The level of knowledge of students about online safety and risk; how does the daily allotted time for the purposes of using the internet and online security change according to a previous training on information security or internet security? ". One-way ANOVA and independent groups t-test method were used to find an answer to this question. One-way ANO-

VA was used to determine the relationship between the daily time spent by the participants using the internet to read news and to follow the media, and their level of knowledge about online safety and risk. One-way ANOVA results showed that students' knowledge levels about online safety and risk does not change depending on the amount of time spent per day using the internet to read news and to follow the media. One-way ANOVA was used to determine the relationship between the daily time spent by the participants for recreational use of the internet and their level of knowledge about online safety and risk. One-way ANOVA results showed that students' knowledge levels about online safety and risk does not change depending on the amount of time spent on entertainment purposes. One-way ANOVA was used to determine the relationship between the daily time spent by the participants for using the internet for educational purposes (doing research, doing homework, continuing distance education) and their level of knowledge about online safety and risk. One-way ANOVA results showed that students' knowledge levels about online safety and risk does not change depending on the amount of time spent daily using the internet for educational purposes (doing research, doing homework, continuing distance education). Independent groups t-test analysis was applied to determine the relationship between the participants' status of having received any previous training on online security or information security and their knowledge level about online security and risk. According to the results of independent groups t-test analysis, students' level of knowledge about online safety and risk does not change according to previous training on online security, information security, cyber security or internet security.

The second research question of the study is "What are the students' views on the online environment developed?" in the form. All of the students (30) stated that the name of the online environment developed was appropriate and that the content available online was up-to-date.

The third research question of the research is "What is the effect of the environment designed for online security and risk-related education on the change in students' knowledge about online security and risk?" In order to test the effectiveness of the experimental practice conducted on students' online safety and risk-related knowledge levels, pre-test and post-test scores were compared with dependent groups t-test, and it was determined that there was a significant increase in students' knowledge levels about online safety and risk after the trainings.

The fourth and final research question of the research is "What is the effect of online safety and risk trainings on the retention of learning?" In order to evaluate the experimental practice in terms of the retention of the learning, the posttest and permanence test scores of the study group were compared with the dependent groups' t-test. It was concluded that there was a significant difference in the

posttest and retention test scores of students' knowledge levels about online safety and risk. This finding was interpreted as the training conducted in the online environment was not sufficient to ensure the permanence of the learned information.

To summarize the results obtained within the scope of the study, the online environments developed in accordance with the targeted achievements and the student level and the trainings carried out in accordance with the teacher's planning through these environments; it can be said that it will contribute to student success. Nowadays, when the time spent in online environments is quite high, it is important for students to be informed about the security problems and risks they may encounter in online environments. For future studies, it can be suggested to conduct experimental studies in which different learning techniques are used for the use of online environments for control and experimental groups.

Keywords: *Online security, internet security, information security, cyber security, online learning, distance education.*



