



T.C.
TOKAT GAZİOSMANPAŞA ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
BİLGİSAYAR VE ÖĞRETİM TEKNOLOJİLERİ EĞİTİMİ ANABİLİM DALI
YÜKSEK LİSANS PROGRAMI

ORTAOKUL ÖĞRENCİLERİNİN DİJİTAL KİMLİK
MAHREMİYETİ BECERİLERİ İLE TEKNOLOJİ
OKURYAZARLIK DÜZEYLERİNİN ÇEVİRİMİÇİ OYUNLARDAKİ
SİBER GÜVENLİK FARKINDALIKLARI ÜZERİNDEKİ ETKİSİ

YÜKSEK LİSANS TEZİ

Süleyman VURAL

Danışman: Doç. Dr. Kerem KILIÇER

TOKAT- 2022

ETİK SÖZLEŞME

Tokat Gaziosmanpaşa Üniversitesi Lisansüstü Eğitim Enstitüsü tez yazım kılavuzuna göre, Doç. Dr. Kerem KILIÇER danışmanlığında hazırlamış olduğum “Ortaokul Öğrencilerinin Dijital Kimlik Mahremiyeti Becerileri İle Teknoloji Okuryazarlık Düzeylerinin Çevrimiçi Oyunlardaki Siber Güvenlik Farkındalıkları Üzerindeki Etkisi” adlı Yüksek Lisans tezinin bilimsel etik değerlere ve kurallara uygun, özgün bir çalışma olduğunu, aksinin tespit edilmesi halinde her türlü yasal yaptırımını kabul edeceğimi beyan ederim.

.../07/2022

Süleyman VURAL

JÜRİ KABUL VE ONAY

Süleyman VURAL tarafından hazırlanan “Ortaokul Öğrencilerinin Dijital Kimlik Mahremiyeti Becerileri İle Teknoloji Okuryazarlık Düzeylerinin Çevrimiçi Oyunlardaki Siber Güvenlik Farkındalıkları Üzerindeki Etkisi” adlı tez çalışmasının savunma sınavı (18/07/2022) tarihinde yapılmış olup aşağıda verilen Jüri tarafından Oy Birliği ile Tokat Gaziosmanpaşa Üniversitesi Lisansüstü Eğitim Enstitüsü Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı’nda Yüksek Lisans Tezi olarak kabul edilmiştir.

Jüri Üyeleri (Unvanı, Adı Soyadı)

İmzası

Üye (Başkan): Dr. Öğr. Üyesi Zeynel Abidin MISIRLI

.....

Üye : Doç. Dr. Kerem KILIÇER

.....

Üye : Dr. Öğr. Üyesi Emre ÇAM

.....

ONAY

.../07/2022

Prof. Dr. Mehmet GÜNEŞ
Lisansüstü Eğitim Enstitüsü Müdürü

ÖNSÖZ

Yüksek lisans eğitimim süresince göstermiş olduğu sabır ve iyi niyetiyle, tezin yazım sürecinde teşriki mesai yaparak yapmış olduğu değerli katkılarla hep yanımda olan danışman hocam Doç. Dr. Kerem Kılıçer'e,

Tez yazım süreci boyunca kendilerini sık sık rahatsız ettiğim, görüş ve fikirleriyle tez çalışmama katkıda bulunan değerli meslektaşlarım Abdulkadir Kara ve Sema İncir'e,

Ölçek uygulama sürecinde Tokat merkez ve ilçelerinde yaptığım çalışmalara katkı sağlayan öğretmen ve okul yöneticilerine göstermiş oldukları nezaketten dolayı teşekkür ediyorum.

Gelişmenin, ilerlemenin bilimle olacağına inanan ve bu inanç uğrunda gece gündüz çalışan, bilimi teknolojiye dönüştürüp ülkemizin gücüne güç, halkımızın refahına katkı sağlayan, kalkınmanın katma değeri yüksek buluşlarla olacağını bilen, yapılamayanı yapmak için ter akıtan, bizleri de bu ideallerle yetiştiren bilim insanlarına, şahsım, milletim, devletim ve gelecek nesiller adına şükranlarımı sunuyorum. Saygıyla...

ÖZET

ORTAOKUL ÖĞRENCİLERİNİN DİJİTAL KİMLİK MAHREMİYETİ BECERİLERİ İLE TEKNOLOJİ OKURYAZARLIK DÜZEYLERİNİN ÇEVİRİMİÇİ OYUNLARDAKİ SİBER GÜVENLİK FARKINDALIKLARI ÜZERİNDEKİ ETKİSİ

Vural, Süleyman

Yüksek Lisans, Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı

Tez Danışmanı: Doç. Dr. Kerem Kılıçer

Temmuz 2022, xiv + 93 sayfa

Bu çalışmanın amacı, ortaokul öğrencilerinin çevrimiçi mahremiyet farkındalık düzeyleri ile dijital okuryazarlık düzeylerinin çevrimiçi oyunlarda siber güvenlik farkındalığı üzerindeki etkisini incelemektir. Araştırmada ortaokul öğrencilerinin siber güvenlik farkındalık durumları, çevrimiçi mahremiyet farkındalığı durumları, dijital okuryazarlık durumları ve çevrimiçi oyun alışkanlıkları gibi özellikleri ve bu değişkenler arasındaki ilişkiler incelenmiştir. Araştırmanın çalışma grubu 2021-2022 eğitim öğretim yılında Millî Eğitim Bakanlığına bağlı Tokat il merkez ve ilçelerinde öğrenim görmekte olan toplam 1480 ortaokul 5, 6, 7 ve 8. sınıf öğrencilerinden oluşmaktadır. Öğrencilere yüz yüze ortamlarda gönüllülük esasına göre ulaşılmıştır. Araştırmada nicel araştırma yöntemlerinden nedensel-karşılaştırmalı araştırma modeli kullanılmıştır. Veri toplama aracı olarak araştırmaya katılan ortaokul öğrencilerinin çevrimiçi oyun alışkanlıklarını belirlemek için kişisel bilgiler formu, Pala (2019) tarafından geliştirilen “Dijital Okuryazarlık” ölçeği, Korkmaz, Vergili ve Töngel (2019) tarafından geliştirilen “Çevrimiçi Mahremiyet Farkındalık” ölçeği ve araştırma amacı doğrultusunda geliştirilen “Siber Güvenlik Farkındalığı” ölçeği kullanılmıştır. Elde edilen verilerin analizi sürecinde nicel verileri analiz etmek için SPSS 22.0 istatistik yazılımı kullanılmıştır. Araştırmada kullanılan ölçeklerden elde edilen veriler yüzde, frekans, ANOVA, korelasyon ve doğrusal ve çoklu regresyon analizi kullanılarak çözümlenmiştir. Yapılan analizlerden elde edilen bulgulardan ulaşılan sonuçlara göre siber güvenlik farkındalığı ile dijital okuryazarlık durumu arasında anlamlı ve pozitif yönde bir ilişki bulunmuştur. Siber güvenlik farkındalığı ile çevrimiçi mahremiyet farkındalığı durumu arasında da anlamlı ve pozitif yönde bir ilişki olduğu sonucuna varılmıştır. Siber güvenlik

farkındalığına her iki değişkenin (dijital okuryazarlık ve çevrimiçi mahremiyet farkındalığı) pozitif yönlü ve anlamlı katkısının olduğu bulunmuştur. Araştırma sonuçlarına göre ortaokul öğrencilerinin çevrimiçi oyunlarda siber güvenlik farkındalığının iyi durumda olduğu anlaşılmıştır. Ayrıca araştırmaya katılan öğrencilerin çevrimiçi oyun oynama platformu olarak en çok cep telefonu kullandığını ve günlük çevrimiçi oyun oynama süreleri olarak 1-2 saat zaman aralığında oyun oynadıkları sonucuna varılmıştır.

Anahtar Kelimeler: Çevrimiçi Oyunlarda Siber Güvenlik Farkındalığı, Dijital Oyun, Dijital Kimlik Mahremiyeti, Teknoloji Okuryazarlığı



ABSTRACT

THE EFFECT OF SECONDARY SCHOOL STUDENTS' DIGITAL IDENTITY PRIVACY SKILLS AND TECHNOLOGY LITERACY LEVELS ON CYBERSECURITY AWARENESS IN ONLINE GAMES

Vural, Süleyman

Master's Thesis, Division of Computer Education and Instructional Technologies

Advisor: Assoc. Prof. Dr. Kerem Kılıçer

July 2022, xiv + 93 pages

This study aims to examine the effect of secondary school students' online privacy and digital literacy levels on cyber security awareness in online games. The study examined, the characteristics of secondary school students such as cyber security awareness status, online privacy awareness status, digital literacy status and online gaming habits and the relationships between these variables. The study group of the research consists of 1480 secondary school 5th, 6th, 7th and 8th grade students studying in the city centre and districts of Tokat under the Ministry of National Education in the 2021-2022 academic year. Students were reached voluntarily in face-to-face environments. The causal-comparative research model, one of the quantitative research methods, was used in the research. Personal information form, “Digital Literacy” scale developed by Pala (2019), “Online Privacy Awareness” scale developed by Korkmaz, Vergili and Töngel (2019) to determine online gaming habits and socio-demographic status of secondary school students participating in the research as data collection tool and the “Cyber Security Awareness” scale, which was prepared in line with the research purpose, was used. During the analysis of the obtained data, SPSS 22.0 statistical program was used to analyze the quantitative data. The data obtained from the scales used in the research were analyzed using percentage, frequency, ANOVA, correlation and linear-multiple regression according to the variable types. According to the results obtained from the analyzes, it was concluded that there is a significant and positive relationship between cyber security awareness and digital literacy status. It was concluded that there is a significant and positive relationship between cyber security awareness and online privacy awareness. It was concluded that both variables (digital literacy and online privacy awareness) have a positive and significant relationship to cyber security

awareness. According to the research results, it was understood that the cyber security awareness of secondary school students in online games is in good condition. In addition, it was concluded that the students participating in the research mostly use mobile phones as an online game playing platform and they play games in 1-2 hours as their daily online game playing time.

Keywords: Cybersecurity Awareness in Online Games, Digital Game, Digital Identity Privacy, Technology Literacy



İÇİNDEKİLER

	Sayfa
ETİK SÖZLEŞME.....	iii
JÜRİ KABUL VE ONAY	iv
ÖNSÖZ	v
ÖZET	vi
ABSTRACT.....	viii
İÇİNDEKİLER	x
TABLO LİSTESİ.....	xii
ŞEKİL LİSTESİ.....	xiii
KISALTMALAR.....	xiv
BÖLÜM I.....	1
GİRİŞ	1
Problem	1
Amaç	6
Önem	7
Sayıtlılar	8
Sınırlılıklar	8
Tanımlar	8
BÖLÜM II	10
KAVRAMSAL ÇERÇEVE	10
Bilgi ve Bilgi Güvenliği Kavramı	10
Bilgi Mahremiyeti ve Dijital Kimlik Mahremiyeti	12
Dijital Oyun Kavramı ve Dijital Oyun Pazarı	13
Dijital Oyunların Sınırlılıkları ve Üstünlükleri	15
Dijital Oyunların Sınırlılıkları	16
Dijital Oyunların Üstünlükleri	17
Bilgi Güvenliği Açısından Dijital Oyunlar	19
BÖLÜM III	21
YÖNTEM	21
Araştırmanın Modeli	21
Evren ve Örneklem.....	21
Veri Toplama Araçları	23

Çevrimiçi Oyunlarda Siber Güvenlik Farkındalığı Ölçeği	23
Dijital Okuryazarlık Ölçeği	31
Çevrimiçi Mahremiyet Farkındalığı Ölçeği.....	32
Veri Toplama Süreci	33
Verilerin Analizi.....	33
BÖLÜM IV	35
BULGULAR.....	35
Ortaokul Öğrencilerinin Çevrimiçi Oyun Alışkanlıkları.....	35
Ortaokul Öğrencilerinin Çevrimiçi Oyunlara Yönelik Siber Güvenlik Farkındalık Düzeyleri	41
Ortaokul Öğrencilerinin Dijital Okuryazarlık Düzeyleri	42
Ortaokul Öğrencilerinin Çevrimiçi Mahremiyet Farkındalık Düzeyleri.....	44
Ortaokul Öğrencilerinin Çevrimiçi Mahremiyet Farkındalık Düzeyleri ile Dijital Okuryazarlık Düzeylerinin Çevrimiçi Oyunlardaki Siber Güvenlik Farkındalıkları Üzerindeki Etkisi.....	45
BÖLÜM V	48
TARTIŞMA	48
BÖLÜM VI.....	55
SONUÇ VE ÖNERİLER.....	55
Sonuç	55
Öneriler.....	56
Uygulamaya Yönelik Öneriler.....	56
Araştırmacılara Yönelik Öneriler	57
KAYNAKÇA.....	59
EKLER.....	70
Ek 1. Çevrimiçi Oyunlarda Siber Güvenlik Farkındalığı Ölçeği	70
Ek 2. Çevrimiçi Mahremiyet Farkındalığı Ölçeği.....	72
Ek 3. Dijital Okuryazarlık Ölçeği.....	73
Ek 4. Araştırma İzni	74
Ek 5. Araştırma Evrenine Ait Öğrenci Sayıları.....	76
Ek 6. Ölçme Araçları Kullanım İzinleri	78
Ek 7. Özgeçmiş	80

TABLO LİSTESİ

Sayfa

Tablo 1. Çalışma Grubundaki Öğrencilere Ait Demografik Bilgiler	22
Tablo 2. Taslak Ölçeğin Uygulandığı Çalışma Grubuna Ait Demografik Bilgiler	25
Tablo 3. Doğrulamalı Faktör Analizi Ölçeğinin Demografik Bilgileri.....	26
Tablo 4. Ölçek Faktör Yük, Bileşik Güvenirlik (CR) ve Cronbach's Alpha Değerleri .	27
Tablo 5. Siber Güvenlik Farkındalığı Ölçeği İçin Çok Faktörlü DFA Uyum İndeksleri	30
Tablo 6. Basıklık ve Çarpıklık Değerleri.....	33
Tablo 7. Günlük Ortalama Çevrimiçi Oyun Oynama Süreleri	34
Tablo 8. Günlük Ortalama Çevrimiçi Oyun Oynama Sıklıkları	34
Tablo 9. Ortaokul Öğrencilerinin Çevrimiçi Oyunları En Çok Oynadıkları Platformlar	36
Tablo 10. Ortaokul Öğrencilerinin Çevrimiçi Oyunlara Yönelik Siber Güvenlik Farkındalık Durumları.....	40
Tablo 11. Ortaokul Öğrencilerinin Dijital Okuryazarlık Düzeylerine İlişkin Durumları	42
Tablo 12. Ortaokul Öğrencilerinin Çevrimiçi Mahremiyet Farkındalık Durumları	43
Tablo 13. Çevrimiçi Mahremiyet Farkındalığının Çevrimiçi Oyunlardaki Siber Güvenlik Farkındalığını Yordanmasına İlişkin Basit Doğrusal Regresyon Analiz Sonuçları	44
Tablo 14. Dijital Okuryazarlığın Çevrimiçi Oyunlardaki Siber Güvenlik Farkındalığını Yordanmasına İlişkin Basit Doğrusal Regresyon Analiz Sonuçları.....	45
Tablo 15. Çevrimiçi Mahremiyet Farkındalığı ve Dijital Okuryazarlık Düzeyinin Çevrimiçi Oyunlardaki Siber Güvenlik Farkındalığını Yordanmasına İlişkin Çoklu Regresyon Analiz Sonuçları	45

ŞEKİL LİSTESİ

	Sayfa
Şekil 1. Ölçek İçin İkinci Düzey DFA Sonuçları	30
Şekil 2. Ortaokul Öğrencilerinin Oynadıkları Çevrimiçi Oyun Türleri.....	35
Şekil 3. Ortaokul Öğrencilerinin Çevrimiçi Oyunları Oynadıkları Yer.....	36
Şekil 4. Ortaokul Öğrencilerinin En Çok Oynadığı Çevrimiçi Oyunlar.....	37
Şekil 5. Ortaokul Öğrencilerinin Çevrimiçi Oyunlar İçin Aylık Ortalama Harcadıkları Para Miktarı	38
Şekil 6. Ortaokul Öğrencilerinin Çevrimiçi Oyun Oynamak İçin Satın Aldığı Cihazlar.....	39
Şekil 7. Ortaokul Öğrencilerinin Takım Halinde Çevrimiçi Oyun Oynarken Ortalama Oyun Oynadıkları Kişi Sayısı.....	40

KISALTMALAR

SGF: Siber Güvenlik Farkındalığı

ÇMF: Çevrimiçi Mahremiyet Farkındalığı

MEB: Millî Eğitim Bakanlığı

TDK: Türk Dil Kurumu

RMSEA: Yaklaşık Hataların Ortalama Karekökü

CFI: Karşılaştırmalı Uyum İndeksi

GFI: İyiilik Uyum İndeksi

AGFI: Düzenlenmiş İyiilik Uyum İndeksi

SRMR: Standardize Edilmiş Ortalama Hataların Karekökü

KMO: Kaiser-Mayer-Olkin

BÖLÜM I

GİRİŞ

Bu bölümde araştırmanın problemi, alt problemleri, amacı, önemi, sayıltıları, sınırlılıkları, tanımlar ve kısaltmalara yer verilmiştir.

Problem

Çocuklar için öğrenme ve sosyalleşme aracı, yetişkinler için rahatlama kaynağı olan oyun yaşamın her döneminde önemli olan bir kavramdır (Aksoy, 2019). Teknolojinin insan yaşamında her şeyi etkilediği göz önüne alındığında oyun kavramının da teknolojinin etkisiyle dönüşüme uğradığı yadsınamaz bir gerçektir. Teknolojinin hızlı bir şekilde gelişmesiyle geleneksel oyunlar yaşamımızdaki yerinin büyük bir kısmını dijital oyunlara bırakmıştır. Hayatın her anını artık sanal hale getirip yaşamı etkisi altına alan internet ve bilgisayar teknolojilerinden oyunlar da ciddi manada etkilemiştir. İnternet kullanımının günümüzde çok daha fazla yaygınlaşması, özellikle mobil cihazlarla online oyunlara kolay erişilebilir olması, dijital oyunları çok daha farklı bir yere taşımıştır. Bununla birlikte şehirleşme kültürünün ve kentsel yapıların oluşturduğu sosyal çevrenin anne babalarca artık güvensiz kabul edilmesi, çocukların bireysel güvenliğinin ön plana çıktığı günümüzde sokaktaki oyun kültürünün dolaylı olarak bilgisayar ortamına taşınmasına daha çok katkı sağlamıştır. Günümüzde tüm toplumsal alanlarda oynanabilen her türlü oyun artık sanal bir ortama aktarılmış durumdadır. Parklarda ve sokaklarda oynanan her türlü oyun, günümüzde artık evlerde, iş yerlerinde veya internet kafe veya PlayStation salonlarında oynanmaktadır. Örneğin, günümüzde çocuklar caddelerde veya spor mekânlarında futbol oynamak yerine, etrafındaki insanlara bağımlı-bağımsız evde veya internet salonlarında dijital ortamı kullanarak futbol oynamaktadır (Kaya, 2013).

Dijital oyun çeşitliliğinin yanında dijital oyun oynamaya başlama yaşı da oldukça gerilemiştir. Bilgi Teknolojileri ve İletişim Kurumu'na göre bireylerin dijital oyunlarla tanışma yaşı 5-6 yaşlara kadar düşmüş durumdadır (www.btk.gov.tr). Bir başka çalışmaya göre ise dijital oyun oynamaya başlama yaşı 4,5 ve bir gün içinde oyun oynama süresinin yaklaşık 179 dakika (3 saat) olduğu ifade etmektedirler. Çocukların eğitim düzeyleri arasındaki oyun oynamaya başlama yaşlarının ilkökul öğrencilerinin lise öğrencilerine göre istatistiksel olarak daha erken yaşta oyun oynamaya başladıklarını fakat

ortaokul öğrencilerine göre daha geç yaşta başladıklarını göstermektedir. Buna göre ortaokul öğrencileri dijital oyunları ilkökul öğrencilerine göre daha yoğun olarak oynamaktadır. Ayrıca çocuklarda dijital oyun oynamaya başlama yaşlarının cinsiyet durumlarına göre benzer olduğu ve gün içerisinde oyunla vakit geçirme sürelerinin erkeklerde kızlara göre daha fazla olduğu ifade edilmektedir. Dijital oyun oynamak için kullanılan teknolojiler açısından bakıldığında ise, ebeveynlere göre çocukların %65,7'i bilgisayar ortamında, %72,1'i akıllı telefonlarla, %85,2'i tablette ve son olarak %24,5'i ise konsollar aracılığı ile dijital oyun oynamaktadır (Mustafaoğlu ve Yasacı, 2018).

Teknolojinin gelişimine paralel olarak giderek daha da büyüyen dijital oyun pazarına bakıldığında ise, 2020 yılı ortaları itibariyle dünya genelinde yaklaşık 3,1 milyar insanın dijital oyun oynadığı görülmektedir. Bu rakam toplam dünya nüfusunun %40'ına denk gelmektedir (Öztürk, 2021). Ayrıca 2020 yılı itibariyle dünya genelinde 2,5 milyar dijital oyuncuya ve milyarlarca dolar karlılığa ulaşarak hızla büyüyen dijital oyunlar mobil platformlarda da 2,5 milyar insana ulaşmıştır. 2018 yılında 138 milyar dolarlık bir pazar payına ulaşan dijital oyunlar, Dijital Oyunlar raporuna göre 2019 yılında 151 milyar dolar, 2020 yılında 165 milyar dolar ve 2021 itibariyle 180 milyar doları bulacağı 2025 yılına kadar 300 milyar dolar seviyelerine çıkacağı tahmin edilmektedir (Sepetçi, 2020).

Benzer şekilde Küresel Gelişmeler Raporuna göre 2020 yılı itibariyle indirilen uygulama sayısı 143 milyarı bulmuş ve mobil uygulama alanlarında elde edilen kazançta mobil oyunların pazar payının %71,7'sini oluşturduğu görülmektedir. İlk defa oyun yükleyen kişilerin sayısı önceki yıla nazaran yaklaşık %33 artış göstererek toplam 56,2 milyara ulaşmıştır. Dijital dünyada mobil oyun pazarının 2019 yılında 63 milyar doları, 2020 yılına geldiğimizde ise 79,5 milyar doları bulduğu görülmüştür. Özellikle Covid-19 salgın döneminin de etkisiyle bu durum mobil uygulama pazarında çok ciddi bir büyüme sağlamış ve devam eden süreçte büyümenin katlanarak artış göstereceği öngörülmektedir (Türkiye Bilişim Derneği Küresel Gelişmeler Raporu [TBD], 2020).

Bu bağlamda bakıldığında günümüzde oyun sektörü sinema sektörünü geçmiş durumdadır. Ayrıca sosyal medya kullanan bireylerin büyük çoğunluğu bu platformları (örneğin Facebook gibi) dijital oyun oynamak için kullandığı görülmektedir. Dijital oyun sektörü günümüzdeki salgın gibi ekonomik krizlerden en az etkilenen ve gelir düzeyi çok yüksek bir sektördür. Ülkemizde 20 binin üzerinde internet kafenin bulunduğu ve bu kafelerin en yoğun kullanım alanlarının dijital oyunlar olduğu belirtilmektedir. Buna

bağlı olarak ülkemizde 20 milyondan fazla insan dijital oyun oynamaktadır (www.btk.gov.tr). Türkiye İstatistik Kurumu'nun 2020 yılının son çeyrekteki verileri incelendiğinde ise ülkemizin 16-74 yaş arası nüfusunun internet kullanım oranının %98,5 olduğu ve doğrudan veya dolaylı olarak internete ulaşabildiğini göstermektedir (Türkiye İstatistik Kurumu [TÜİK], 2020).

Teknolojinin oyunlarda neden olduğu dönüşüme paralel olarak dijital yerli olarak kabul edilen günümüz çocuklarının oyun tercihleri değişerek çocukların oyuna olan merakı ve isteği her geçen gün artmaktadır. Geçmişte açık alanda kendi arkadaş çevresiyle oyun oynamayı tercih eden çocuklar şimdilerde teknolojinin hızlı bir şekilde gelişmesiyle beraber kapalı mekanlarda, tanımadığı sanal ortamlardaki hayali veya gerçek bireylerle çevrimiçi oyunlar oynamaktadırlar. Etkisini günden güne daha da artıran sanal ortamdaki eğlence ve oyun kültürü hayatımızda kapladığı alanı artırmakta ve etkisini bir sosyalleşme aracı olarak kullanmaktadır (Horzum, Ayas ve Balta, 2012).

Genç ve yetişkinlerin dijital oyunları oynama amacı daha çok oyunlardan keyif alma ve vakit geçirme olarak görülse de bu durum ilköğretim çağı ve daha öncesi yaştaki bireylerin oynadığı oyunlarda farklı motivasyon amaçları taşımaktadır (Üstündağ, 2019). Güven (2018)'e göre dijital oyunlar, çocuklarda hem sınıf seviyesinde hem de cinsiyet açısından benzer anlamda onların eğlenceli zamanlar geçirmesini sağlayan aktiviteler olduğu görülmektedir. Dahası dijital oyunlar kişiye keyif veren, onun mutlu olmasını sağlayan, çevrimiçi ortamlarda sosyalleşmesine katkı sağlayan bir aktivite, kendini ifade edebilecek beceri kazanması için bir imkân, etkinlik ve stresin yoğunluğunu azaltmayı sağlayan bir yöntem olarak tanımlanmaktadır. Ancak dijital oyunların bireylerin yaşamında zaman alan, eğitim süreçlerini aksatma ihtimali olan ve uzun dönemde kişinin gelişimine etki edebilen (Yücel, 2019) bir yapısının olduğu unutulmamalıdır. Özellikle bağımlılık düzeyinde etkisi olan dijital oyunlar bireylerin oyun içerisinde güç sahibi olmak, verilen aşamaları geçebilmek, rakiplerini geride bırakabilmek, oyun arkadaşlığı, birbirlerine yardımcı olmak, ekip dayanışması, keşfetme, sorumluluk alma gibi motivasyonlar sağlayabilmektedir. Bu tarz motivasyon sağlama yöntemleri ile oyun oynayan bireyler, kendilerine oyunda sunulan kuralları yapması gereken bir görev kabul ederek bir seviyenin içindeki tüm aşamaları geçerek ilerlemeye çalışmaktadır. Oyunlardaki tüm seviyelerin sonunda bir ödül olabileceği gibi oyun oynayan bireylerin

seviye atlama aşamalarını yapıp yapamayacağını kontrol edecek bir durum da olabilir (Yücel, 2019).

Her ne kadar teknolojik ortamlarda oynanan oyunlar cazibeli ve eğlenceli olsa da başta bağımlılık olmak üzere çocuklar üzerinde birçok olumsuz etki yaratmaktadır. Bilgisayar oyunları ilk olarak 1960'lı yıllarda ortaya çıkmaya başlamış ve o zamanlarda yapılan araştırmalarda da bilgisayar oyunlarının bağımlılık yaptığı ortaya konulmaktadır. 1990 yılı ve sonrasında daha çok popüler olan bilgisayar oyunları, teknolojinin hızlı bir şekilde gelişme göstermesiyle sanal gerçekliğin senaryolaştırılmasında rol oynamaya başlamıştır. Teknolojinin gelişmesi ve teknolojik araçlardaki ilerlemeler bilgisayar oyunlarını dijital oyunlara çevirmiş yalnız bilgisayar ortamıyla sınırlı kalmayıp mobil, sanal gerçeklik gözlükleri, simülasyonlar ve oyun konsolları olmak üzere çeşitli teknolojik aletlerle de oynanabilir kılmıştır. Dijital ortamlar yoluyla ortaya çıkan sanal ortamlar, kişilerin gerçek yaşamından kopmadan başka ortam deneyimleri yaşamasına olanak sağlamıştır. Bu tecrübeleri dijital ortamlar yoluyla deneyimleyen kullanıcılar sanal ortam yoluyla çevrimiçi iletişimini ve ilişkilerini genişletirken gerçek yaşamın getirdiği somut durumlardan uzaklaşabilmektedir. Bilhassa genç bireylerin bağımlısı olduğu bu dijital oyunlar, onları gerçek yaşamın sosyalliğinden alarak asosyal kılabilmekte ve sanal ortamda sosyal bir çevre kurmalarına yol açarak gerçek dünyadan uzaklaşmasına neden olmaktadır (Karaduman ve Aciyan, 2020).

İçerikleri açısından incelendiğinde ise birçok oyun şiddet içermektedir ve kurgusunda şiddet olan dijital oyunlar devamlı şiddetin bir sorun çözme yolu olduğunu, hedefe ulaşmak, galip gelmek, daha fazla kişiye egemenlik kurmak için her türlü yolun kullanılması gerektiği mesajını kullanıcılara vermektedir. Bunun yanında dijital ortamların kullanımı çocukların çok fazla enerji harcamadan kişisel vakit geçirmelerine sebep olmakta, çocukların pasif bir şekilde alıcı olmasına neden olmakta ve çocuğun etrafına olan ilgisini azaltmaktadır. Bu durum ebeveynler ile çocukları arasındaki iletişim ve disiplin sorunlarına da yol açabilmektedir (Toran, Ulusoy, Aydın, Deveci ve Akbulut, 2016).

Dijital oyunların bir diğer olumsuz etkisi ise ilköğretim çağı ve öncesi çocuklarda dikkat eksikliği sorunları, agresif hareketler, fiziksel pasiflik, obezite ve uyku düzensizliği problemleri ile dijital oyunlar arasında ilişki kurmasıdır. Gündelik yaşamda teknolojinin çok fazla kullanımı; yemek yeme alışkanlıklarında, teknoloji kullanım

süresinde ve uyku için ayrılması gereken sürede de düzensizliğine neden olmaktadır. Ayrıca çocukların zihinsel ve duygusal gelişimi üzerine kaygı verici neticelere yol açmaktadır (Brown, 2011; akt, Mustafaoğlu ve Ark. 2018).

Dijital teknolojilerin kullanımında ortaya çıkan olumsuz etkilerinden bir başka durum ise bağımlılığa sebep olan beyindeki ödül ceza sisteminin haz duygusundaki aşırı değişimden dolayı işlevini yapamamasıdır. Bu sebeplerden dolayı çocukların dijital aletlere ulaşması güçleştiğinde veya yasaklandığında bağımlılık haline özgü davranışlar ortaya çıkabilmektedir (Mustafaoğlu, Zirek, Yasacı ve Özdiñler, 2018).

Belirtilen tüm bu olumsuz etkilerinin yanında dijital oyunların kişisel mahremiyet açısından da çocuklar üzerinde olumsuz etkileri bulunmaktadır. Erken yaşta çevrimiçi oyunlarla tanışan çocuklar bu oyunlar aracılığıyla başka kullanıcılarla iletişim kurmakta, birlikte ortak oyun amacı ile çeşitli davranışlarda bulunmaktadır. Ancak çocuklarına günlük yaşamda tanımadığı insanlarla konuşmamayı, evde tek başına kaldıklarında tanımadıkları insanlara evin kapısını açmamayı, telefonda konuşurken bilmedikleri kişilere herhangi bir bilgi vermemeyi öğreten, çocuklarının gittikleri yeri, oyun arkadaşlarını, izledikleri TV programlarını ve okudukları kitapları belirleyen aileler; teknolojinin sunduğu sanal ortamlarda gezinen çocuklarını gerektiği kadar denetleyememekte ve onlara rehberlik etmeleri gerektiğinin farkında değildirler (Canbek ve Sarıoğlu, 2007).

Zamanının çoğunu dijital dünyada geçiren çocuklar ve ergenler, ebeveynleri tarafından yeterince bilinçli şekilde denetlenemediklerinden bu durum onların sanal dünyanın yanlış ortamlarına girmesini olası kılmaktadır (Young, 2004; akt: Söğüt, 2020). Çünkü çocuklar ve ergenler dijital ortamın potansiyel tehlikelerinden etkilenmeye en açık kişilerdir. Dijital teknolojilerin bilinçli bir şekilde kullanıldığında kayda değer faydaları olsa da çocukların ve gençlerin, sınırları olmayan dijital ortamda doğabilecek tehlikelere karşı korunmasında ebeveynlere büyük bir sorumluluk düşmektedir (Canbek ve Sarıoğlu, 2007; Söğüt, 2020).

Özellikle aile bireylerinin sosyal medya davranışları ve sosyal medyadaki profil algılarından dolayı çocuklar, dijital dünyanın zararlı olduğu gerçeğini göz ardı etmektedir. Anne babaların dijital dünyadaki mahremiyet konusunda yeterli dikkati göstermemesi, çocuklarında akran gruplarıyla oynadığı dijital oyunlarda aynı davranışa

sebebiyet vermektedir. Bu durum, güvenlik olgusunun çocuklar tarafından önemsenmesine ciddi etki etmektedir. Küçük yaştan itibaren değişik yaş grubu tarafından dijital oyunların oynanması ve küçük yaştaki çocukların aktif olarak yer aldıkları oyunlarda kontrolsüz uzun süreler geçirmesi beraberinde dijital güvenlik açıklarına neden olmaktadır.

Bu bağlamda teknolojinin sürekli gelişmesi ve dijital oyunların sanal gerçekliklerinin ciddi şekilde gelişerek yaşamın bir parçası haline gelmesi, öğrencilerin oyunlardaki davranış algılarında da değişiklik olduğunu ortaya koymaktadır. Çocukların oyunlara olan bağlılığı veya bağımlılık yapacak düzeyleri mahremiyet konusunda yeterli düzeyde önlem alınmasına engel olmaktadır. Ebeveynlerin bilgi güvenliği ve dijital mahremiyet konusundaki farklı dijital okuryazarlık düzeyi, çocukların bilgi güvenliği konusunda kontrolsüz site girişlerini denetleyememesine neden olmakta ve ayrıca dijital oyun dünyası bireylere güvensiz ortamın kapılarını biraz daha aralamaktadır.

Öğrencilerin bilgi mahremiyeti konusundaki hazırbulunuşluk düzeyleri de korunma ve bilgi paylaşımında güvenlik açığı noktasında önemli bir sorun teşkil etmektedir. Bu durum bilgi mahremiyeti dolandırıcılıklarını ve güvenlik risklerini dijital oyun çağındaki çocukları karşı karşıya getirmektedir. Bu nedenle çevrimiçi oyunlar oynayan çocukların siber güvenlik farkındalıkları ile teknoloji okuryazarlık düzeylerinin dijital kimlik mahremiyeti açısından incelenmesi önemli bir durumdur.

Bu araştırma ile ortaokul öğrencilerinin siber güvenlik farkındalıkları ile teknoloji okuryazarlık düzeyleri incelenerek çevrimiçi dijital oyunlarda gerçekleştirilen dijital kimlik mahremiyeti ihlalleri belirlenecektir. Ayrıca araştırma ile siber güvenlik farkındalığı ile dijital okuryazarlık düzeyinin çevrimiçi dijital oyunlardaki dijital kimlik mahremiyeti becerileri üzerindeki etkisi araştırılacaktır.

Amaç

Bu çalışmada Tokat ilinde öğrenim gören ortaokul öğrencilerinin dijital kimlik mahremiyeti becerileri ile teknoloji okuryazarlık düzeylerinin çevrimiçi dijital oyun ortamlarındaki siber güvenlik farkındalıkları üzerindeki etkisinin araştırılması amaçlanmıştır. Bu amaç doğrultusunda çalışmada aşağıdaki sorulara cevap aranmıştır.

1. Ortaokul öğrencilerinin çevrimiçi oyun alışkanlıkları nasıldır?

2. Ortaokul öğrencilerinin çevrimiçi oyunlara yönelik siber güvenlik farkındalık düzeyi nasıldır?
3. Ortaokul öğrencilerinin dijital okuryazarlık düzeyi nasıldır?
4. Ortaokul öğrencilerinin çevrimiçi mahremiyet farkındalık düzeyleri nasıldır?
5. Ortaokul öğrencilerinin çevrimiçi mahremiyet farkındalık düzeyleri ile dijital okuryazarlık düzeylerinin çevrimiçi oyunlarda siber güvenlik farkındalığı üzerindeki etkisi nedir?

Önem

Günümüz dünyasında teknolojinin yaşamın bir parçası olması, bilginin teknoloji ile birlikte sunulması değişen toplumlara göre mahremiyet ve güvenlik kavramlarının değişmesi bireylerin yeni önlemler almasını ve bu önlemleri yaşamın her kademesinde uygulayabilmesini gerektirmektedir. Bu araştırma, ortaokul kademesinde bulunan öğrencilerin siber güvenlik ve bilgi güvenliği kavramlarının ne kadar farkında olduğunu araştırmakla beraber oyun çağındaki çocukların sokaktaki oyunu artık dijital ortamlara taşıyarak kendilerine yeni yaşam alanları oluşturması ve bu sanal yaşam ortamlarında dijital kimlik mahremiyetini ne kadar gerçekleştirebildiğini anlamak için yapılmaktadır. Bu doğrultuda gerçekleştirilecek araştırma incelediği konu ve alanyazına katkı sağlaması bakımından önemlidir.

Ayrıca dijital oyun pazarının giderek büyüdüğü ve çevrimiçi dijital oyun oynama yaşının giderek düştüğü göz önüne alındığında ortaokul düzeyindeki öğrencilerin çevrimiçi dijital oyunlardaki dijital kimlik mahremiyeti becerilerine etki eden değişkenlerin incelenmesi açısından da önem arz etmektedir. Elde edilecek bulgular dijital kimlik mahremiyeti üzerine çalışan araştırmacılara ve ebeveynlere yol gösterecektir.

Bunun yanında gerçekleştirilecek araştırma ile siber güvenlik farkındalığı ve çevrimiçi dijital oyunlardaki dijital kimlik mahremiyeti becerileri ile ortaokullarda verilen “Bilişim Teknolojileri ve Yazılım” dersindeki “Etik ve Güvenlik” ünitesindeki kazanımların ne ölçüde içselleştirildiğini de ortaya koyacaktır. Bu nedenle araştırma sonuçları uygulama sürecinde ilgili kazanımların edinimiyle ilgili uygulayıcılara önemli katkılar sağlayacaktır.

Sayıtlar

Bu araştırmanın sayıtları şunlardır;

- Araştırmaya katılacak Tokat ili ve çevre ilçelerindeki ortaokul öğrencilerinin araştırma ölçeğine doğru ve samimi yanıtlar vereceği,
- Oluşturulacak örneklem gurubunun sayı ve niteliğinin evreni yeterince temsil ettiğı varsayılmıştır.

Sınırlılıklar

Bu araştırmanın sınırlılıkları şunlardır;

- Araştırma 2021-2022 eğitim öğretim yılıyla,
- Tokat ili genelindeki ortaokul öğrencileriyle,
- Çevrimiçi oynanan çok kullanıcılı dijital oyunlarla,

Siber güvenlik, teknoloji okuryazarlığı ve dijital kimlik mahremiyeti değişkenlerinin kapsamıyla sınırlıdır.

Tanımlar

Dijital Oyun: Sanal ortamda konsol (joystick) oyunları, bilgisayar oyunları ve online oyunlar olarak yaygın bir biçimde oynanan yazılım, donanım ve grafik destekli oyunlardır (Esentaş, Güzel ve Vural, 2018).

Çevrimiçi Oyun: Bilgisayar ve taşınabilir dijital aygıtlar ile bir veya daha fazla kişi tarafından internet ağı üzerinden oynanan oyunlardır.

Dijital Kimlik: Bir kullanıcının oyun oynamak gibi tanımlanmış bir ortama dahil olduğunda üstlendiğı kimliktir (Davison, 2012).

Dijital Okuryazarlık: 21. yüzyıl bireylerinin yaşam durumlarında hedeflere ulaşmalarını desteklemek için dijital araçları kullanmaları için gerekli olan becerilerdir (Fu, 2013).

Siber Güvenlik: Siber alanı ve düzeni ve kullanıcı varlıklarının güvenliğini sağlamak için kullanılacak araçlar, yöntemler, güvenlik olguları, yönergeler, tehlikeli durumlar

yönetimi, siber güvenlik eğitimi, güvence ve teknolojilerin toplamıdır (Von Solms ve Van Niekerk, 2013).

Mahremiyet: Kişisel özerkliği, demokratik katılımı, kimlik yönetimini ve sosyal koordinasyonu kapsayan çok yönlü bir kavramdır (Phillips, 2004).



BÖLÜM II

KAVRAMSAL ÇERÇEVE

Bilgi ve Bilgi Güvenliği Kavramı

Bilgi kelimesinin Latince'deki karşılığı herhangi bir şeyi şekillendirme olarak ifade edilse de sözlüklerde birçok anlamı bulunmaktadır. Örnek olarak tanımlara bakılacak olursa bilgi:

- Geçerliliği kanıtlanmış inançlar,
- İlim, bulgu ve gözlem vasıtasıyla elde edilen her türlü realite, veri ve kavrayış,
- Sosyal hayatta meydana gelen ve karşımıza çıkan durumları anlamamızı sağlayan işaretler ve kodlar,
- İnsanın varlığı bilmesi ve ilk sezgi durumunda aklın benimsediği temel fikirler ve yöntemlerden faydalanan bireyin bulgulara yüklediği anlam olarak tanımlanmaktadır.

Bilginin günümüzü etkileyen en önemli varlık olduğu bir gerçektir. Bu noktadan bakıldığında, günümüzün en kıymetli hammaddesi olan bilgiyi anlamak, özümsemek ve bilgi ile ilgili konuları araştırmak, insanlık var olduğundan beridir geçen zamanda geleceğe yönelik ilerlememizi biçimlendiren en önemli araçtır. Yaşadığımız çağda bilginin günümüze damga vuran bir varlık olduğu inkâr edilemez gerçektir. Bu yönden baktığımızda günümüzde çok kıymetli bir hammadde olan bilgiyi ifade etmek, anlamlandırmak ve kavramak ile ilgili durumları inceleyerek insanoğlunun var olduğundan beridir geçen zamanda geleceğe yönelik ilerlememizi sağlayan en önemli anahtardır. Bilgi, günümüz dünyasında önemli bir yere sahiptir. Ancak sadece bugünü değil dünü anlamak ve geleceğe yön vermek için de anahtar rol oynamaktadır (Canbek ve Sağıroğlu, 2006).

Bilginin değeri eğitimde, sağlıkta, hayatın sanat, yaşam gibi çeşitli alanlarında insanoğlunun ilk çağlarından beri anlaşılmakta ve gelecek kuşaklara farklı şekillerde aktarılmaktadır. Bilginin aktarılması ilk zamanlarda masallar hikayeler ve destanlar yoluyla olmuş olsa da daha sonraki dönemlerde medreseler, kiliseler üniversiteler ve yazılı kaynaklar yoluyla olmuştur. Ancak son dönemlerde teknolojinin gelişmesiyle beraber insanoğlu arasındaki iletişim hızlanmış ve iş birliği artmıştır. Bu durum bilgi çağı olarak adlandırılan yeni bir dönemi başlatmıştır. Yaşadığımız döneme adını veren bilgi,

günümüzde insanların yaşantısını yönlendirdiği gibi gelecekte de insanların yaşantısının yönünü belirleyecektir (Vural, 2007).

Bilgi güvenliği ise teknolojik ortamlarda bilginin veya verilerin kaydedilmesi ve transferi sırasında verilerin bütünlüğünün korunmasından izni olmayan kişilerden korunması için emniyetli bir veri işleme platformu oluşturma gayretlerinin tümüdür. Bu durumun gerçekleşmesi için yeterli güvenlik kuralları belirlenmeli ve belirlenen bu kurallar uygulanmalıdır. Bu kurallar; faaliyetlerin incelenmesi, erişimlerin izlenmesi, kayıtlı değişikliklerin değerlendirilmesi ile silme işleminin kısıtlanması gibi bazı kullanım durumlarıyla sınırlandırılabilir. Bilgi güvenliği en genel anlamıyla güvenlikle ilgili konuları kapsamlı olarak ele alan güvenlik mühendisliğinin bir alt basamağı olarak kabul edilmektedir (Canbek ve Sağıroğlu, 2006).

Veri ve teknoloji olarak bilgisayar güvenliğinde karşı taraf, amacı kötü olan insanlar (korsanlar veya hackerler) ve yapmaya çalıştıkları saldırılardır. Mevcut bilgi güvenliğinin yapısını ele geçirmek veya güvenlik duvarını aşmak, yetersiz bırakmak, bireylere direkt veya dolaylı yollarla hasar vermek, sistemleri bozmak, sistemleri çalışamaz hale getirmek, çöktürmek veya tamamen bozmak gibi yapılan teşebbüsler saldırı veya hamle olarak ifade edilmektedir. Korsanlar hedeflerine ulaşmak için değişik yöntemler geliştirerek saldırılar yapmaktadırlar. Ne tür bir saldırı olacağının bilinmesi, saldırının doğru bir şekilde analizinin yapılması ve gereken tedbirlerin alınması, bilgi güvenliği için hayati önem taşımaktadır.

Bilgi güvenliği” bilginin bir varlık olarak zararlardan muhafaza edilmesi, uygun teknolojinin, doğru hedefle ve doğru biçimde kullanılarak verinin her türlü alanda, elde edilmesini istemediğimiz kişileri önleme” olarak ifade edilir. Bir başka tanıma göre ise bilgi güvenliği; bilgilere yasadışı yollarla ulaşılmasından, bilgilerin kullanılmasından, açığa vurulmasından, silinmesinden, değiştirilmesinden veya tahrip edilmesinden koruma yöntemidir. Bu bağlamda bilgi güvenliği; gizliliğin, bütünlüğün ve kullanılabilirliğin muhafazası konusunu önemser (Altun, 2014). Bilgisayar teknolojisindeki güvenlik ise, “resmi ve tüzel kişilerin bu bilgisayar teknolojilerini kullanırken karşılaşılabilecekleri her türlü tehdit ve tehlikelerin çözümlemesini yaparak gerekli tedbirleri en başta almak” olarak ifade edilmektedir (Canbek ve Sağıroğlu, 2006).

Yukarıda da ifade edildiği gibi bilgi güvenliği iki taraflı olarak ele alınmaktadır. Teknik olarak bilginin saklanması, her türlü yasa dışı yollara karşı korunması gibi önemli faktörlerin yanında bireysel olarak bilgilerin korunarak ve paylaşılacak olan bilgilerin seçilmesi kararının verilmesi önemli görülmektedir. İnsan etkeninin bilgi güvenliğinde güvenliği zaafa düşürdüğü kabul edildiğinde güvenliğin tekrar sağlanmasında kişilere bu konularda eğitimler vermek ve kişilerin yeterli bilgi düzeyine sahip olmalarını sağlamak oldukça önemli bir hal almaktadır. Bu maksatla kişilere teknik anlamda eğitim vermenin yanında kişilerde bilgi güvenliği farkındalığı oluşturmak daha faydalı olacaktır. Bilgi güvenliği farkındalığının teknik detaylarına bireyler ne kadar hâkim olursa bireyler kendilerini güvende hissetmelerinin yanında çevrelerini de bu konuda bilgilendirerek bu manada korumaya almış olacaktır (Dönmez, 2019). Kişiler, resmi kurum ve kuruluşlar genelde ciddi herhangi bir olay ortaya çıkmadığı sürece bilgi güvenliği konularında en başta sıkı önlemler alma eğiliminde bulunmamaktadır. Bu yüzden bilgi güvenliği farkındalığını kazandırmak gerekmektedir (Yılmaz, Şahin ve Akbulut, 2016).

Öğrencilerin şifre güvenliği, sanal ortamda güvenli iletişim, zararlı yazılımların kontrolü, dosya muhafazası, kişisel teknolojik aletlerin güvenliği, firewall güvenliği ve virüslere karşı filtreleme programlarının kullanımı, online arkadaş bulma ve internet ortamının yeterince güvenli olup olmadığı konularında farkındalık seviyeleri çok düşüktür. Yapılan araştırmalar göstermektedir ki ailelerin öğrencilerin internete bağlanmaları konusunda koydukları kuralların öğrencilerin bilgi güvenliği farkındalık seviyeleri üzerinde herhangi bir değişiklik oluşturmamaktadır. Yine yapılan araştırmaların sonucu göstermektedir ki öğrenciler etik konularda temel olarak yeterli bilinç seviyesine sahipken, öğrencilerin standartlar ve bilgi isteyen konularda bilgi güvenliği farkındalık seviyesinin daha azdır. Bu durum bilgi güvenliği ve farkındalığı hakkında yapılan eğitimlerin ve uygulamaların yeterli düzeyde olmadığını göstermektedir (M. Tekerek, 2013; A. Tekerek, 2013).

Bilgi Mahremiyeti ve Dijital Kimlik Mahremiyeti

Mahremiyet veya özel hayat genel anlamda bireylerin tek başına yaşayabildikleri, istedikleri gibi hareket edip düşünebildikleri, diğer insanlarla ne şekilde bir ilişki ve iletişim kuracaklarına yer, zaman ve şartlara şahsen kendilerinin karar verdikleri bir ortam ve bu ortam sayesinde sahip oldukları haklara ifade etmektedir (Yüksel, 2003). Mahremiyet, insanoğlunun zamanın her döneminde her toplumda karşılaştığı ve anlam

olarak toplumdan topluma farklılık gösterdiği esnek bir terimdir. Yaşadığımız yüzyılda teknolojik modernleşme ile beraber sosyal ve toplumsal yönlerden mahremiyet, özel yaşamın sınırlarını daraltarak tartışmalı bir hale getirmiştir (Çalışkan, 2019).

Günümüzde yapılan araştırmalardan bazıları göstermektedir ki mahremiyet dijital dünyada günümüz insanının temel bir sorunudur. Diğer taraftan kişiler, özel bilgilerini önemsiz ödülleri karşılığında paylaşabilmektedir. Bu ödüller kimi zaman şirketlerin veya sanal ortamların hediye ettiği fırsatlarken kimi zaman ise sosyal medya ortamlarında arkadaşlarının dikkatini çekme şeklinde olabilmektedir. Yaşadığımız çağda kendi güvenliğimizi korumak için dijital dünyada mahremiyete hala ihtiyaç duyulmaktadır. (Trepte ve Reinecke, 2011; akt, Sezen ve Erden 2018).

Kişilerin dijital ortamlarda meydana gelen mahremiyet haklarına olan saldırılar, bilgi ve iletişim teknolojilerindeki hızlı gelişme ve dönüşümlerle daha kolay hale gelmiştir. Bu zaman diliminde kişilere özgü birçok biçimde içerik üretilmekte ve bu içerikler dijital ortamlarda saklanmaktadır. Bu içerikler dijital ortamlarda kişilerin özel yaşamlarıyla ilgili pek çok bilgiyi de içermektedir. Kişinin sanal ortamdaki davranışları, kişisel gizliliği de dahil olmak üzere, kişinin gerçek yaşamını önemli ölçüde yansıtmaktadır. (Eroğlu, 2018).

Gelişen teknolojinin oluşturduğu denetim kapasitesindeki sayısal artış doğal olarak niteliksel bazı sonuçları meydana getirmektedir. İzleme sıradan bir durum haline gelmekte, yayılmakta ve derinleşmektedir. Resmi ve özel kurumların özel hayata yaptıkları müdahaleleri önlemenin, gözetimden kaçınılmasıyla direk bağlantılı olduğu açıktır. Fakat teknoloji, kanunen denetlenmeyen kişisel gözetim yöntemlerini mümkün kılarak, gözetimden sakınmayı zorlaştırmakta, hatta imkânsız duruma getirmektedir (İzgi, 2009).

Dijital Oyun Kavramı ve Dijital Oyun Pazarı

Oyun kavramı” becerileri ve zekayı geliştiren, belirli oyun yöntemleri olan, hoş vakit geçirmeyi sağlayan eğlence” olarak tanımlanabilir. Oyun denilince klasik olarak akla gelen ilk çağrışım eğlenmek ve hoş bir şekilde vakit geçirme anlamına gelir ve ebeveynlerden çocuklara kadar her yaşta insanın oynayabileceği oyunlar mutlaka vardır (Altunay, 2004). Dijital oyun ise; bilgisayar çevre birimleri ya da konsolların bilgisayar

programları ile etkileşiminin olduğu, belirli kural ve hedefleri olan sistemlerin tamamı olarak tanımlanmaktadır (Günay, 2011). Bir başka tanıma göre ise dijital oyunlar, bilgisayar yazılımları aracılığıyla gerçekliğin bir kopyasının, üretilerek sunulduğu ortamlardır (Darıcı, 2015).

Günümüzde tüm toplumsal alanlarda oynanabilen her türlü oyun artık sanal bir ortama aktarılmış durumdadır. Parklarda ve sokaklarda oynanan her türlü oyun, günümüzde artık evlerde, iş yerlerinde veya internet kafe veya PlayStation salonlarında oynanabilmektedir. Örneğin, günümüzde çocuklar caddelerde veya spor mekânlarında futbol oynamak yerine, etrafındaki insanlara bağımlı-bağımsız evde veya internet salonlarında dijital ortamı kullanarak futbol oynamaktadır (Kaya, 2013).

Türkiye’de hizmet veren oyun ve e-spor ajansı Gaming in Turkey verilerine göre en fazla tercih edilen dijital oyunların günümüzde 15 yaş altı çocukların oynadığı oyunlar olduğu belirtilmektedir (www.gaminginturkey.com). Ancak dijital oyunlar yalnızca gençlerin değil yetişkin bireylerin de tercih ettikleri oyun türüdür. Alanyazın incelendiğinde 2020 yılı ortaları itibariyle dünya genelinde yaklaşık 3,1 milyar insanın dijital oyun oynadığı görülmektedir. Bu rakam toplam dünya nüfusunun %40’ı oranına denk gelmektedir. Salgın döneminde 2020 yılının nisan ayı itibariyle karantinede kalan insan sayısındaki artıştan dolayı dünya genelinde oyun seyirci sayısında %100’lük bir oranda artışla 3,6 milyar seviyelerine ulaştığını bildirmektedir (Öztürk, 2021).

2020 yılı Türkiye Oyun Sektörü Raporuna göre salgın döneminde evde kalan her 5 kişiden 4’ü bir dijital oyun oynadığı belirtilmektedir. Uluslararası oyun piyasası 2020’de %19,6’lık bir gelişme ile 175 dolar seviyesine ulaşmıştır (www.gaminginturkey.com). 2020 yılı bütün olarak değerlendirildiğinde diğer yıllara göre farklı değerlendirilmesi gereken bir yıl olmuştur. Pandemi nedeniyle tüm dünyada kısıtlamaların olması ve tüm aktivitelerin ev içi ile sınırlandırılması zorunluluğundan dolayı 2020’de daha önce hayatında hiç oyun oynamamış kişiler bile oyun oynayarak zaman geçirdiği belirtilmektedir. Bu durum hem dijital oyun oynayan oyuncu sayısında artışa hem de en önemli eğlence alanı olan oyuna ayrılan parasal kaynağın da artmasına sebep olmuştur (www.gaminginturkey.com).

Dijital oyunların ülkemizde gelişimi incelediğinde; 1980’li yıllar da oyun oynama potansiyeli olan insanlar ilk atari oyunuyla tanışmışlardır. Renkli televizyonların hayata

girmesiyle ve insanlara yeni bir eğlence arayışını getirmesiyle video izlemeye talep artmıştır. O gün ki şartlarda insanların atari makinasını hem maliyeti hem de boyutu itibariyle evlere alması zor olduğundan toplu olarak oynayabilecekleri ortamlara ihtiyaç duymuşlardır. Bu durumda ülkenin çoğu yerinde atari salonlarının açılmasına sebep olmuştur. İnternetin yaygınlaşmasıyla çevrimiçi ortamlarda bazı web siteleri de oyunculara, gelecek yıllarda bir arada oyun oynama imkânı vermiştir. Ülkemizdeki bu sebepler, günümüze kadar dijital oyunların önemli bir yol kat etmesini sağlamıştır. Yeni bir alan ve yeni bir medya ortamı olarak dijital oyunlar yaşamımızda yer bulmuştur.

Dijital ortamların yeni bir iletişim ortamı olarak yer bulmasına kadar geçen sürede birçok yerli şirketin dışında, üniversiteler ve servis sağlayıcılarda oyun sektörüne kayda değer katkı sunmuşlardır. Dijital oyunların gelişimine en büyük katkı ise oyun yazılımcılarını, oyunun pazarlama sürecindeki aktörlerini, kurum ve kuruluşları bir araya toplayarak sektörün güvenli bir şekilde büyümesini ve yerli oyun sektörünün önünü açmak amacıyla, T.C. Gençlik ve Spor Bakanlığına bağlı olarak Türkiye Dijital Oyunlar Federasyonu'nun kurulmasını sağlamıştır. Federasyon aile ve çocukların bilinçlendirmesiyle beraber dijital oyunların konumlandırılmasına da aracılık etmiştir (Büyüksakal ve Cansabuncu, 2020).

2020 yılının sonlarına geldiğimizde, yaşamımızın her alanında etkisi olan pandemi süreci oyun sektörünü de doğrudan etkisi altına almıştır. Zaten gelişmekte olan oyun sektörünün gelişim hızı pandemi sebebiyle daha da hızlanmıştır. Dünyanın genelindeki bu gelişme Türkiye içinde geçerli olmaktadır. Çevrim dışı oyunlar yerini, çevrim içi turnuvalara bırakmıştır. Organize edilen sayısız oyun turnuvaları, bilgisayar oyuncuları ve aynı zamanda oyun markaları için yeni bir dünya oluşturmuştur. Bu durumun en önemli örneği ise, dijital oyun sektörünün en çok yatırım yapılan sektör olmasıdır. 2020 ağustos ayı itibariyle oyun pazarında gerçekleşen hisse satış işlemlerinde yaklaşık 2 milyar dolarlık borsada işlem oluşması sonucunda, oyun pazarını en çok yatırım yapılan pazar durumuna taşımıştır (www.gaminginturkey.com).

Dijital Oyunların Sınırlılıkları ve Üstünlükleri

Günümüzde çok çeşitli türleri bulunan dijital oyunların sahip oldukları özelliklere göre önemli üstünlükleri ve aynı zamanda sınırlılıkları bulunmaktadır. Dijital oyunların sınırlılıkları ve üstünlükleri başlıklar halinde verilmiştir.

Dijital Oyunların Sınırlılıkları

Dijital oyunların denetimsiz bir şekilde oynanması problemleri de beraberinde getirmektedir. Bu duruma verilecek en ciddi problem örneği ise dijital oyun bağımlılığıdır (Göldağ, 2019). Bağımlılık genel anlamda, bir maddenin zamanla artan seviyede amacı dışında ve o maddeye karşı duyulan haz sonucu, bireyin hayatında problemlere sebep olduğu halde kullanımına devam edilen ve maddenin alımı azaltıldığında veya bırakıldığında ihtiyaç belirtilerinin ortaya çıktığı bir durumdur. Bu bağımlılık yapan maddelerin genel özelliği tüketimini şiddetlendiren etkide bulunmalarıdır. Beyindeki ödül mekanizmasına etkilerinden dolayı bağımlılık yapan maddelerin haz verici özelliği ve bireylerin devamlı kullanarak bağımlı hale gelmesine sebep olur. Bağımlı birey, hayatındaki bütün olumsuz sonuçlara karşın, bağımlılık yapıcı maddeyi iradesi dışında zorlama yoluyla kullanmaya devam eder (Uğurlu, Şengül ve Şengül, 2012).

Dijital oyun bağımlılığı ise bireylerin çeşitli teknolojik cihazlar aracılığı ile uzun süreler boyunca dijital oyun oynaması nedeniyle fiziksel, sosyal ve duygusal olarak problemler yaşaması durumudur. Dijital oyunların hedef kitlesinin özellikle çocuklar olduğu düşünüldüğünde çocukların bu oyun sektöründen nasıl etkilendiği önemli bir konu olarak ele alınmalıdır. Dijital oyunlar gitgide artan bir şekilde çocuğun ailesi ve arkadaşlarıyla olan sosyal bağlarını koparmakta, okul ve çalışma düzenini değiştirmekte, okula olan aidiyet duygusunu azaltmakta veya bağımlı duruma dönüşmesi gibi sorunlara sebep olmaktadır. Diğer bağımlılık türlerinde de var olduğu gibi devamlı artan haz alma duygusundan dolayı bağımlı olan bireyler dijital oyunlara daha fazla zaman harcamaktadır. Bu bireyler zamanının çoğunu oyun oynamakla harcadıkları için aileleri ve arkadaşları ile ciddi iletişim sorunları yaşamaktadırlar. Bu durum okuldaki yaşantılarını da olumsuz şekilde etkilemektedir (Erboy ve Vural, 2010).

Birçok evde çocuklara ait bilgisayar olması, çocuklarının bilgisayar oyunu oynamaktan zevk alması, çocukların zamanının çoğunu bilgisayar başında geçirmesi, dijital oyunların ergenlik dönemindeki çocukların sosyalleşme sürecine olumsuz etkisi olabileceğini göstermektedir (Koçak ve Köse, 2014). Bağımlı bir hale gelmiş seviyede dijital oyunu oynamak; oyun oynamaktan öğrencilerin vazgeçememesine, gerçek yaşam ile oyun arasında ilişki kuramamasına, günlük rutinlerini aksatmasına ve bilgisayar oyununu diğer işlerine tercih etmek gibi neticelere sebep olmaktadır. Tüm bu nedenler

çocukların okuldaki başarısı ve sosyalleşme sürecine olumsuz bir şekilde etki edeceği varsayılmaktadır (Horzum, 2011).

Dijital oyunların zararlı etkilerinden bir diğeri de içeriğinde yoğun bir şekilde şiddet barındırmasıdır. Oyunların içeriğinde sık sık şiddetin kullanılması kişiler üzerinde şiddete meyil etme veya şiddeti sıradanlaştırma etkilerinin görülmesine rastlamak mümkündür. Dijital oyunların birçoğu, oyuncuların rakiplerine karşı üstün gelmek amacıyla belirledikleri oyun karakterini sürekli geliştirmesi üzerine senaryolaşmaktadır. Oyun içerisindeki bu durum, devamlı artan ve etkisini hiç azaltmayan rekabeti de beraber artırmaktadır. Bu durum oyuncular arasında gergin bir iletişim ve ilişkiye sebep olmaktadır. Bu ilişki bazen gerçek yaşamda oyuncular arasında yaralama ve daha da ileri giderek öldürme boyutuna kadar varmaktadır. İçeriğinde şiddet barındıran oyunları oynayan insanların kişilik özelliklerinde sinirli ve agresif davranışlar sergilediğini ortaya çıkaran çalışmalarda bulunmaktadır (İrmak ve Erdoğan, 2016).

Dijital oyunlar, ergenlik dönemindeki kişilerde çevresiyle olan ilişkilerinde ve sosyalleşme sürecindeki problemlere de neden olmaktadır. Bir kısım ergenler, çoğu zaman yüz yüze olan iletişimden kaçındıkları ve yalnız bir hayatı tercih ettikleri görülmektedir. Ergenler, dijital oyunlar yüzünden aileleri ile aralarındaki ilişkiyi zararlı bir hale getirmektedir. Aile ve toplumsal çevrenin sosyalleşme sürecine sağladığı katkı, dijital oyunlar sebebiyle bu sürecin dışında kalmakta veya etkinliğini ciddi şekilde azaltmaktadır (Koçak ve Köse, 2014).

Dijital Oyunların Üstünlükleri

Bilgisayar oyunları, yalnızca eğlenmek için yapılan bir eylem değil, çocukların ve ergenlerin tek başına herhangi bir şey öğrenmek için zorluk çekmeden yaptığı, becerilerini ortaya koyma fırsatını veren eğitim sürecini de içermektedir (Yiğit, 2007). Bazı araştırmalar, dijital oyun temelli yapılan öğretim yöntemlerinin öğrencilerin derse karşı olan ilgisini artırdığını ve güdülenmesini sağladığını göstermiştir. Derslerde kullanılan oyun temelli eğitsel yöntemler öğrencilerin daha çok ilgisini çekmektedir. Öğrenciler klasik olan kitaptan okuma ve düz anlatım gibi yöntemleri, oyun-temelli öğretime göre daha az ilgi çekici bulmaktadır (Bakar, Tüzün ve Çağıltay, 2008). Benzer şekilde öğrenme şekilleri farklı olan bireylerin öğrenmesine yardımcı olmak adına bilgisayar oyunları çoklu zekâ kuramı açısından da değerlendirilebilir. Oyunlar yapıları

gereği sözel, görsel, işitsel, kinestetik ve içsel zekâlara hitap edebilecek potansiyele sahiptir (Yiğit, 2007).

Oyunlar yalnızca eğlendirme maksatlı olmayıp eğlenmenin yanında öğretmeyi de hedeflediğinden ciddi oyunlar şeklinde ifade edilmektedir. Bireyler yaşamları boyunca oyun olarak yaptıkları eylemlerinde iş olarak yaptıklarından daha fazla haz aldığı bilinmektedir. Ayrıca oyun olarak yaptıkları etkinliklerin öğrenmeyi daha kalıcı hale getirdiği belirlenmiştir. İyi kurgulanmış dijital oyunlar hem çocuk eğitiminde hem de yetişkin eğitiminde kullanılmaya başlanmıştır. Oyunların zamanla sadece eğlence maksatlı olduğu düşüncesi de yavaş yavaş etkisini yitirmektedir. Ciddi oyunlar bireylerde sorun çözme, karmaşık düşünme, taktik geliştirme, iletişim yeteneği ve cesaret gibi yetenekleri kazandırmaktadır. Dikkat eksikliği probleminden dolayı öğrenme güçlüğü olan bireylerde daha kolay öğrenme imkânı sağlamaktadır. Örneğin hiperaktivite bozukluğu olan kişiler yapılan bir etkinliğin aşamalarının sırasını takip etme ve tamamlama durumunda sıkıntı yaşarken, bu durumdaki kişiler bilgisayar oyunlarının kolay ilgi çekmesinden dolayı uzun süre etkinliği devam ettirirler ve öğrenmeyi daha etkili bir hale getirirler (Çakır, 2013).

Vangsnes ve diğerleri (2012) ise öğretmenlerin bilgisayar oyunu etrafında oluşturmaya çalıştıkları pedagojik etkileşimlere, çocuklar tarafından arkadaşlarıyla aralarında rekabetçi bir şekilde yaklaşıldığı konusunda dikkati çekmektedir. Dijital oyunlardan bazılarında bireyler bir takımın parçası olma ve çeşitli görevleri yerine getirme çabası içerisinde. Başardığı zaman ödüllendirme yöntemi ile oyun oynayan kişinin sosyalleşmesine veya farklı sosyal roller edinmesine olanak sağlamaktadır (Gür, 2018).

Ayrıca oyunlar eğlenerek öğrenmeyi kolaylaştırırken aynı zamanda öğrencinin motivasyonunun ve özgüveninin artmasına fayda sağlamaktadır. Bu nedenle sayısal, analitik ve dil öğrenme gibi derslerde oyunla öğretim yoğun olarak kullanılmakta ve öğrenciler oyunla öğretim yöntemine ilgi duymaktadır (Bayırtepe ve Tüzün, 2007). Dijital teknolojilerle oyun yaratıcılığı ve üretkenliği sınırlandırdığı gerekçesiyle eleştirilmektedir ama Bolstad (2004) dijital teknolojilerin, dijital kameralar, programlanabilir oyuncaklar kullanarak ve seçici ve destekleyici bir yaklaşımla yaratıcı bir yönde kullanılabileceğini öne sürmektedir. “Geleneksel” bilgisayar oyunlarından

farklı olarak, programlanabilir ve bilgisayar tarzı düşünmeyi geliştirebilir taşınabilir tablet bilgisayarlar ve akıllı telefonlar, bahsi geçen olumsuzlukları azaltabilir.

Dijital teknolojiler çocukların öğrenmesine ve motivasyonlarına katkı sağlayan bir araç olarak da görülmektedir. Dijital teknolojiler ve oyunlar ile ilgili olarak bir yandan bunun 21. yüzyılda başarı için vazgeçilmez bir araç olduğu öne sürülürken, diğer yandan da gelişim döneminde çocukların bundan olumsuz etkileneceğine ve tehlikelerine dair endişeler dile getirilmektedir. Araştırmacılar tarafından dijital oyunlarla ilgili tartışmada iki boyut ön plana çıkarılmaktadır. Birincisi, dijital teknoloji yoluyla öğrenme konusudur. Bu yolla ayrıca dijital oyuncaklar sıklıkla pazarlama aracı olarak kullanılmakta ve öğrenmede motivasyon sağladığı ileri sürülmektedir. Ancak araştırmalar dijital oyunların ve oyuncakların ilk birkaç buluşmanın ardından o potansiyelini yitirdiğini, dijital etkileşimin tek başına öğrenmeyi garanti etmediğini ortaya koymaktadır. İkincisi ise kullanıcıların dijital oyunlar dolayısıyla ekranda uzun süre sabit kalmalarının fiziksel etkinlik ve sosyal etkileşimi baskıladığı hususudur. Bu yüzden kullanıcılar daha çok grup oyunlarına davet edilmekte ve bilgisayar oyunlarından daha çok hareket gerektiren oyunlara yönlendirilmektedir (Flynn, Richert ve Wartella, 2018).

Çocukların dijital teknoloji oyunları ile olan ilişkisini inceleyen Rideout (2011) araştırmasında, çocukların çoğunun her gün bilgisayar kullanmasına rağmen, bilgisayardan ve dijital oyunlardan daha fazla, televizyon ekranına maruz kaldığını belirtmektedir. İskoç çocukların evde dijital teknolojilerle olan günlük deneyimlerine yönelik çalışmalar içerisinde hem Plowman ve diğerleri (2012) hem de Vandewater (2007) araştırmalarında, “yaygın popüler görüşün aksine” çocukların dijital oyunlar yüzünden dışarıda oynamaktan geri kalmadığını, dijital oyunların çocukların tüm etkinlik alanlarını değiştirmekten ziyade çocukların oyun çerçevesine katkıda bulunduğunu ortaya koymaktadır. Bu bağlamda bakıldığında dijital oyunların çocuklar üzerinde hem sosyalleşmesi hem de asosyalleşmesi yönünde etkisi bulunduğu söylenebilir

Bilgi Güvenliği Açısından Dijital Oyunlar

Dijital dünya, bilgi dağılımı ve paylaşımı konusunda denetimsiz bir ortamdır. Özellikle internet teknolojisinde Web 2.0 araçlarının yaygınlaşması bilgi paylaşımını daha kolay hale getirmiştir. İnternet kullanıcılarının Web 2.0 teknolojisi ile ilgili yeterli bir bilgisi olmasa dahi internet ortamından bilgi paylaşımını kolay bir şekilde

yapabilmektedir. Dijital ortamlarda internet kullanıcılarından bazıları iletişim kurdukları insanlarla gerçek kimlik bilgileriyle değil sahte olan yaş, meslek, cinsiyet gibi kimlik bilgilerini kullanabilmektedirler. Özellikle çocukları hedef alan tehlikeli kişiler bu durumu çocukların aleyhine kullanmakta ve onları özellikle hedef olarak belirleyebilmektedirler (Sırakaya ve Seferoğlu, 2018).

Teknolojik aletleri veya internet ortamını kullanan çocuklar ve ergenler, kullandıkları bu ortamların kendilerine, ailelerine ve teknolojik aletlere gelebilecek olumsuz durumları genel olarak düşünmemektedir. Örneğin, çevrimiçi bir oyun ortamında çocukların tıkladığı bir bağlantı bilgisayara virüs bulaşmasına neden olabilir ve bilgilerinin çalınmasıyla sonuçlanabilir. Bu virüsler farklı yöntemlerle bilgisayara zarar verebilir. Özellikle internet ortamında çocukların ilgisini çekebilecek bu tarz durumlar kolayca yaşanabilmektedir (Canbek ve Sağıroğlu, 2007).

Sosyal medya ve çevrimiçi dijital oyun kullanıcıları bu platformlarda birbirleriyle her an iletişim kurma imkânına sahiptir. Bu gibi durumlarda çocukların kimlerle iletişim halinde olduğu ve iletişim kurduğu insanların doğru insanlar olup olmadığı konusunda ayırt edecek bir dönemde değildirler. Çevrimiçi dijital ortamlardan ve sosyal medya ortamlarından gelecek olan iletişim isteklerine karşı ebeveynlerin ve ilköğretim çağı çocukların bu sanal ortamda oluşacak arkadaşlık isteğine karşı bilinçlendirilmelidir. Çünkü yapılan araştırmalarda ilköğretim çağı çocukların %35'i ve lise çağı öğrencilerinin ise %40'ının dijital oyun oynarken karşı taraftaki kişilerle sohbet ettiğini göstermiştir. Sosyal medya ve dijital oyun ortamlarında ciddi bir tehlike olarak bir başka durum ise lise ve ortaokul öğrencilerinin internet ortamında tanımadığı yabancılarla online iletişim kurmasıdır. Böyle durumlarda aileler çocuklarının hangi platformlarda hangi oyunları oynadığını sıkı bir şekilde takip etmeli, aile içinde oynanacak oyunları tercih etmeli ve bu oyun oynama süresindeki zamanı birlikte geçirecek şekilde ayarlamalıdır (Yaman, Çubukçu, Küçükali ve Yurdakul, 2020).

BÖLÜM III

YÖNTEM

Araştırmanın Modeli

Ortaokul öğrencilerinin çevrimiçi çok kullanıcıli oyunlarda siber güvenlik farkındalığı üzerinde dijital kimlik mahremiyeti becerileri ile teknoloji okuryazarlık düzeyinin etkisinin incelendiği araştırma nicel araştırma yöntemlerinden nedensel-karşılaştırmalı araştırma modeline göre gerçekleştirilmiştir. Nedensel-karşılaştırmalı araştırma modeli, insan katılımcıların özelliklerini manipüle etmenin mümkün olmadığı veya kabul edilebilir olmadığı durumlarda sosyal araştırma yapmak için idealdir. Gerçek deneysel araştırmanın yerine geçer ve gerçek bir deneysel, hatta yarı deneysel bir tasarımın uygulanmasının pratik veya etik olmadığı durumlarda, neden-sonuç veya korasyonel ilişkiler hakkındaki hipotezleri test etmek için kullanılabilir (Simon ve Goes, 2018, s. 98). Nedensel karşılaştırma meydana gelmiş bir vakanın nedenlerini, bu nedenlere etki eden parametreleri veya bir etkinin neticelerini ayırmayı amaçlayan bir araştırma çeşididir. Bilimsel çalışmalarda genel olarak bağımsız değişkenlerin bağımlı değişkenlere olan etkilerini incelemek istendiğinde kullanılan bir yöntemdir (Büyüköztürk ve diğerleri, 2019). Araştırmada ortaokul öğrencilerinin çevrimiçi oyunlardaki siber güvenlik farkındalığı bağımlı değişken, bu değişkenin üzerinde etkisinin incelendiği dijital kimlik mahremiyeti ve teknoloji okuryazarlık düzeyi bağımsız değişkenlerdir.

Evren ve Örneklem

Araştırmanın evrenini Tokat ili genelinde 2021-2022 eğitim öğretim yılında 5, 6, 7 ve 8. sınıfta öğrenim gören ortaokul öğrencileri oluşturmaktadır. Tokat ili ve ilçelerinde ortaokul düzeyinde toplam 28989 öğrenci bulunmaktadır. Araştırmada tabakalı örnekleme yöntemi ve kolayda örnekleme yöntemi bir arada kullanılarak evreni temsil edecek örneklem belirlenmiştir. Tabakalı örnekleme yöntemi, evreni oluşturan alt birimler ve bu alt birimlerin evren büyüklüğü içerisindeki oranının dikkate alındığı bir örnekleme yöntemidir (Büyüköztürk ve diğerleri, 2019). Buna göre öğrencilerin öğrenim gördüğü okul türü ve bulundukları yer (il merkezi ve ilçeler) birer tabaka olarak belirlendikten sonra her bir tabakanın oranı dikkate alınarak kolayda örnekleme yöntemiyle en kolay ve ulaşılabilir olan öğrenciler araştırmaya dahil edilmiştir.

Örneklem sayısını belirlemek için ise Cohen, Manion ve Morrison (2000) tarafından belirlenen tablo kullanılmıştır. Buna göre %95 güvenle olması gereken örneklem sayısı minimum 379 olarak belirlenmiştir. Yapılan araştırmada bu örneklem sayısı ile yeterli kalınmayıp toplam 1480 çevrimiçi oyun oynayan ortaokul öğrencisiyle yüz yüze veri toplanmıştır. Katılımcılara ait demografik bilgiler Tablo 1’de verilmiştir.

Tablo 1. Demografik Bilgiler

		Frekans	Yüzde (%)
Cinsiyet	Kız	688	46,5
	Erkek	792	53,5
Sınıf	5	447	30,20
	6	473	32,0
	7	326	22,0
	8	234	15,80
Günlük Ortalama İnternet Kullanım Süresi	1 Saatten Az	286	19,30
	1-2 Saat	658	44,50
	3-4 Saat	335	22,60
	5-6 Saat	105	7,10
	6 Saatten Fazla	96	6,50
Sahip Olunan Teknolojik Cihazlar	Bilgisayar	616	20,67
	Tablet	683	22,92
	Akıllı Telefon	930	31,21
	Akıllı Saat	200	6,71
	Oyun Konsolu	182	6,11
	Akıllı TV	369	12,38
		Aritmetik Ortalama	Standart Sapma
Yaş		11,98	1,09

Tablo 1’de de görüldüğü gibi 1480 katılımcıdan 792 kişi erkek 688 kişi kız öğrencilerinden oluşmaktadır. Sınıflar bazında öğrenci dağılımına baktığımızda 5. Sınıf öğrenci sayısı 447, 6. Sınıf Öğrenci sayısı 473, 7. Sınıf öğrenci sayısı 326 ve 8. Sınıf öğrenci sayısının 234 olduğu görülmektedir. Günlük ortalama internet kullanım süresine baktığımızda en fazla yığılmanın 658 öğrenci ile 1-2 saat aralığında olduğu ve bu süreyi 335 öğrenci ile 3-4 saat internet kullanımının takip ettiği görülmektedir.

Veri Toplama Araçları

Araştırma problemlerine yanıt bulmak ve verileri toplamak amacıyla 5 farklı bölümden meydana gelen veri toplama aracı hazırlanmıştır. İlk bölüm demografik bilgi formudur. Bu bölümde katılımcıların, cinsiyet, sınıf, yaş, günlük ortalama internet kullanım süresi ve sahip olunan teknolojileri belirlemeye yönelik kategorik ve sıralama düzeyinde sorular bulunmaktadır. İkinci bölüm ortaokul öğrencilerinin çevrimiçi oyun alışkanlıklarını belirlemek amacıyla oluşturulan “Çevrimiçi Oyun Bilgileri” formudur. Bu bölümde ortaokul öğrencilerinin çevrimiçi oyun alışkanlıklarına ilişkin kategorik ve sıralama düzeyinde sorular yer almaktadır. Üçüncü bölüm araştırma kapsamında geliştirilen “Çevrimiçi Oyunlarda Siber Güvenlik Farkındalığı” ölçeğidir. Dördüncü bölüm Pala (2019) tarafından geliştirilen “Dijital Okuryazarlık” ölçeğidir. Beşinci bölüm ise, Korkmaz, Vergili ve Töngel (2019) tarafından geliştirilen “Çevrimiçi Mahremiyet Farkındalık” ölçeğidir.

Çevrimiçi Oyunlarda Siber Güvenlik Farkındalığı Ölçeği

Araştırma kapsamında ortaokul öğrencilerinin çevrimiçi oyunlardaki siber güvenlik farkındalık düzeylerini belirlemek amacıyla bir ölçek geliştirilmiştir. Ölçek geliştirme sürecinde DeVellis (2016)’nın belirttiği aşamalar takip edilmiştir. Her bir aşamada yapılan işlemler alt başlıklar halinde verilmiştir.

Madde Havuzunun Oluşturulması

Ölçeğin geliştirilmesi sürecinde ilk başta ölçek konusunu teşkil eden siber güvenlik farkındalığı ile ilgili literatür taraması yapılmıştır. Literatür incelendiğinde ortaokul öğrencilerine yönelik olarak çok fazla sayıda siber güvenlik ile ilgili öğrenci davranışlarını düzenlemeye yönelik uyarıların olduğu görülmüş ancak siber güvenlik farkındalığı durumunu tespit eden anket ve ölçeğin olmadığı tespit edilmiştir. Literatür araştırmasından sonra hangi alanlarda öğrenciye yönelik tehdit tespiti veya bilgi farkındalığı oluşturulmak isteniyorsa o alanda 4 faktör (Siber Zorbalık, Gizlilik Sorunları, Ücret Bilgilerini Koruma ve İzlenebilirliği Önleme) tespit edilerek toplamda 77 adet taslak madde oluşturulmuştur. Daha sonra taslak maddeler tekrar incelenerek, 43 soruluk bir madde havuzu oluşturulmuştur. Oluşturulan madde havuzu ulusal ve uluslararası siber güvenlik ile ilgili çalışma yapan resmi ve özel kuruluşların en çok siber güvenlik açığı

oluşturan alanlara ağırlık verilmiştir. Maddelerin yazım sürecinde 5’li Likert tipinde 43 madde oluşturulmuş ve her bir madde için “Hiç Katılmıyorum”, “Katılmıyorum”, “Kısmen Katılıyorum”, “Katılıyorum”, “Tamamen Katılıyorum” arasında değerlendirme aralıkları belirlenmiştir.

Uzman Görüşünün Alınması

Kapsam geçerliliğini tespit etmek ve bir bütün olarak ölçeği değerlendirmek amacıyla 6 farklı uzman görüşüne başvurulmuştur. Uzmanlardan 5 öğretim üyesi "Bilgisayar ve Öğretim Teknolojileri Eğitimi" bölümünden 1 öğretim üyesi ölçme ve değerlendirme bölümünden seçilmiştir. Uzman görüşü sonucu ölçeğin kapsam geçerlilik indeksini hesaplamak için uzmanların vermesi istenen cevaplar “Gerekli”, “Gerekli ama düzeltilmeli” ve “Gereksiz” şeklinde üç aşamalı olarak puanlanması istenmiştir. Değeri düşük olan ve gereksiz olarak ifade edilen 13 madde uzman görüşü sonrasında çıkarılmıştır. Kalan 30 maddeden ise 6 maddenin anlamlandırılması noktasında dil bilgisi düzeltilmesi yapılmıştır.

Uzman görüşleri sonrasında düzeltmeler yapılan 30 madde için ayrıca kapsam geçerlilik indeksi (KGİ) hesaplanmıştır. KGİ, maddelerin ölçekte olması ya da olmamasına ilişkin kapsam geçerliğine dayalı bir madde istatistiği olup $KGO = Nu / (N/2) - 1$ formülüne göre hesaplanmaktadır (Lawshe, 1975). Buna göre, Nu, maddeye “Gerekli” diyen toplam uzman sayısını ve N ise maddeye ilişkin görüş bildiren toplam uzman sayısını ifade etmektedir. Yapılan hesaplama sonucu oluşturulan madde havuzundaki 13 madde çıkarıldıktan sonra kalan 30 maddeye ilişkin kapsam geçerlilik indeksi 0,9444 olarak bulunmuştur. Elde edilen kapsam geçerlik indeksi (KGİ) değerinin kapsam geçerlilik ölçütü (KGÖ) değerinden büyük olması ($KGİ > KGÖ$) ölçekte kalan maddelerinin kapsam geçerliğinin istatistiksel olarak anlamlı olduğunu göstermektedir. Kapsam geçerlilik ölçütü (KGÖ) değeri, madde havuzunda yer alan tüm maddelerin (43 Madde) kapsam geçerlilik oranlarının ortalaması alınarak 0,7695 hesaplanmıştır.

Taslak Ölçeğin Uygulanması

Bir sonraki aşamada uzman görüşü sonucunda son hali verilen taslak ölçek geçerlik ve güvenirlik çalışmaları yapılması amacıyla Tokat il merkezindeki 5 ortaokulda (iki ortaokul, iki imam hatip ortaokulu ve bir özel ortaokul) öğrenim gören 5, 6, 7 ve 8.

sınıf düzeyindeki ortaokul öğrencilerine iki farklı zamanda şubat ve mart ayları içerisinde uygulanmıştır. Çalışmanın yapılacağı okullar belirlenirken okulların bulunduğu mahallelerin sosyo-ekonomik ve kültürel yapıları ile eğitim öğretim olanağı farklılığı göz önünde bulundurulmuştur. Çalışmaya katılan öğrencilere çevrimiçi oyun oynayıp oynamadıkları sorulmuş ve bu konudaki hazırbulunuşluk düzeyleri dikkate alınmıştır.

Birinci uygulamada taslak ölçek 720 ortaokul öğrencisine yüz yüze uygulanmıştır. Toplanan verilerden 71 verinin hatalı ve düzensiz girişi yapıldığından bilgisayara girişi yapılmadan elenmiş daha sonra Z skorları $-3 < Z < +3$ aralığı dışında olan 236 veri silinerek 413 veri üzerinden açıklayıcı faktör analizi yapılmıştır. Araştırmaya katılan 413 ortaokul öğrencisinin demografik bilgileri Tablo 2’de gösterilmiştir. Ayrıca çarpıklık değeri ve basıklık değerine bakıldığında; çarpıklık (Skewness) değerinin $-3 < \text{Çarpıklık} < +3$ aralığında olduğu basıklık (Kurtosis) değerinin de $-10 < \text{Basıklık} < +10$ aralığında olduğu görülmüştür. Hesaplanan çarpıklık değerleri -2,776 ile 0,886 arasında, basıklık değerleri ise -1,565 ile 8,603 arasındadır.

Tablo 2. Taslak Ölçeğin Uygulandığı Çalışma Grubuna Ait Demografik Bilgiler

Değişkenler		Frekans (f)	Yüzde (%)
Cinsiyet	Kız	186	45
	Erkek	227	55
Sınıf	5. Sınıf	76	19
	6. Sınıf	104	25
	7. Sınıf	105	25
	8. Sınıf	128	31
İnternet Kullanım Süresi	1 Saatten Az	103	24,9
	1-2 Saat	170	41,2
	3-4 Saat	85	20,6
	5-6 Saat	25	6,1
	6 Saatten Fazla	30	7,2
Oyun Oynama Süreleri	1 Saatten Az	187	45,3
	1-2 Saat	148	35,8
	3-4 Saat	46	11,1
	5-6 Saat	15	3,6
	6 Saatten Fazla	17	4,1

Tablo 2’de görüldüğü gibi 413 öğrenciden 227 kişi ile en fazla erkek öğrencinin katılım sağladığı ve internet kullanım süresinin en fazla 1-2 saat aralığında olduğu, bu süreyi 103 kişi ile 1 saatten az süresinin takip ettiği görülmüştür. Katılımcıların oyun oynama sürelerinin en fazla (n=187) 1 saatten az olduğu ve bu sayıyı 148 öğrenci ile 1-2 saat arasında kullanan öğrencilerin takip ettiği görülmektedir. Sınıf düzeyine bakıldığında en çok 8. sınıftaki öğrencilerin araştırmaya dahil olduğu belirlenmiştir.

Açımlayıcı faktör analizi sonucunda ortaya çıkan ölçeğin yapısını doğrulamak için ikinci bir uygulamaya daha çıkılarak toplanan verilerle doğrulayıcı faktör analizi yapılmıştır. Bunun için ölçek Tokat ilindeki biri özel ikisi devlet ortaokullarında öğrenim gören ve daha önce araştırmaya dahil edilmemiş 503 ortaokul öğrencisine uygulanmıştır. Toplanan verilerin analiz öncesinde Z skorlarına bakılmış ve Z skorları açısından $-3 < Z < +3$ aralığı dışında kalarak uç değer olan 236 veri araştırma kapsamı dışında bırakılarak 267 veri üzerinden doğrulayıcı faktör analizi yapılmıştır. Araştırmaya katılan 267 ortaokul öğrencisine ait demografik bilgiler Tablo 3’te gösterilmiştir. Ayrıca analiz öncesi çarpıklık değeri ve basıklık değerlerine bakılmıştır. Buna göre; çarpıklık (Skewness) değerlerinin $-3 < \text{Çarpıklık} < +3$ sınırında olduğu basıklık (Kurtosis) değerlerinin de $-10 < \text{Basıklık} < +10$ sınırında olduğu görülmüştür. Hesaplanan çarpıklık değerleri -2,456 ile 0,757 arasındadır ve basıklık değerleri ise -1,635 ile 6,083 arasındadır.

Tablo 3. Doğrulayıcı Faktör Analizi Ölçeğinin Demografik Bilgileri

Değişkenler		Frekans (f)	Yüzde (%)
Cinsiyet	Kız	119	44,6
	Erkek	148	55,4
Sınıf	5. Sınıf	71	26,6
	6. Sınıf	59	22,10
	7. Sınıf	55	20,6
	8. Sınıf	82	30,7
İnternet Kullanım Süresi	1 Saatten Az	66	24,7
	1-2 Saat	110	41,2
	3-4 Saat	58	21,7
	5-6 Saat	19	7,1
	6 Saatten Fazla	14	5,2
Oyun Oynama Süreleri	1 Saatten Az	99	37,1
	1-2 Saat	112	41,9

3-4 Saat	43	16,1
5-6 Saat	5	1,9
6 Saatten Fazla	8	3,0

Tablo 3’te görüldüğü gibi 267 öğrenciden 148 kişi ile en fazla katılım sağlayan erkek öğrencinin olduğu ve internet kullanım süresinin en fazla 1-2 saat aralığında olduğu bu süreyi 66 kişi ile 1 saatten az süresinin takip ettiği görülmüştür. Katılımcıların oyun oynama sürelerinin 1-2 saat (n=112) olduğu ve bu sayıyı 99 öğrenci ile 1 saatten az arasında kullanan öğrencilerin takip ettiği görülmektedir. Sınıf düzeyine bakıldığında en çok 8. sınıftaki öğrencilerin araştırmaya dahil olduğu belirlenmiştir.

Geçerlilik ve Güvenirlik Çalışması

Açımlayıcı faktör analizi. Ölçek geliştirme sürecindeki birinci uygulamayla elde edilen veriler üzerinde yapılan açımlayıcı faktör analizi sonucuna göre Kaiser-Mayer-Olkin (KMO) değeri 0,783 olarak hesaplanmıştır. Bartlett küresellik testinin sonucu 1669,414 bulunmuş, p değeri ise $p < 0,5$ olarak hesaplanmıştır. Buna göre veri setinin faktör analizi için uygun olduğu görülmüştür. Gerçekleştirilen faktör analizi sonucunda 12 maddenin (5, 7, 9, 10, 11, 13, 14, 20, 24, 25, 27 ve 29) faktör yük değerleri arasındaki farkın 0,10’dan küçük olması nedeni ile analizden çıkarılmıştır. Madde çıkarımından sonra kalan 18 madde üzerinde yapılan faktör analizi sonucunda 4 faktörlü bir yapı bulunmuştur. Bulunan yapının açıkladığı toplam varyans %50,73, faktör yük değerleri en düşük 0,507, en yüksek 0,811 arasında değişmektedir. Ölçeğin açımlayıcı faktör analizi sonucunda bulunan faktörler siber zorbalık, gizlilik sorunları, ücret bilgilerini koruma ve izlenebilirliği önleme olarak isimlendirilmiştir. Ölçeğin birinci faktörü olan “siber zorbalık” faktörü 5 maddeden, ikinci faktörü olan “gizlilik sorunları” faktörü 3 maddeden, üçüncü faktörü olan “ücret bilgilerini koruma” faktörü 4 maddeden ve son olarak dördüncü faktörü olan “izlenebilirliği önleme” faktörü 6 maddeden oluşmaktadır.

Güvenirlik çalışması kapsamında ise her bir faktör için hesaplanan iç tutarlılık katsayısı (Cronbach Alpha) 0,62 ile 0,74 arasında değişmektedir. Geneli kapsayan güvenilirlik katsayısı ise $\alpha = 0,77$ olarak hesaplanmıştır. Güvenirlik için bir başka güvenilirlik katsayısı olan bileşik güvenilirlik (Composite Reliability-CR) değeri de hesaplanmıştır. Buna göre her bir faktör için hesaplanan bileşik güvenilirlik değeri (CR) 0,78 ile 0,82 arasındadır. Ölçeğin geneline ilişkin bileşik güvenilirlik katsayısı 0,94 olarak

hesaplanmıştır. Ölçeğe ait faktör yük, bileşik güvenirlik ve Cronbach's Alpha değerleri Tablo 4'te verilmiştir.

Tablo 4. Ölçek Faktör Yük, Bileşik Güvenirlik (CR) ve Cronbach' Alpha Değerleri

Faktörler	Faktör Yükü	CR	Cronbach's Alpha
Siber Zorbalık		0,82	0,73
1. Çevrimiçi oyunlarda diğer oyuncuları doğru olmayan bazı davranışları (yalan söyleme, hile yapma vb.) yapmaya zorlarım.	,705		
4. Çevrimiçi oyunlarda rakiplerime onları küçük düşürücü takma isimlerle hitap ederim.	,702		
6. Çevrimiçi oyun oynarken takım arkadaşlarım ve/veya rakip oyuncularla alay ederim.	,770		
7. Çevrimiçi oyun oynarken kazanmak amacıyla doğru olmayan davranışlar (yalan söyleme, hile yapma, zorbalık vb.) yapması için arkadaşlarıma baskı yaparım.	,644		
9. Çevrimiçi oyun oynarken kazanmak için yaptığım doğru olmayan davranışları (yalan söyleme, hile yapma, zorbalık vb.) gerçek hayatta da yapmakta bir sakınca görmem.	,612		
Gizlilik Sorunları		0,80	0,62
12. Çevrimiçi oyunlarda kullanıcı adı ve şifre bilgilerimi takım arkadaşlarımla paylaşıyorum.	,811		
23. Çevrimiçi oyun oynarken seviye atlamak için benden istenildiğinde kişisel bilgilerimi paylaşıyorum.	,800		
24. Çevrimiçi oyun oynadığım oyunculara her zaman güvenirim.	,656		
Ücret Bilgilerini Koruma		0,78	0,70
26. Çevrimiçi oyunlarda kredi kartı bilgisini vermeden önce oyun platformlarının (Steam, Valorant, Minecraft vb.) güvenirliğini kontrol ederim.	,585		
27. Çevrimiçi oyunlarda ödeme yapmam gerektiğinde ailemin bilgisi dahilinde ödeme yaparım.	,765		
28. Çevrimiçi oyunun bölümlerinde ilerleyebilmek için özel yetenek, aksesuar, silah gibi özellikleri satın almam	,787		

gerektiğinde güvenilir ödeme yöntemlerini (Sanal Kart, Banka Havalesi vb.) tercih ederim.

32. Çevrimiçi oyunlarda sadece güvenilir oyun platformlarına (Valorant, Minecraft vb.) ödeme yaparım. ,594

İzlenebilirliği Önleme

0,80

0,74

17. Oynadığım çevrimiçi oyunların her biri için birbirinden farklı giriş şifresi kullanırım. ,507

33. Çevrimiçi oyunlarda lisanslı oyunları tercih ederim. ,683

34. Çevrimiçi oyun oynadığım cihazımda (Bilgisayar, Tablet, Telefon vb.) güncel bir antivirüs yazılımı kullanırım. ,718

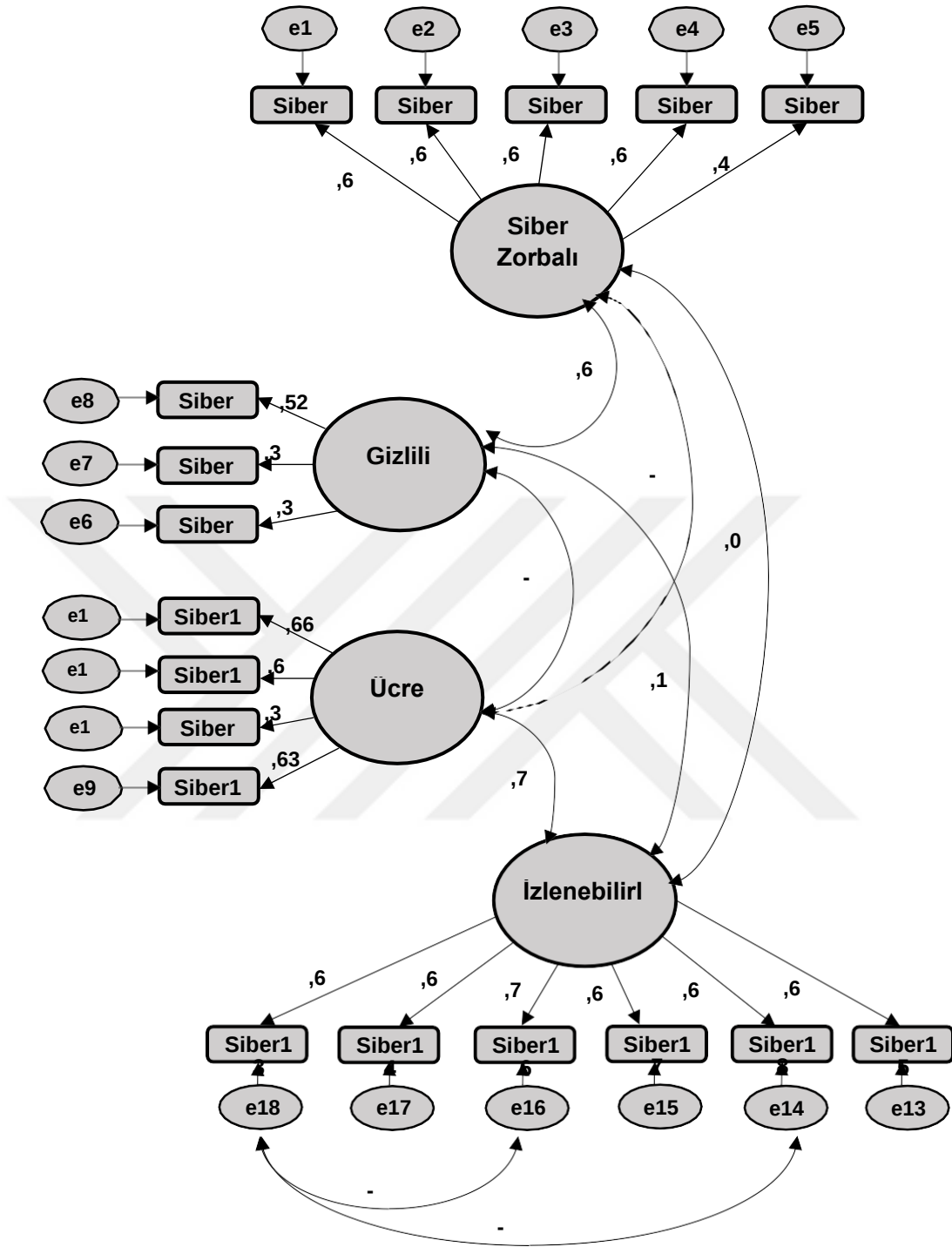
39. Çevrimiçi oyunları güvenilir ortamlardan/ sitelerden indiririm. ,714

41. Çevrimiçi oyun oynarken güvenlik riskleri ile karşılaşabileceğimin farkındayım. ,535

43. Çevrimiçi oyun oynarken izlenebilirliği önlemek için gerekli olmayan erişim izinlerini (konum, mikrofon, kamera vb.) kapatırım. ,636

Geliştirilen ölçeğin dış geçerliliğini belirlemek için benzer yapıyı ölçeğin çevrimiçi mahremiyet farkındalığı ölçeği kullanılarak katılımcıların her iki ölçeğe verdikleri yanıtlar arasındaki ilişkiye bakılmıştır. Buna göre her iki ölçek için hesaplanan Pearson Momentler çarpımı korelasyon katsayısı $r=0,525$, $p<.05$ hesaplanmıştır. Buna göre her iki ölçek arasında pozitif yönlü orta düzeyde ve istatistiksel olarak anlamlı bir ilişki bulunmaktadır. Çevrimiçi mahremiyet farkındalığı ölçeğinin iç tutarlılık katsayısı $\alpha=0,85$ olarak bulunmuştur.

Doğrulamalı faktör analizi. Açıklayıcı faktör analizi ile belirlenen ölçme modelinin geçerliliğini ve doğruluğunu test etmek amacıyla ölçeğin son hali farklı bir çalışma grubunda tekrar uygulanmıştır. Gerçekleştirilen birinci düzey çok faktörlü doğrulamalı faktör analizi sonucunda Şekil 1’de görüldüğü gibi gözlenen değişkenlerin faktör yüklerinin 0,33 ile 0,78 arasında olduğu ve bu değerlerin istatistiksel olarak anlamlı olduğu ($p<.05$) görülmüştür. Model uyumu değerleri incelendiğinde model uyumu (beklenen kovaryans matrisi ile gözlenen matrisler arasındaki fark) istatistiksel olarak anlamlı bir biçimde farklı değildir ($\chi^2=231.675$, $df=127$, $p<.05$).



Şekil 1. Ölçek İçin İkinci Düzey DFA Sonuçları

Tablo 5. Siber Güvenlik Farkındalığı Ölçeği İçin Çok Faktörlü DFA Uyum İndeksleri

Uyum İstatistikleri	İyi Uyum	Modele Ait Uyum Değeri
P	$p>.05$	0.000
χ^2/df	≤ 5	1.824
RMSEA	≤ 0.08	0.058
SRMR	< 0.08	0.063
GFI	≥ 0.90	0.91
AGFI	≥ 0.90	0.88
CFI	≥ 0.90	0.90
IFI	≥ 0.90	0.90

Ayrıca Tablo 5'te verilen model uyumu için değerlendirilen ve alanyazında en yaygın kullanılan (Kline, 2005; Tabachnick ve Fidell, 1996) alternatif uyum indekslerine göre $\chi^2/df=1.824$, RMSEA=0.058, SRMR=0.063, GFI=0.91, AGFI=0.88, IFI=0.90 ve CFI=0.90 değerlerinin iyi (kabul edilebilir) uyum olarak ifade edilen aralık sınırında olması doğrulayıcı faktör analizi ile test edilen teorik modelin uygunluğunu göstermektedir. Buna göre örtük değişkenin gözlenen değişkenleri anlamlı bir biçimde yordadığı ve örtük değişkenin gözlenen değişkenler ile yeterli bir biçimde temsil ettiği belirlenmiştir. Sonuç olarak ortaokul öğrencilerinin çevrimiçi oyunlardaki siber güvenlik farkındalıklarını ölçmek amacıyla hazırlanan 18 maddelik ölçeğin dört faktörden oluşan yapıyı doğru bir şekilde ölçtüğü doğrulanmıştır.

Dijital Okuryazarlık Ölçeği

Ortaokul öğrencilerinin çevrimiçi oyunlardaki dijital okuryazarlık düzeylerini belirlemek için Pala (2019) tarafından geliştirilen 5'li Likert tipinde 21 maddeden oluşan, her bir madde "Hiçbir Zaman", "Nadiren", "Bazen", "Çoğu Zaman", "Her Zaman" arasında değer almış olan, Dijital Okuryazarlık Ölçeği kullanılmıştır. Ölçek Erzincan ili merkezindeki üç ortaokulda 5. sınıfta öğrenim gören 168 ortaokul öğrencileri üzerinde geliştirilmiştir. Ölçek 4 faktörlü bir yapıya sahiptir. Bu faktörler "Bilgi-işlem", "İletişim", "Güvenlik" ve "Problem çözme" olarak ifade edilmiştir. Dört faktörlü ölçeğin açıkladığı toplam varyans %50,75'tir. Açımlayıcı faktör analizi sonucu elde edilen dört faktörlü ölçeğin yapı geçerliliği, doğrulayıcı faktör analiziyle test edilmiştir. Doğrulayıcı faktör analizi sonucunda $\chi^2/df=2.72$, RMSEA=0.04, SRMR=0.04, GFI=0.94, AGFI=0.92, NFI=0.96 ve CFI=0.97 değerleri bulunarak ölçeğin dört faktörlü modelinin uyumlu

olduğu ve ölçeğin doğrulandığı bulunmuştur. Ölçeğin, Cronbach Alpha güvenirlik katsayısı .877 ve test tekrar test güvenirlik katsayısı .72 olduğu belirtilmiştir. Çalışma sonuçlarına göre dijital okuryazarlık ölçeğinin geçerli ve güvenilir bir ölçek olduğu sonucuna varılmıştır.

Çevrimiçi Mahremiyet Farkındalığı Ölçeği

Araştırmada ortaokul öğrencilerinin çevrimiçi mahremiyet farkındalık düzeylerini belirlemek için Korkmaz, Vergili ve Töngel (2019) tarafından bireylerin çevrimiçi ortamlarda gizlilik farkındalıkları düzeyini belirlemek amacıyla geliştirilen 5’li Likert tipinde 17 maddeden oluşan, her bir madde “Kesinlikle Katılmıyorum”, “Katılmıyorum”, “Kararsızım”, “Katılıyorum”, “Kesinlikle Katılıyorum” arasında değer almış olan, çevrimiçi mahremiyet farkındalığı ölçeği kullanılmıştır. Ölçek Amasya ve Ordu Üniversitesinde eğitim gören 552 üniversite öğrencisi üzerinde geliştirilmiştir. Ölçek 3 faktörlü bir yapıya sahiptir. Bu faktörler “Dikkat”, “Güvenlik”, “İletişim ve Paylaşım” olarak ifade edilmiştir. Üç faktörlü ölçeğin açıkladığı toplam varyans %47,709’dur. Açımlayıcı faktör analizi sonucu elde edilen üç faktörlü ölçeğin yapı geçerliliği, doğrulayıcı faktör analiziyle test edilmiştir. Doğrulayıcı faktör analizi sonucunda $\chi^2(sd=108, N=514) = 343.186$, $\chi^2/sd = 3,178$; $p<.001$, RMSEA= .065, S-RMR= .064, GFI= .929, AGFI= .900, CFI= .903, NFI= .866 ve IFI= .904 değerleri bulunmuştur. Ölçeğin, Cronbach Alpha güvenirlik katsayısı .794 ve test tekrar test güvenirlik katsayısı .630 olduğu belirtilmiştir. Çalışma sonuçlarına göre çevrimiçi farkındalık ölçeğinin geçerli ve güvenilir bir ölçek olduğu sonucuna varılmıştır.

Üniversite öğrencileri üzerinde geliştirilen ölçek ortaokul öğrencilerine uygulanmadan önce, ortaokul öğrencileri üzerinde geçerlik ve güvenirlik çalışmaları yapılmıştır. Buna göre 413 ortaokul öğrencisinden toplanan verilerle doğrulayıcı faktör analizi yapılarak üniversite öğrencileri üzerinde geliştirilen ölçeğin yapısı ortaokul öğrencileri üzerinde tekrar test edilmiştir. Gerçekleştirilen birinci düzey çok faktörlü doğrulayıcı faktör analizi sonucunda gözlenen değişkenlerin faktör yüklerinin 0,32 ile 0,77 arasında olduğu ve bu değerlerin istatistiksel olarak anlamlı olduğu ($p<.05$) görülmüştür. Model uyumu değerleri incelendiğinde model uyumu (beklenen kovaryans matrisi ile gözlenen matrisler arasındaki fark) istatistiksel olarak anlamlı bir biçimde farklı değildir ($\chi^2=205,345$, $df=113$, $p<.05$).

Ayrıca model uyumu için değerlendirilen ve alanyazında en yaygın kullanılan (Kline, 2005; Tabachnick ve Fidell, 1996) alternatif uyum indekslerine göre $\chi^2/df=1.817$, RMSEA=0.045, SRMR=0.048, GFI=0.94, AGFI=0.92, IFI=0.96 ve CFI=0.96 değerlerinin iyi (kabul edilebilir) uyum olarak ifade edilen aralık sınırında olması doğrulayıcı faktör analizi ile test edilen teorik modelin uygunluğunu göstermektedir. Buna göre örtük değişkenin gözlenen değişkenleri anlamlı bir biçimde yordadığı ve örtük değişkenin gözlenen değişkenler ile yeterli bir biçimde temsil ettiği belirlenmiştir. Sonuç olarak üniversite öğrencilerinin çevrimiçi mahremiyet farkındalıklarını ölçmek amacıyla geliştirilen 17 maddelik ölçeğin 3 faktörlü yapısının ortaokul öğrencileri üzerinde doğru bir şekilde ölçtüğü doğrulanmıştır.

Veri Toplama Süreci

Araştırmanın veri toplama sürecinde öncelikle Tokat İl Milli Eğitim Müdürlüğünden gerekli izinler alındıktan sonra uygulama yapılacak okullarla birebir görüşülerek veri toplama süreci planlanmıştır. Alınan izinler doğrultusunda veriler araştırmacı tarafından yüz yüze uygulanmıştır. Araştırma verileri 2021-2022 eğitim öğretim yılı bahar yarıyılı başında Şubat, Mart ve Nisan aylarında yapılmıştır yaklaşık 10 hafta sürmüştür. Veri toplama sürecinde Millî Eğitim Bakanlığı'na bağlı 15 ortaokuldaki 5, 6, 7 ve 8. sınıflarda öğrenim gören ortaokul öğrencilerinden hem ölçek geliştirme süreci hem de araştırmanın amaçlarına yönelik olarak yüz yüze toplam 2900 veri toplanmıştır.

Verilerin Analizi

Toplanan verilerin analizi öncesi 1720 veri içerisinde veriler kontrol edilerek geçersiz olan 211 veri analiz dışında bırakılmıştır. Veri toplama araçlarında bulunan değerlendirme aralıkları dikkate alınarak her bir katılımcının veri toplama aracına verdikleri cevaplar IBM SPSS 22 yazılımına işlenmiştir. Ayrıca analiz öncesi veri setinin Z skorlarına bakılmış ve $-3 < Z < 3$ aralığında olmayan 29 veri araştırma dışında bırakılarak 1480 veri üzerinden analizler gerçekleştirilmiştir. Daha sonra veri analizi öncesi parametrik testlerin gerçekleştirilebilmesi için normallik analizi yapılmıştır. Verilerin normalliği için basıklık ve çarpıklık değerlerine bakılmıştır. Toplanan verilere ilişkin basıklık ve çarpıklık değerleri Tablo 6'da verilmiştir.

Tablo 6. Basıklık ve Çarpıklık Değerleri

	Basıklık	Çarpıklık
Siber Güvenlik Ölçeği	-,494	-,346
Çevrimiçi Mahremiyet Farkındalığı Anketi	,030	-,773
Dijital Okuryazarlık Ölçeği	-,024	,205

Tablo 6’da görüldüğü gibi test sonuçlarının normal dağılım aralığı olan -1 ile +1 arasında değerleri gösterdiği belirlendikten sonra araştırma soruları dikkate alınarak analizler gerçekleştirilmiştir. Buna göre;

Birinci araştırma sorusunun çözümlenmesinde araştırmaya katılan ortaokul öğrencilerinin siber güvenlik farkındalık düzeylerinin belirlenmesinde aritmetik ortalama, standart sapma, yüzde, frekans gibi betimsel istatistikler kullanılmıştır.

İkinci, üçüncü ve dördüncü araştırma soruları için aritmetik ortalama, standart sapma, yüzde, frekans gibi betimsel istatistiklerin yanı sıra ölçeklerden elde edilen sonuçlar değerlendirme aralıkları belirlenerek çözümlenmiştir. Değerlendirme aralığı her bir ölçekteki 5’li Likert tipi ifadeler için $n=5$ olmak üzere $(n-1/n)$ formülünden yararlanarak yapılmıştır.

Araştırmanın beşinci araştırma sorusunun çözümlenmesinde ise bağımsız değişkenlerin tek tek ve bir arada bağımlı değişken üzerindeki etkilerini belirlemek için basit ve çoklu doğrusal regresyon analizleri yapılmıştır.

BÖLÜM IV

BULGULAR

Ortaokul Öğrencilerinin Çevrimiçi Oyun Alışkanlıkları

Ortaokul öğrencilerinin çevrimiçi oyun alışkanlıkları; sırasıyla günlük ortalama çevrimiçi oyun oynama süresi, oyun oynanan platformlar, oyun oynama sıklığı, oynanan oyunların türleri, çevrimiçi oyun oynanan yer, en çok oynanan çevrimiçi oyunlar, çevrimiçi oyun için aylık yapılan harcama, oyun için satın alınan teknolojik cihazlar ve takım halinde oynanan oyunlarda ortalama kaç kişi sayısı değişkenlerine göre incelenmiş ve bulgular frekans ve yüzde olarak sunulmuştur.

Araştırma kapsamında ortaokul öğrencilerinin günlük ortalama çevrimiçi oyun oynama süreleri Tablo 7’de çevrimiçi oyun oynama sıklıkları ise Tablo 8’de verilmiştir.

Tablo 7. Günlük Ortalama Çevrimiçi Oyun Oynama Süreleri

	1 Saatten Az		1-2 Saat		3-4 Saat		5-6 Saat		6 Saatten Fazla	
	f	%	f	%	f	%	f	%	f	%
Hafta içi	552	37,3	594	40,1	210	14,2	54	3,6	70	4,7
Hafta sonu	295	19,9	566	38,2	390	26,4	118	8,0	111	7,5
Toplam	847	28,61	1160	39,19	600	20,27	172	5,81	181	6,11

Tablo 8. Çevrimiçi Oyun Oynama Sıklıkları

	Frekans (f)	Yüzde (%)
Haftada 1 Defadan Az	198	13,4
Haftada En Az Bir Defa	270	18,2
Haftada 1 Defadan Fazla	498	33,6
Hemen Hemen Her Gün	344	23,2
Düzenli Olarak Her Gün	170	11,5
Toplam	1480	100,0

Tablo 7 ve 8’de görüldüğü gibi ortaokul öğrencilerinin yarısından fazlasının (%67,80) çevrimiçi oyunlarda hafta içi ve hafta sonu dahil günlük ortalama 2 saate kadar vakit geçirmektedir. Ayrıca araştırma kapsamındaki ortaokul öğrencileri hafta içi ağırlıklı olarak 2 saate kadar oyun oynarken (%77,40) hafta sonu bu süre 4 saate kadar çıkmaktadır

(%64,60). Öğrencilerin haftada bir defadan fazla olmak üzere düzenli olarak çevrimiçi oyun oynadığı görülmüştür.

Ortaokul öğrencilerinin oynadıkları çevrimiçi oyun türlerine ilişkin bilgiler Şekil 2’de verilmiştir.



Şekil 2. Ortaokul Öğrencilerinin Oynadıkları Çevrimiçi Oyun Türleri

Şekil 2’de görüldüğü gibi ortaokul öğrencilerinin çevrimiçi olarak en çok macera oyunlarını (f=863; %26,53), savaş oyunlarını (f=831; %25,55) ve strateji oyunlarını (f=497; %15,28) oynadığı belirlenmiştir. Ortaokul öğrencilerinin en az oynadığı oyun türü ise rol yapmadır (f=234; %7,19).

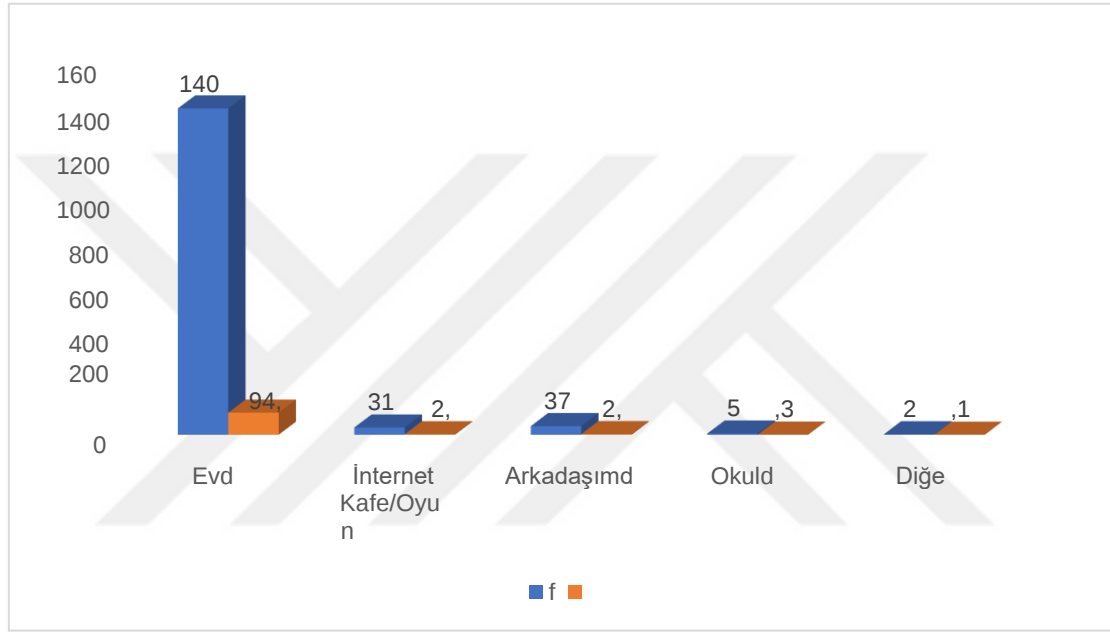
Araştırma kapsamında ortaokul öğrencilerinin çevrimiçi oyunları en çok hangi platform üzerinden oynadıklarına ait bilgiler Tablo 9’da görülmektedir.

Tablo 9. Ortaokul Öğrencilerinin Çevrimiçi Oyunları En Çok Oynadıkları Platformlar

Platformlar	f	%
Cep Telefonu	704	47,6
Bilgisayar	385	26,0
Tablet	381	25,7
Xbox	8	0,5
Diğer	2	0,1
Toplam	1480	100,0

Tablo 9’da görüldüğü gibi araştırmaya katılan ortaokul öğrencileri çevrimiçi oyunları en çok cep telefonu (%47,6) platformu üzerinden oynadıkları en az ise Xbox (%0,5) platformu üzerinden oynamaktadırlar. Diğer taraftan ortaokul öğrencilerinin bilgisayar ve tablet üzerinden oyun oynama durumlarının birbirine yakın olduğu görülmektedir.

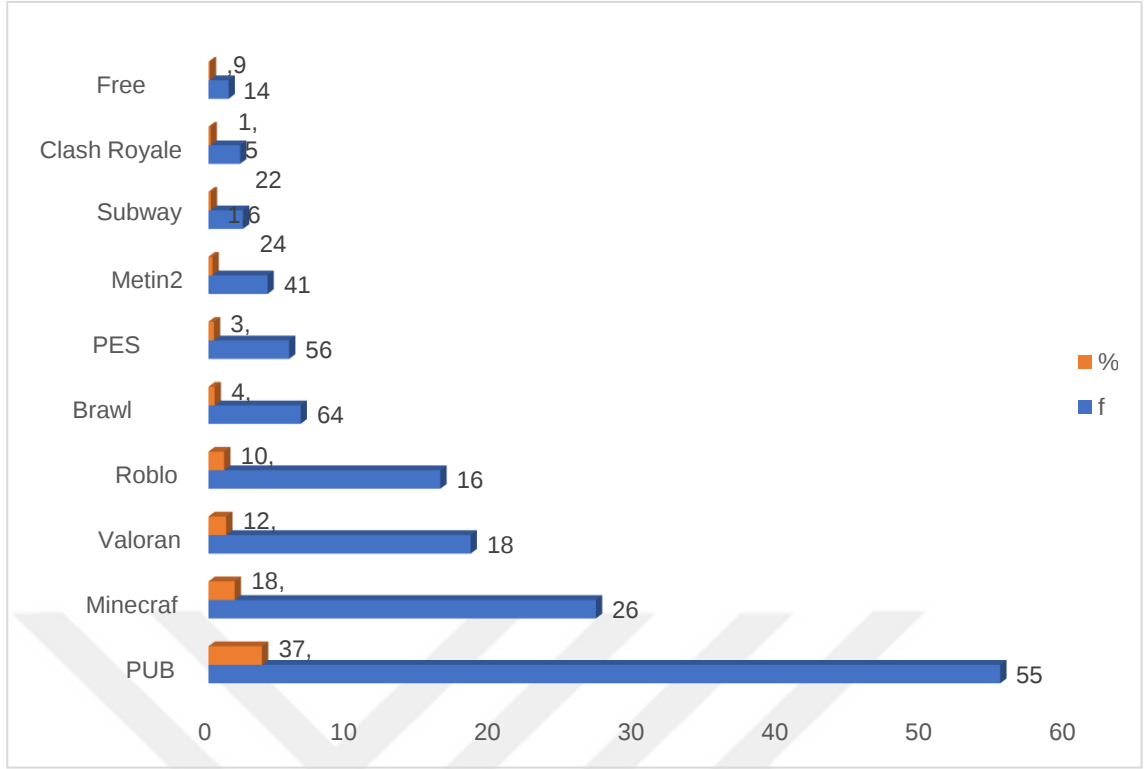
Ortaokul öğrencilerinin çevrimiçi oyunları oynadıkları yere ilişkin bilgiler Şekil 3’te verilmiştir.



Şekil 3. Ortaokul Öğrencilerinin Çevrimiçi Oyunları Oynadıkları Yer

Şekil 3’te görüldüğü gibi ortaokul öğrencileri çevrimiçi oyunları genellikle evde (%94,9) oynamaktadır. Öğrencilerin çevrimiçi oyunları sırasıyla arkadaşlarında (%2,5), internet kafe/oyun salonunda (%2,1) ve okul ortamında (%0,3) oynadıkları belirlenmiştir.

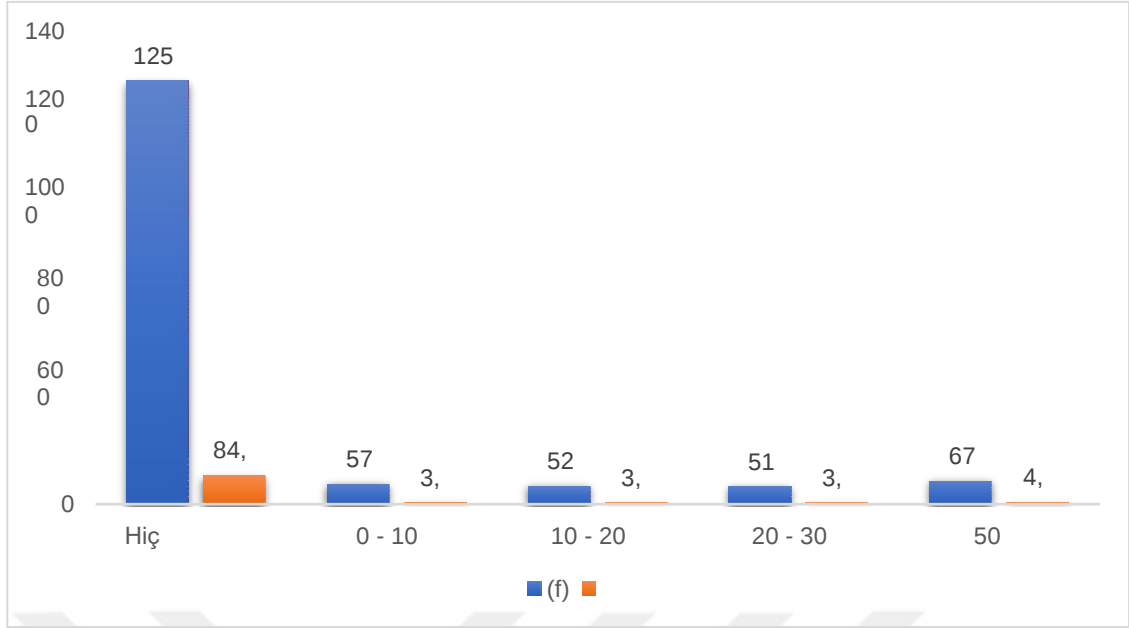
Ortaokul öğrencilerinin en çok oynadığı 55 farklı çevrimiçi oyundan ilk 10 da yer alan çevrimiçi oyun ise Şekil 4’te görülmektedir.



Şekil 4. Ortaokul Öğrencilerinin En Çok Oynadığı Çevrimiçi Oyunlar

Şekil 4'te görüldüğü gibi ortaokul öğrencilerinin en çok oynadığı 55 farklı çevrimiçi oyun içerisinde en çok oynayan oyunun PUBG (%37,2) ve Minecraft (%18,2) oyunları olduğu görülmektedir. Buna göre araştırmaya katılan ortaokul öğrencilerinin yarısı (%55,4) çevrimiçi olarak PUBG veya Minecraft oyunlarını oynamaktadır.

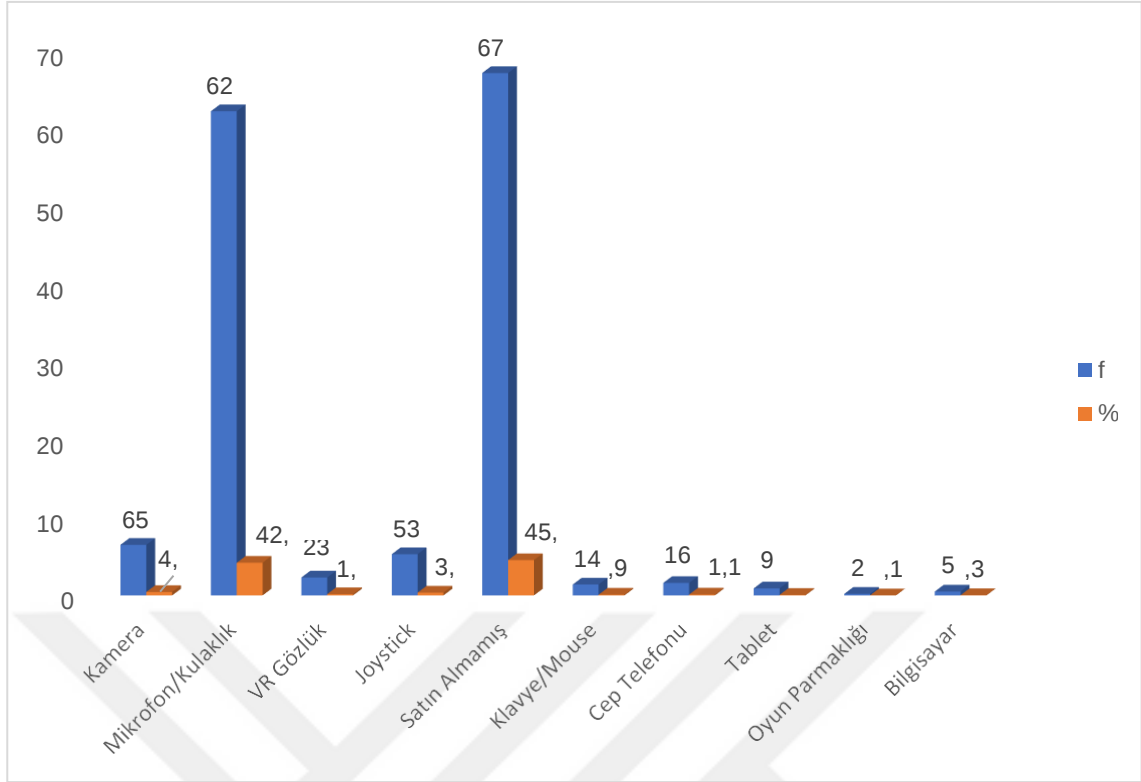
Ortaokul öğrencilerinin çevrimiçi oyunlar için aylık ortalama harcadıkları para miktarına ilişkin bulgular Şekil 5'te verilmiştir.



Şekil 5. Ortaokul Öğrencilerinin Çevrimiçi Oyunlar İçin Aylık Ortalama Harcadıkları Para Miktarı

Şekil 5’te görüldüğü gibi araştırmaya katılan ortaokul öğrencileri çevrimiçi oyunlara çoğunlukla hiç harcama yapmadığı (%84,7) buna karşın az miktardaki ortaokul öğrencisinin çevrimiçi oyunlar için ortalama aylık 0-50 TL arasında harcama yaptığı görülmektedir. Bu durum araştırma kapsamındaki öğrencilerin çevrimiçi oyun için büyük çoğunluğunun aylık olarak ciddi miktarda para harcamadığını göstermektedir. Çevrimiçi oyunlara harcama yapanlar içerisinde ise aylık olarak en fazla 50 TL (%4,5) çevrimiçi oyunlara harcama yapıldığı görülmektedir.

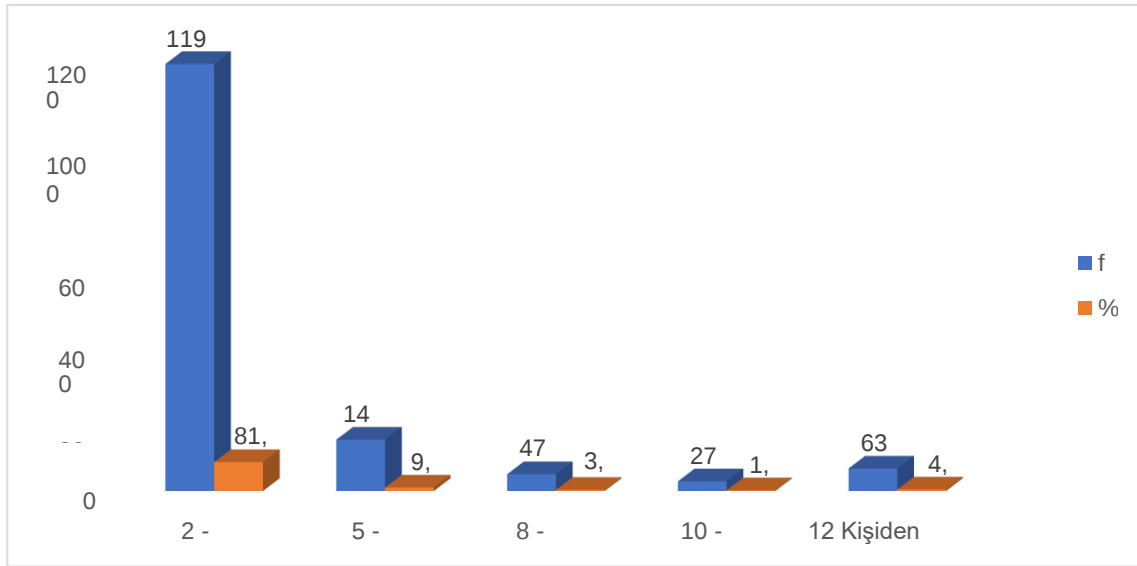
Ortaokul öğrencilerinin çevrimiçi oyun oynamak için satın aldığı cihazlara ilişkin bulgular Şekil 6’da verilmiştir.



Şekil 6. Ortaokul Öğrencilerinin Çevrimiçi Oyun Oynamak İçin Satın Aldığı Cihazlar

Şekil 6’da görüldüğü gibi araştırmaya katılan ortaokul öğrencilerinin yarısından fazlasının (%54,7) çevrimiçi oyunlar için teknolojik araç satın aldığı buna karşın diğer bölümünün (%45,3) çevrimiçi oyunlar için teknolojik araç satın almadığı görülmektedir. Öğrencilerin çevrimiçi oyunlar için satın alınan teknolojik cihazlar incelendiğinde en fazla mikrofon/kulaklık (%42,0) aldıkları görülürken en az oyun parmaklığı (%2,0) aldıkları görülmektedir.

Ortaokul öğrencilerinin takım halinde çevrimiçi oyun oynarken ortalama oyun oynadıkları kişi sayısına ilişkin bulgular Şekil 7’de verilmiştir.



Şekil 7. Ortaokul Öğrencilerinin Takım Halinde Çevrimiçi Oyun Oynarken Ortalama Oyun Oynadıkları Kişi Sayısı

Şekil 7’de görüldüğü gibi, araştırma kapsamındaki öğrenciler çevrimiçi oyun oynarken en çok 2 ile 4 kişi (%81) arasındaki takımlarda oyun oynamaktadır. Daha sonra sırasıyla 5-7 kişilik takımlar (%9,7) ve 12 kişiden fazla olan takımlar (%4,3) gelmektedir. Diğer taraftan ortaokul öğrencileri çevrimiçi oyunlarda en az 10-12 kişilik takımlarda (%1,8) oyun oynamaktadır.

Ortaokul Öğrencilerinin Çevrimiçi Oyunlara Yönelik Siber Güvenlik Farkındalık Düzeyleri

Araştırma kapsamında ortaokul öğrencilerinin çevrimiçi oyunlara yönelik siber güvenlik farkındalık düzeylerini belirlemek amacıyla geliştirilen ölçekten elde edilen sonuçlar değerlendirme aralıkları belirlenerek çözümlenmiştir. Değerlendirme aralığı 5’li Likert tipi ifadeler için $n=5$ olmak üzere $(n-1/n)$ formülünden yararlanarak yapılmıştır. Ölçekteki olumsuz maddeler anlaşılabilirliği artırmak amacıyla ters çevrilerek ortalamaları hesaplanmıştır. Ölçek geneli ve her bir alt boyut açısından genel durumları Tablo 10’da verilmiştir.

Tablo 10. Ortaokul Öğrencilerinin Çevrimiçi Oyunlara Yönelik Siber Güvenlik Farkındalık Durumları

	Ortalama ($\bar{X}$)	Standart Sapma (SS)	Minimum	Maximum
Ölçek geneli	3,94	0,57	2,22	5,00

Siber Zorbalık	4,56	0,71	1,00	5,00
Gizlilik Sorunları	4,42	0,68	1,00	5,00
Ücret Bilgilerini Koruma	3,38	1,19	1,00	5,00
İzlenebilirliği Önleme	3,55	0,89	1,00	5,00

Tablo 10’da görüldüğü gibi araştırmaya katılan 1480 ortaokul öğrencisinin çevrimiçi oyunlara yönelik siber güvenlik farkındalık ortalama puanı 3,94 olarak hesaplanmıştır. Buna göre ortaokul öğrencilerinin çevrimiçi oyunlara yönelik siber güvenlik farkındalık düzeylerinin iyi olduğu görülmüştür. Alt boyutlar açısından farkındalıkları incelendiğinde ise ortaokul öğrencilerinin en çok siber zorbalık ($\bar{X}=4,56$; $SS=0,71$) boyutuna ilişkin becerilere, en az ise ücret bilgilerini koruma ($\bar{X}=3,38$; $SS=1,19$) alt boyutuna ilişkin becerilere sahip olduğu görülmüştür.

Siber zorbalık ($\bar{X}=4,56$; $SS=0,71$) ve gizlilik sorunları ($\bar{X}=4,42$; $SS=0,68$) alt boyutları açısından ortaokul öğrencilerinin çok iyi düzeyde oldukları görülmektedir. Buna göre ortaokul öğrencilerinin çevrimiçi oyunlarda doğru olmayan davranışlar yapma, rakipleriyle alay etme, takım arkadaşlarına baskı kurma, kullanıcı adı ve şifre bilgilerini takım arkadaşlarıyla paylaşma, kişisel bilgilerini paylaşma ve çevrimiçi oyunlara daima güvenme gibi olumsuz davranışlara ilişkin farkındalıklarının olduğu görülmektedir.

İzlenebilirliği önleme ($\bar{X}=3,55$; $SS=0,89$) boyutunda ise ortaokul öğrencilerinin çevrimiçi oyunlarda birbirinden farklı giriş şifresi kullanma, güncel antivirüs yazılımı kullanma, lisanslı oyunları tercih etme, güvenilir sitelerden oyunları indirme, gerekli olmayan erişim izinlerini kapatma gibi beceriler açısından iyi oldukları görülmektedir.

Ücret bilgilerini koruma ($\bar{X}=3,38$; $SS=1,19$) alt boyutunda ise ortaokul öğrencilerin güvenilir oyun platformlarına ödeme yapma, güvenilir ödeme yöntemlerini tercih etme, ödeme yapmadan önce platformların güvenilirliğini kontrol etme ve ailesinin bilgisi dahilinde ödeme yapma gibi becerilerde ortalamanın altında ve diğer boyutlara göre daha düşük düzeyde farkındalıklarının olduğu görülmektedir.

Ortaokul Öğrencilerinin Dijital Okuryazarlık Düzeyleri

Araştırma kapsamında ortaokul öğrencilerinin dijital okuryazarlık düzeylerini belirlemek amacıyla uygulanan ölçekten elde edilen veriler analiz edilerek ölçek geneline ve alt boyutlarına ilişkin bulgular Tablo 11’de verilmiştir

Tablo 11. Ortaokul Öğrencilerinin Dijital Okuryazarlık Düzeylerine İlişkin Durumları

	Ortalama ($\bar{X}$)	Standart Sapma (SS)	Minimum	Maximum
Ölçek geneli	3,63	0,65	1,57	5,00
Bilgi-İşlem	3,82	0,76	1,00	5,00
İletişim	3,11	1,03	1,00	5,00
Güvenlik	4,02	0,75	1,00	5,00
Problem Çözme	3,50	0,95	1,00	5,00

Tablo 11’de görüldüğü gibi araştırmaya katılan 1480 ortaokul öğrencisinin dijital okuryazarlık düzeyine ilişkin genel ortalama puanı 3,63 bulunmuştur. Buna göre ortaokul öğrencilerinin dijital okuryazarlık düzeylerinin iyi olduğu görülmektedir. Alt boyutlar açısından incelendiğinde ise ortaokul öğrencilerinin en çok güvenlik ($\bar{X}=4,02$; $SS=0,75$) alt boyutuna ilişkin becerilere, en az ise iletişim ($\bar{X}=3,11$; $SS=1,03$) alt boyutuna ilişkin becerilere sahip olduğu görülmüştür.

Bilgi-işlem ($\bar{X}=3,82$; $SS=0,76$) ve güvenlik ($\bar{X}=4,02$; $SS=0,75$) alt boyutları açısından ortaokul öğrencilerinin çok iyi düzeyde oldukları görülmektedir. Buna göre ortaokul öğrencileri; internette bilgiye ulaşmak için arama motorlarını kullanma, arama yaparken filtreleri kullanma, internette her bilginin güvenilir olmadığını bilme, internetten ulaşılan bilginin güvenilirliğini sağlamak için bilgiyi farklı kaynaklarla karşılaştırabilme, dosya ve içerikleri dijital ortamlara kaydedebilme, dijital araçları kullanırken kuralların farkında olma, internette bilgi paylaşımında bulunabilme ve dijital araçları korumak için şifreler kullanabilme, kimlik bilgilerini internette paylaşmama, dijital teknolojilerin sağlığa olumsuz etkilerini bilme ve teknolojinin çevreye pozitif ve negatif etkilerinin farkında olma gibi olumlu davranışları sergileyebildikleri görülmektedir.

Problem çözme ($\bar{X}=3,50$; $SS=0,95$) alt boyutunda ise öğrencilerin yeni bir durum veya uygulama kullanırken teknik bir problem oluştuğunda destek ve yardım bulabilme, dijital teknolojileri kullanırken ortaya çıkan sorunları çözebilme, dijital teknolojileri kullanmada teknik olmayan problemleri çözebilme, programların veya araçların teknolojik problemlerini çözebilme, teknolojiyle ilgili problemleri çözmek için dijital araçları kullanabilme gibi beceriler açısından iyi oldukları görülmektedir.

İletişim ($\bar{X}=3,11$; $SS=1,03$) alt boyutunda ise öğrencilerin kaydettiği dosya ve içeriklere tekrar ulaşabilme, cep telefonu internet e-posta ve sohbet etme programlarıyla iletişim kurabilme, internet üzerinde resim ve dosya paylaşabilme, sosyal ağları kullanabilme gibi becerilerde ortalamanın altında ve diğer boyutlara göre daha düşük düzeyde oldukları görülmektedir.

Ortaokul Öğrencilerinin Çevrimiçi Mahremiyet Farkındalık Düzeyleri

Araştırma kapsamında ortaokul öğrencilerinin çevrimiçi mahremiyet farkındalık düzeylerini belirlemek amacıyla uygulanan ölçekten elde edilen veriler analiz edilerek ortaokul öğrencilerinin ölçek geneli ve her bir alt boyut açısından genel durumları Tablo 12’de verilmiştir. Ölçekteki olumsuz maddeler anlaşılabilirliği artırmak amacıyla ters çevrilmiş ve ortalamalar buna göre hesaplanmıştır.

Tablo 12. Ortaokul Öğrencilerinin Çevrimiçi Mahremiyet Farkındalık Durumları

	Ortalama ($\bar{X}$)	Standart Sapma (SS)	Minimum	Maximum
Ölçek geneli	3,90	0,81	1,35	5,00
Dikkat Faktörü	3,92	1,00314	1,00	5,00
Güvenlik Faktörü	3,75	1,03070	1,00	5,00
İletişim ve Paylaşım Faktörü	4,05	1,03778	1,00	5,00

Tablo 12’de görüldüğü gibi araştırmaya katılan 1480 ortaokul öğrencisinin çevrimiçi mahremiyet farkındalık ortalama puanı 3,90 bulunmuştur. Buna göre, ortaokul öğrencilerinin çevrimiçi mahremiyet farkındalık düzeylerinin iyi olduğu görülmektedir. Alt boyutlar açısından incelendiğinde ise, ortaokul öğrencilerinin en çok iletişim ve paylaşım ($\bar{X}=4,05$; $SS=1,03$) alt boyutuna ilişkin çevrimiçi mahremiyet farkındalığının olduğu, en az güvenlik ($\bar{X}=3,75$; $SS=1,03$) alt boyutuna ilişkin çevrimiçi mahremiyet farkındalığının olduğu görülmüştür.

İletişim ve paylaşım ($\bar{X}=4,05$; $SS=1,03$) ile dikkat ($\bar{X}=3,92$; $SS=1,00$) alt boyutları açısından ortaokul öğrencilerinin farkındalıklarının yüksek düzeyde olduğu görülmektedir. Buna göre, ortaokul öğrencileri çevrimiçi ortamlarda tanımadığı kişilerle kişisel bilgilerini paylaşma, izinsiz paylaşım yapma, tanımadığı kişileri takip etme veya arkadaş olma, tanımadığı kişilerle iletişim kurma gibi olumsuz davranışları sergilemedikleri belirlenmiştir. Ayrıca dikkat alt boyutu açısından kullandığı çevrimiçi

platformlarda gizlilik ayarlarını kontrol etme, çevrimiçi ortamlarda kullandığı hesapların gizlilik ayarlarını kontrol etme, güçlü şifre oluşturma, güvenilir mesajları anlama, paylaşımlarının korsanlar tarafından kullanılabileceğinin farkında olma gibi mahremiyet açısından pozitif davranışları da sergiledikleri belirlenmiştir.

Güvenlik ($\bar{X} = 3,75$; $SS = 1,03$) alt boyutunda ise öğrencilerin çerez dosyaları hakkında bilgi sahibi olma, mobil cihaz uygulamalarının izin taleplerine dikkat etme, internet sitelerinin ve mobil cihazların güvenlik sertifikaları ve veri şifreleme yöntemlerini kontrol etme ve web tarayıcılarındaki eklentilerin hangi bilgilere erişebileceğinin farkında olma gibi becerilerde ortalamanın altında ve diğer boyutlara göre daha düşük düzeyde oldukları belirlenmiştir.

Ortaokul Öğrencilerinin Çevrimiçi Mahremiyet Farkındalık Düzeyleri ile Dijital Okuryazarlık Düzeylerinin Çevrimiçi Oyunlardaki Siber Güvenlik Farkındalıkları Üzerindeki Etkisi

Ortaokul öğrencilerinin çevrimiçi mahremiyet farkındalık düzeyleri ile dijital okuryazarlık düzeylerinin çevrimiçi oyunlardaki siber güvenlik farkındalıkları üzerindeki etkisini belirlemek için basit ve çoklu doğrusal regresyon analizi yapılmış ve sonuçlar Tablo 13, Tablo 14 ve Tablo 15'te verilmiştir.

Tablo 13. Çevrimiçi Mahremiyet Farkındalığının Çevrimiçi Oyunlardaki Siber Güvenlik Farkındalığını Yordanmasına İlişkin Basit Doğrusal Regresyon Analiz Sonuçları

Değişken	B	Standart Hata B	β	T	P	İkili r	Kısmi r
Sabit	2,658	,065	-	41,107	,000	-	-
Çevrimiçi Mahremiyet Farkındalığı	,328	,016	,466	20,256	,000	,466	,466
Güvenlik Farkındalığı							
R = .466	R ² = .217						
F _(1,147) = 410,289	p < .05						

Tablo 13'te verilen analiz sonuçları incelendiğinde çevrimiçi mahremiyet farkındalığının, çevrimiçi oyunlardaki siber güvenlik farkındalığına pozitif yönlü, anlamlı bir etkisi olduğu görülmektedir ($R = .466$, $R^2 = .217$, $F_{(1,147)} = 410,289$, $p < .01$). Siber güvenlik farkındalığına ilişkin toplam varyansın %21,7'ini çevrimiçi mahremiyet

farkındalığı ile açıkladığı görülmektedir. Regresyon katsayılarının anlamlılığına ilişkin t-testi sonuçları incelendiğinde ise, siber güvenlik farkındalığı üzerinde çevrimiçi mahremiyet farkındalığı değişkeninin anlamlı bir yordayıcılığı olduğu ($p \leq .01$) görülmektedir.

Tablo 14. Dijital Okuryazarlığın Çevrimiçi Oyunlardaki Siber Güvenlik Farkındalığını Yordanmasına İlişkin Basit Doğrusal Regresyon Analiz Sonuçları

[illegible]

Tablo 14’te verilen analiz sonuçları incelendiğinde dijital okuryazarlığın, çevrimiçi oyunlardaki siber güvenlik farkındalığına pozitif yönlü, anlamlı bir etkisi olduğu görülmektedir ($R=.290$, $R^2=.084$, $F_{1,147}=136,107$, $p<.01$). Siber güvenlik farkındalığına ilişkin toplam varyansın %8,4’ini çevrimiçi dijital okuryazarlık ile açıkladığı görülmektedir. Regresyon katsayılarının anlamlılığına ilişkin t-testi sonuçları incelendiğinde ise, siber güvenlik farkındalığı üzerinde dijital okuryazarlık değişkeninin anlamlı bir yordayıcılığı olduğu ($p<.01$) görülmektedir.

Tablo 15. Çevrimiçi Mahremiyet Farkındalığı ve Dijital Okuryazarlık Düzeyinin Çevrimiçi Oyunlardaki Siber Güvenlik Farkındalığını Yordanmasına İlişkin Çoklu Regresyon Analiz Sonuçları

[illegible]

Tablo 15'te görüldüğü gibi gerçekleştirilen çoklu doğrusal regresyon analizi sonucunda ortaokul öğrencilerinin çevrimiçi mahremiyet farkındalığı ve dijital okuryazarlık düzeylerinin çevrimiçi oyunlardaki siber güvenlik farkındalığı üzerinde orta düzeyde, pozitif yönlü ve anlamlı etkisi olduğu görülmüştür ($R=.505$, $R^2=.256$, $p<.01$). Çevrimiçi mahremiyet farkındalığı ve dijital okuryazarlık düzeyi birlikte, çevrimiçi oyunlardaki siber güvenlik farkındalığının toplam varyansın %25'ini açıklamaktadır.

Standardize edilmiş regresyon katsayısına göre (β), yordayıcı değişkenlerin siber güvenlik farkındalığı üzerindeki göreceli önem sırası; çevrimiçi mahremiyet farkındalığı ($\beta=.423$) ve dijital okuryazarlık ($\beta=.200$) olduğu görülmektedir. Buna göre, çevrimiçi oyunlardaki siber güvenlik farkındalığı üzerinde çevrimiçi mahremiyet farkındalığı dijital okuryazarlığa göre daha önemlidir. Regresyon katsayılarının anlamlılığına ilişkin t-testi sonuçları incelendiğinde ise, çevrimiçi oyunlardaki siber güvenlik farkındalığı üzerinde çevrimiçi mahremiyet farkındalığı ve dijital okuryazarlık düzeyinin anlamlı bir yordayıcılığı olduğu ($p<.01$) görülmektedir. Buna göre, dijital okuryazarlık ve çevrimiçi mahremiyet farkındalığı becerileri değişkenleri regresyon modeline sokulduğunda çevrimiçi oyunlardaki siber güvenlik farkındalığını açıklamada her iki değişkenin anlamlı katkısının olduğu, çevrimiçi mahremiyet farkındalığıyla birlikte dijital okuryazarlık becerilerinin bir arada artırılmasının çevrimiçi oyunlardaki siber güvenlik farkındalığının artmasına olumlu etkisinin olduğu görülmektedir.

BÖLÜM V

TARTIŞMA

Araştırmanın amacı, ortaokul öğrencilerinin dijital kimlik mahremiyeti ile teknoloji okuryazarlık düzeylerinin siber güvenlik farkındalıkları üzerindeki etkisinin araştırılmasıdır. Ayrıca araştırma kapsamında ortaokul öğrencilerinin çevrimiçi oyunlardaki davranışları, siber güvenlik farkındalığı, çevrimiçi mahremiyet durumları ve dijital okuryazarlık düzeyi incelenmiştir. Araştırma sonucunda öncelikle ortaokul öğrencilerinin çevrimiçi oyunlarda siber güvenlik farkındalıklarının, çevrimiçi mahremiyet farkındalığının ve dijital okuryazarlık durumlarının yüksek olduğu görülmüştür.

Alanyazında bu konuda benzer ve farklı sonuçlar yer almaktadır. Örneğin; Karacı, Akyüz ve Bilgici (2017) üniversite öğrencilerine yönelik olarak yapmış oldukları çalışmada öğrencileri eğitim kademeleri cinsiyet lise türleri ve internet kullanım yılı gibi çeşitli değişkenlere göre siber güvenlik davranışı açısından inceleyerek öğrencilerin siber güvenliğe yönelik farkındalıklarının yeterli düzeyde olduğunu tespit etmişlerdir. Yapmış oldukları çalışmada alt boyutlardan kişisel gizliliğe karşı öğrencilerin farkındalık düzeylerinin iyi olduğunu belirtmişlerdir. Yanı sıra yine alt faktörlerden ücret bilgilerinin korunması noktasında da öğrencilerin farkındalık düzeyinin iyi olduğu sonucuna varmışlardır. Bu durum araştırma kapsamında geliştirilen siber güvenlik ölçeğinin gizlilik ve ücret bilgilerini koruma alt faktörleriyle benzer bir sonucun tespit edildiğini göstermektedir. Ayrıca araştırma bulgularında erkek öğrencilerin kız öğrencilere göre daha fazla siber güvenlik farkındalık düzeyi gösterdikleri belirlenmiştir.

Gülseçen (2021) tarafından yapılmış olan başka bir çalışmada ise Kocaeli ili Körfez ilçesindeki Millî Eğitim Bakanlığı'na bağlı ortaokullarda eğitim görmekte olan 7 ve 8. sınıf öğrencilerinden toplam 2831 ortaokul öğrencisinin siber güvenlik farkındalık düzeyinin orta seviyede olduğu sonucuna varılmıştır. Araştırmanın alt faktörleri açısından bakıldığında ortaokul öğrencilerinin gizliliği koruma ve ödeme bilgilerini koruma alt boyutlarında düşük düzeyde siber güvenlik farkındalığı göstermiş oldukları tespit edilmiştir.

Zahri, Susanty ve Mustaffa (2017) tarafından Malezya’da 10-12 yaş arası ortaokul seviyesindeki öğrencilere yönelik yapılan araştırmada, öğrencilerin siber güvenlik farkındalık düzeyinin orta düzeyde olduğu tespit edilmiştir. Yine Malezya’da Al-Jerbie ve Jali (2014) tarafından 952 ortaokul öğrencisine yönelik yapılan araştırmada, ortaokul öğrencilerinin siber güvenlik hazırbulunuşluk düzeyi dikkate alınarak yapılan ön çalışmada öğrencilerin siber güvenlik konusunda düşük düzeyde bir farkındalık gösterdikleri tespit edilmiştir.

Tirumala, Sarrafzadeh ve Pang (2016)’da Yeni Zelanda da 8-12 yaş gurubundaki öğrenciler üzerinde yaptıkları çalışmada öğrencilerin siber güvenlik farkındalık düzeylerinin düşük düzeyde olduğu görülmüştür. Ayrıca öğrencilerin siber güvenlik konularındaki terimlere de yabancı olduğu ve konunun önemi hakkında bilgi sahibi olmadıkları tespit edilmiştir. Alotaibi ve diğerlerinin (2016) Suudi Arabistan’daki 18 yaş üzeri 629 yetişkin birey üzerinde yapmış oldukları çalışmada ise siber güvenlik farkındalıklarının düşük düzeyde olduğu tespit edilmiştir.

Yılmaz, Karaoğlu Yılmaz, Öztürk ve Karademir (2017) tarafından Bartın il merkezindeki 2029 lise düzeyindeki öğrenciye yönelik yapılan bir başka çalışmada öğrencilerin büyük bölümünün siber güvenlik farkındalık düzeyinin yeterli seviyede olmadığı ve çevrimiçi risklerle karşılaşabilecekleri tespit edilmiştir. Bu durum ortaokul ve lise öğrencilerinin siber güvenlik farkındalık düzeylerinin düşük olduğunu göstermektedir. Buna göre, ortaokul ve lise düzeyinde verilen siber güvenlik farkındalık eğitim ve uygulamalarının yeterli düzeyde olmadığını söylenebilir.

Aslan (2019) ise lise öğrencileri üzerinde yapmış olduğu bir diğer çalışmada öğrencilerin siber güvenlik farkındalık düzeylerinin orta seviyede olduğunu tespit etmişlerdir. Araştırma alt boyutları açısından bakıldığında kişisel gizlilik alt boyutunun yüksek düzeyde olduğu ancak ödeme bilgilerini koruma boyutunda orta düzeyde oldukları belirlenmiştir.

Gharie (2021) tarafından yaklaşık 6206 kız öğrenciye yönelik olarak yapılan siber güvenlik farkındalığı çalışmasında, öğrencilerin siber güvenlik konusunda yeterli bilgiye sahip olmadığı ve siber güvenlik farkındalık düzeyinin düşük olduğu tespit edilmiştir.

Araştırmada ortaokul öğrencilerinin internette günlük ortalama 2 saate yakın vakit geçirdiği tespit edilmiştir. Bununla ilgili olarak ortaokul öğrencilerine yöneltilen günlük internet kullanım süresi sorusuna öğrenciler, 1-2 saat cevabını vermiştir. Alanyazında bu durumla ilgili benzer bir çalışmanın ise Çelen, Çelik ve Seferoğlu (2011) tarafından yapıldığı ve çalışma sonucunda çocukların günlük internet kullanımına 10 yaşında başladıkları, günlük internet kullanımı süresinin 1-1,5 saat arasında olduğu ve çocukların interneti yüksek (%49) oranda oyun oynamak için kullandıkları tespit edilmiştir. İki çalışma arasındaki süreye bakıldığında çocuklarda günlük ortalama internet kullanım süresinin değişmediği görülmektedir. Çelen, Çelik ve Seferoğlu (2011) tarafından yapılan diğer bir çalışmada 9-16 yaş arası çocukların internet kullanım süresinin 1,5 saat olduğu, Mıhçı Türker ve Kılıç Çakmak (2019) tarafından yaklaşık 6800 öğrenciye yapılan araştırmada, araştırmaya katılan öğrencilerin yarısı 30 dk. ile 2 saat arasında günlük internet kullandıkları ifade edilmektedir. Taştekin (2019) ise 30 kişilik oyun bağımlısı ortaokul öğrencisiyle yapmış olduğu araştırmada, öğrencilerin günlük ortalama 3,5 saat internet kullandıkları tespit edilmiştir. Oyun bağımlıları üzerinde gerçekleştirilen alanyazındaki çalışmalar bir bütün olarak ele alındığında, öğrencilerin günlük internet kullanım sürelerinin araştırma bulgularıyla benzer şekilde yüksek olduğu görülmektedir.

Araştırmada ortaokul öğrencilerinin çevrimiçi oyunları en çok cep telefonu platformu üzerinde oynadıkları belirlenmiştir. Benzer olarak Taştekin (2019) tarafından yapılan çalışmada öğrencilerin yüksek oranda cep telefonundan oyun oynadıkları ifade edilmiştir. Karaman ve Yaşar (2019) tarafından yapılan bir diğer çalışmada da 43 ortaokul öğrencisinin en çok akıllı telefon üzerinden oyun oynadıkları belirlenmiştir. Benzer şekilde Aslan (2019) tarafından meslek lisesi öğrencileriyle yapılan çalışmada öğrencilerin çevrimiçi oyunları en çok akıllı telefon üzerinden oynadıkları bulunmuştur. Buna göre, alanyazında yapılan diğer çalışmalarda elde edilen bulgular araştırma bulgularıyla örtüşmektedir. Bu durum çevrimiçi oyun oynamak için farklı kademedeki öğrencilerin oyun oynama platformu olarak en çok akıllı telefon kullanıldığını göstermektedir.

Araştırmadan elde edilen sonuca göre araştırmaya katılan 1480 ortaokul öğrencisinin çevrimiçi mahremiyet farkındalık ortalama puanı 3,90 bulunmuştur. Buna göre, ortaokul öğrencilerinin çevrimiçi mahremiyet farkındalık düzeylerinin iyi olduğu görülmektedir. Elde edilen araştırma sonucuna göre alanyazında da benzer ve farklı

sonuçlara ulaşılmıştır. Örneğin; Töngel (2019) tarafından Amasya ve Ordu üniversitelerinde öğrenim gören toplam 608 üniversite öğrencisine yönelik yapılan ve gerçekleştirilen araştırmayla aynı ölçeğin kullanıldığı araştırmada üniversite öğrencilerinin mahremiyet farkındalık ortalama puanı 3,98 olduğu belirlenmiştir. Bu durumda iki farklı eğitim kademesindeki öğrencilerin çevrimiçi mahremiyet farkındalık düzeyi yakın bir sonuç gösterdiği görülmektedir. Sığın (2019) tarafından lise ve üniversite öğrencilerine yönelik sosyal medya kullanan gençlerin mahremiyet algılarına yönelik yapılan araştırmada ise, lise öğrencilerinin mahremiyet algısı ve farkındalığının üniversite öğrencilerine göre daha düşük olduğu tespit edilmiştir. Kaya (2019) tarafından 150 üniversite öğrencisine yapılan bir başka çalışmada ise, sınıf değişkenine göre belirlenen çevrimiçi mahremiyet algısı düzeyinin anlamlı bir şekilde farklılaştığı belirlenmiştir. Yapılan çalışmada üniversite birinci sınıf öğrencilerinin çevrimiçi mahremiyet algısı düzeyinin üst sınıflardaki öğrencilere oranla daha yüksek olduğu belirlenmiştir. Bu durum ortaokul düzeyinden lise ve üniversiteye geçişte çevrimiçi mahremiyet durumuna olan algıda azalma olduğu şeklinde yorumlanabilir. Akçalar (2020) tarafından farklı iş kollarında çalışan ve eğitim durumlarına göre yapılan araştırmada, dijital mahremiyet farkındalığı en yüksek olan bireylerin yüksek lisans mezunu olduğu belirlenmiştir. Yüksek lisans mezunlarını ise lise mezunları takip etmektedir. Lorenz, Sousa ve Tomberg (2012) tarafından üniversite öğrencilerine yönelik yapılan araştırmada ise, internet ortamında birçok fazla alanda sosyalleşen öğrencilerin diğer öğrencilere oranla potansiyel çevrimiçi mahremiyet tehditlerinin daha bilincinde oldukları tespit edilmiş ve öğrencilerin özel ve eğitsel etkileşimler arasında ayırım yapamadıkları sonucuna varmıştır. Weinberger, Bouhnik ve Zhitomirsky-Geffet (2017) tarafından İsrail'deki farklı alanlarda öğrenim gören 169 öğrenciyle yapılan çalışmada, katılımcıların mahremiyet kaygısı ve çevrimiçi mahremiyet özyeterliği arttıkça mahremiyet paradoksu davranışına yönelik eğilimlerinin azaldığı tespit edilmiştir.

Ayrıca gerçekleştirilen araştırma ortaokul öğrencilerinin çevrimiçi mahremiyet düzeylerinin siber güvenlik farkındalığı ve dijital okuryazarlık düzeyiyle pozitif yönde anlamlı bir ilişkisinin olduğunu da göstermiştir. Bu sonuç alanyazındaki benzer çalışmaların bulgularıyla örtüşmektedir. Örneğin, Mıhçı (2016) tarafından ortaokul öğrencilerinin çevrimiçi mahremiyet farkındalığını tespit etmek amacıyla yapılan çalışmada ortaokul öğrencilerinin çevrimiçi mahremiyet farkındalık düzeyinin yüksek olduğu tespit edilmiştir. Töngel ve Mehmet (2021) ise, üniversite öğrencileri üzerinde

gerçekleştirdikleri araştırma sonuçlarına göre öğrencilerde çevrimiçi mahremiyet farkındalığının yüksek olduğunu ayrıca dijital okuryazarlık ve çevrimiçi mahremiyet arasında anlamlı bir ilişkinin olduğunu ifade etmişlerdir. Okumuş ve Atılgan (2021) üniversite öğrencileri üzerinde gerçekleştirdikleri çalışmada dijital okuryazarlık düzeyi ile dijital mahremiyet kaygısı arasında pozitif yönlü ve doğrusal bir ilişki olduğunu tespit etmişlerdir. Alanyazında araştırma bulgularıyla farklı araştırmalar da bulunmaktadır. Örneğin, Akar ve Akar (2021) tarafından üniversite öğrencileri üzerinde gerçekleştirilen çalışmada öğrencilerin sosyalleşmek ve çevresinde kabul edilmek için ortaokul ve lisans düzeyindeki mahremiyet algısına ters paylaşım ve davranışlar gösterdiklerini ve bu durumun çevrimiçi platforma göre mahremiyet algısında farklı davranışlara neden olabileceğini belirtmişlerdir.

Araştırmada elde edilen sonuçlardan bir diğeri de çevrimiçi oyun oynayan 1480 ortaokul öğrencisinin dijital okuryazarlık düzeyine ilişkin genel ortalama puanı 3,63 bulunmuştur. Buna göre ortaokul öğrencilerinin dijital okuryazarlık düzeylerinin iyi olduğu görülmektedir. Dijital okuryazarlık ölçeğinin alt boyutlarına bakıldığında bilgi işlem alt boyutunda ortalamanın 3,82 olduğu, problem çözme alt boyutunun 3,50 olduğu, iletişim boyutunun 3,50 olduğu ve son olarak güvenlik alt boyutunun ise 4,02 olduğu tespit edilmiştir. Elde edilen araştırma sonucuna göre literatürde de benzer ve farklı sonuçlara ulaşılmıştır. Çelik (2021) tarafından yapılan Gaziantep ilinde öğrenim gören ortaokul kademesindeki 5, 6, 7 ve 8. sınıflardaki toplam 632 öğrenciyle gerçekleştirilen araştırma sonucuna göre ortaokul öğrencilerinin dijital okuryazarlık düzeyine ilişkin genel ortalama puanının 3,12 olduğu görülmektedir. Dijital okuryazarlık ölçeğinin alt boyutlarına bakıldığında, bilgi işlem alt boyutunda ortalamanın 3,28 olduğu, problem çözme alt boyutunun 2,95 olduğu, iletişim boyutunun 2,49 olduğu ve son olarak güvenlik alt boyutunun ise 3,64 olduğunu tespit etmişlerdir. Yine benzer bir çalışma Zurnacı (2019) tarafından Doğu Anadolu'nun bir ilçesinde ortaokulda öğrenim gören 8. sınıf öğrencileri üzerinde gerçekleştirilmiştir. Araştırma kapsamında toplam 24 öğrenci üzerine yapılan çalışmada öğrencilerin dijital okuryazarlık düzeyinin oldukça düşük olduğunu tespit etmiştir. Araştırma kapsamındaki öğrencilere uygulanan eğitimler sonucunda öğrencilerin dijital okuryazarlık düzeyinde pozitif yönde anlamlı bir değişim olduğunu ifade etmiştir. Bayrakçı (2020) ise, farklı eğitim kademelerinde gerçekleştirdiği çalışmada yüksek lisans öğrencilerinin lisans öğrencilerine kıyasla daha yüksek dijital okuryazarlık ortalama puanına sahip olduğu ayrıca ilköğretim ve ortaokul mezunlarının diğer

eğitim durumlarına kıyasla dijital okuryazarlık ortalama puanı bakımından daha düşük seviyede olduğu sonucuna varmıştır. Bir başka araştırma ise Kaya (2020) tarafından Konya ili Selçuklu ilçesinde devlet okulunda öğrenim gören 847 ortaöğretim öğrencileri üzerinde gerçekleştirilmiştir. Araştırma sonucunda ortaöğretim öğrencilerinin dijital okuryazarlık düzeyinin yüksek olduğu sonucuna ulaşmıştır. Benzer şekilde Öztürk (2020) tarafından Kırıkkale ilinde öğrenimine devam eden 500 farklı lise türündeki lise öğrencisine yönelik yapılan çalışmada öğrencilerin dijital okuryazarlık düzeyinin çok yeterli olduğu belirlenmiştir. Bağçecik (2021) tarafından lise 9 ve 10. sınıflarda okuyan toplam 17.574 öğrenciyle gerçekleştirilen çalışmada ise, öğrencilerin dijital okuryazarlık düzeylerinin oldukça yüksek olduğu sonucuna ulaşmıştır. Benzer şekilde Yaşar (2019) tarafından eğitim fakültesinde öğrenim görmekte olan 16 öğretmen adayı üniversite öğrencisi üzerinde gerçekleştirilen çalışmadan elde edilen sonuçlara bakıldığında öğretmen adaylarının dijital okuryazarlık düzeyinin yeterli düzeyde olduğunu tespit etmiştir. Yeşildal (2018) tarafından 18 yaş üzeri toplam 500 yetişkin bireye yönelik yapılan çalışmada bireylerin dijital okuryazarlık düzeylerinin iyi olduğu sonucuna ulaşmıştır. Tekeli (2018) tarafından gerçekleştirilen huzur evinde ikamet eden 65 yaş üzeri toplam sekiz bireye yönelik yapılan çalışmada ise, bireylerin temel düzeyde dijital okuryazarlık becerisine sahip olduğu sonucuna ulaşılmıştır. Alanyazındaki çalışmaların sonuçları genel olarak incelendiğinde öğrencilerin ve bireylerin kullanım alanlarına göre dijital okuryazarlık düzeylerinin farklılık gösterdiği görülmektedir. Teknolojinin her geçen gün hayatın içine daha çok yerleşmiş olması nedeniyle küçük yaş gurubunun daha spesifik konularda dijital okuryazarlık düzeyinin daha yüksek olduğunu göstermektedir. Okullardaki ders ortamındaki teknoloji kullanımı ve teknolojiye kolay ulaşım bu durumun başlıca nedeni olarak gösterilebilir.

Ayrıca araştırmada dijital okuryazarlık düzeyi ile siber güvenlik farkındalığı arasında pozitif yönlü anlamlı bir ilişkinin olduğu tespit edilmiştir. Alanyazında bu bulguyla benzer çalışmalar bulunmaktadır. Örneğin, Töngel ve Mehmet (2021) üniversite öğrencilerine yönelik olarak yapmış oldukları çalışmada dijital okuryazarlık düzeyinin lisans öğrencilerinde ortalamanın üzerinde olduğunu tespit etmişlerdir. Benzer şekilde Üstündağ, Güneş ve Bahçıvan (2017), fen bilgisi öğretmenliği bölümünde okuyan lisans öğrencilerine yönelik olarak yaptıkları çalışmada dijital okuryazarlık düzeyinin iyi olduğunu tespit etmişlerdir. Göldağ (2021) tarafından İnönü üniversitesinde 265 lisans öğrencisi ile yapılan bir diğer çalışmada ise, öğrencilerin dijital okuryazarlık düzeyi ile

dijital veri güvenliği arasındaki ilişki incelenmiş ve bu değişkenlerin birbiriyle yüksek düzeyde pozitif yönlü anlamlı bir ilişki olduğu tespit edilmiştir. Buna göre öğrencilerin dijital okuryazarlık düzeyi arttıkça dijital veri güvenliği farkındalığının da arttığı görülmüştür. Dönmez (2019) lise öğrencilerine yönelik bilgi güvenliği farkındalığı ve dijital okuryazarlık düzeyi arasındaki ilişkiye yönelik yapmış olduğu çalışmada öğrencilerin dijital okuryazarlık düzeyi ile bilgi güvenliği arasında pozitif yönlü anlamlı bir ilişkinin olduğunu tespit etmişlerdir.

Gerçekleştirilen araştırma kapsamında geliştirilen ölçeğin alt boyutlarında bilgi güvenliği farkındalığı ve dijital okuryazarlık düzeyinin mahremiyet alt boyutu ile ilişkisinin en fazla olduğunu tespit etmiştir. Bu bulgu Talan ve Aktürk (2021) tarafından gerçekleştirilen araştırma bulgusuyla benzerdir. Talan ve Aktürk (2021), lise öğrencilerine yönelik bilgi güvenliği ile dijital okuryazarlık düzeyi arasındaki ilişkiyi incelemek için yaptıkları çalışmada iki değişken arasında pozitif yönlü bir ilişki olduğunu tespit etmişlerdir. Buna göre, dijital okuryazarlık düzeyi arttıkça bilgi güvenliği farkındalığının da arttığı sonucu görülmektedir.

Derin ve Gençoğlu (2020) tarafından ortaokul öğrencilerine yönelik olarak bilgi güvenliği farkındalığını tespit etmek amacıyla yapılan çalışmada ise, öğrencilerin bilgi güvenliği konusunda almış oldukları eğitimin yetersiz olduğu, öğrencilerin hazırbulunuşluk düzeyinin düşük olduğu ifade edilmektedir. Alanyazında yapılan çalışmalar, farklı kademelerdeki öğrencilerin dijital okuryazarlık düzeyine göre bilgi güvenliği farkındalığı olduğunu göstermektedir. Bu durum öğrencilerde yeterli siber güvenlik farkındalığı oluşturmak için dijital okuryazarlık düzeyinin de orantılı olarak artırılması sonucunu ortaya koymaktadır.

BÖLÜM VI

SONUÇ VE ÖNERİLER

Sonuç

Sonuç olarak teknoloji ve çevrimiçi oyunların, hayatın her noktasındaki hızlı gelişimini görmezden gelmek mümkün değildir. Oyun, bireylerin yaşamlarının her aşamasında olan bir olgudur. Teknoloji ve bilgi çağı olarak adlandırılan günümüzde çocukların çevrimiçi oyunlara olan ilgisi her geçen gün artmaktadır. Bu ilgi, çevrimiçi oyunlarda belirli sınırlar içinde ortaokul öğrencilerinin kendilerini tehlikeye atan durumlardan korunmasını zorunlu hale getirmiştir. Dijital dünya, sınırları olmayan, güvenilirliğin her geçen gün tartışıldığı bir mecra olmuştur. Bu çalışmada ortaokul öğrencilerinin dijital okuryazarlık düzeyleri ile çevrimiçi mahremiyet farkındalığı durumunun çevrimiçi oyunlardaki siber güvenlik farkındalığına etkisinin belirlenmesi hedeflenmiştir. Bu çerçevede araştırmada beş alt sorunun cevabı aranarak ortaokul öğrencilerinin çevrimiçi oyunlardaki genel durumları, dijital okuryazarlık düzeyleri, çevrimiçi mahremiyet farkındalıkları, çevrimiçi oyunlardaki siber güvenlik farkındalıkları ve çevrimiçi oyunlardaki siber güvenlik farkındalığını dijital okuryazarlık düzeyi ile çevrimiçi mahremiyet farkındalığının ne kadar yordadığı incelenmiştir. Buna göre araştırma sonucunda ulaşılan sonuçlar şunlardır;

- Ortaokul öğrencilerinin çevrimiçi oyunlardaki alışkanlıkları için çok fazla para harcamadıkları, günlük bir iki saat çevrimiçi oyun oynadıkları, çevrimiçi oyun oynama platformu olarak en çok cep telefonunun kullanıldığı, çevrimiçi oyun oynamak için 2 ile 4 kişilik takımlar halinde oyun oynandığı, 55 farklı çevrimiçi oyun içerisinde en çok PUBG oyununun oynandığı, çevrimiçi oyun oynama ortamı olarak ortaokul öğrencilerinin daha çok ev ortamını kullandıkları ve çevrimiçi oyun oynama türleri içerisinde en çok macera oyununu oynadıkları sonucuna ulaşılmıştır.
- Ortaokul öğrencilerinin çevrimiçi oyunlara yönelik siber güvenlik farkındalık düzeyinin iyi düzeyde olduğu ve siber güvenlik durumlarına karşı farkındalıklarının olduğu sonucu elde edilmiştir.

- Ortaokul öğrencilerinin dijital okur yazarlık düzeyinin iyi düzeyde olduğu ve diğer değişkenlere göre nispeten biraz düşük düzeyde kaldığı sonucu elde edilmiştir.
- Ortaokul öğrencilerinin çevrimiçi oyun ortamlarındaki mahremiyet farkındalığını ve mahremiyet konusundaki ön bilgisini tespit etmek için çevrimiçi mahremiyet farkındalığı ölçeği uygulanmış ve ortaokul öğrencilerinin çevrimiçi mahremiyet farkındalık düzeyinin iyi düzeyde olduğu sonucuna varılmıştır.
- Son olarak çevrimiçi oyunlardaki siber güvenlik farkındalığı değişkenine, dijital okuryazarlık düzeyi ve çevrimiçi mahremiyet farkındalığı değişkenlerinin ayrı ayrı ve birlikte etkisi incelenmiştir. Buna göre, çevrimiçi oyunlardaki siber güvenlik farkındalığı üzerinde dijital okuryazarlık değişkeninin ve çevrimiçi mahremiyet farkındalığının ayrı ayrı anlamlı bir yordayıcı olduğu sonucu elde edilmiştir. Her iki değişken birlikte ele alındığında ise, çevrimiçi oyunlardaki siber güvenlik farkındalığı üzerinde dijital okuryazarlık değişkeni ile çevrimiçi mahremiyet farkındalığı değişkeninin birlikte anlamlı bir yordayıcılığının olduğu sonucuna ulaşılmıştır. Sonuç olarak dijital okuryazarlık ve çevrimiçi mahremiyet farkındalığının çevrimiçi oyunlardaki siber güvenlik farkındalığı üzerinde etkisinin olduğu ve iki değişken bir arada ele alındığında çevrimiçi mahremiyet farkındalığının dijital okuryazarlık düzeyine göre daha çok çevrimiçi oyunlardaki siber güvenlik farkındalığına etki ettiği sonucuna ulaşılmıştır.

Öneriler

Araştırma sonuçlarından elde edilen bulgular doğrultusunda uygulamaya ve ileride yapılacak araştırmalara yönelik aşağıdaki önerilerde bulunulmuştur.

Uygulamaya Yönelik Öneriler

- Araştırma çalışmasında ortaokul öğrencilerinin dijital okuryazarlık düzeyleri, çevrimiçi mahremiyet farkındalığı ve siber güvenlik farkındalığına göre daha düşük bir seviyede olduğu tespit edilmiştir. Bu nedenle ortaokul öğrencilerinin

5 ve 6. sınıf Bilişim Teknolojileri ve Yazılım dersinde dijital okuryazarlık becerilerini geliştirecek daha çok etkinliğe yer verilebilir.

- Gerçekleştirilen çalışmada ortaokul öğrencilerinin siber güvenlik farkındalık düzeylerinin iyi seviyede olduğu tespit edilmiştir. Ancak günümüzde teknoloji ve yazılımın gelişim hızı göz önünde alınarak öğrencilerin siber güvenlik farkındalık düzeylerini korumak veya mükemmel bir seviyeye çıkarmak için okul dışında veli bilinçlendirilmesi yönünde de eğitimler, seminerler veya konferans gibi etkinlikler düzenlenebilir.
- Ortaokul öğrencilerinin çevrimiçi oyunları en çok cep telefonu kullanarak oynadıkları yapılan çalışmada tespit edilmiştir. Bu durum Chiong ve Shuler (2010) tarafından ‘ver eline’ etkisi olarak ifade edilen, öğrencilerin cep telefonunda çevrimiçi oyunları g n birlik aktive olarak g rmediklerini desteklemektedir. Bu nedenle  ocukların bu mecrada neler yaptıklarına ve kendilerini nasıl koruduklarına dikkat  ekmek i in ailelerin daha hassasiyet g stermelerini sa layacak politikalar geli tirilebilir.
- Ortaokul öğrencilerinin çevrimi i oyunlarda oynadıkları oyunlar i erisinde Metin 2 ve Mavi Balina gibi yasaklı oyunların oldu u tespit edilmi tir. Bu nedenle her ge en yıl b y k bir b y me g steren dijital oyun i eriklerinin barındırdı ı riskleri ve zararları konusunda bilin lenmenin artırılaca ı ve   rencilerin yasaklı olarak kabul edilen oyunları oynamamaları i in gerekli  nlemlerin alınaca ı politikalar  retiler.
-   rencilerin haftada iki saatten fazla oyun oynadıkları ara tırma sonucunda belirlenmi tir. Bu durumun e itimin her yerde ve her zaman sa lanması i in ders i eriklerinin  e itlendirilerek  oklu zek  kuramını destekleyecek bi imde  evrimi i oyunların   retim s recinde yaygınla tırılması sa lanabilir.

Ara tırmacılara Y nelik  neriler

- Ara tırmada  evrimi i oyunlardaki siber güvenlik farkındalı ı  evrimi i mahremiyet farkındalı ı ve dijital okuryazarlık de i kenleriyle birlikte ele alınmı tır. Yapılacak nicel  alı malarda akademik ba arı, ekonomik durum gibi  e itli de i kenlerle  evrimi i oyunlardaki siber güvenlik farkındalı ı becerisi arasındaki ili kiler incelenebilir.

- Teknoloji kullanım yaşının anaokulu seviyesine düştüğü göz önüne alınarak ilkokul ve okulöncesi dönemdeki çocukların çevrimiçi oyunlardaki siber güvenlik farkındalıklarını inceleyecek araştırmalar yapılabilir.
- Bu araştırmada sadece Tokat ili ve çevresinde öğrenim gören ortaokul öğrencilerinin çevrimiçi oyunlardaki siber güvenlik farkındalık durumları ele alınmıştır. Daha geniş perspektifte konunun incelenmesi için daha geniş bir örneklem grubundaki öğrencilerin çevrimiçi oyunlardaki siber güvenlik farkındalık durumları araştırılabilir.
- Ortaokul öğrencilerinin çevrimiçi oyunlarda karşılaştıkları güvenlik sorunlarının neler olduğunu anlayabilmek için daha küçük bir çalışma grubunda nitel bir araştırma desenlenebilir.
- Araştırmada geliştirilen çevrimiçi oyunlara yönelik siber güvenlik farkındalığı ölçeğinin farklı eğitim kademelerinde de uygulanarak, ölçeğin farklı yaş kademelerinde de geçerlilik ve güvenirliği araştırmacılar tarafından test edilebilir.

KAYNAKÇA

- Akar, H. ve Akar, F. (2021). Sosyal medyada mahremiyet algısı: Üniversite öğrencileri araştırması. *İnönü Üniversitesi İletişim Fakültesi Elektronik Dergisi (İNİF E-Dergi)*, 6(1), 285-297. <https://doi.org/10.47107/inife-dergi.886334>
- Akçalar, A. (2020). *Dijital Mahremiyet: 21. Yüzyıl Bilgi Profesyonellerinin Yetkinlikleri*. Yayınlanmamış yüksek lisans tezi, Marmara Üniversitesi Türkiyat Araştırmaları Enstitüsü, İstanbul.
- Aksoy, A. B. (2019). Erken çocukluk döneminde oyun ve oyunun gelişimsel katkıları. A.B. Aksoy ve H. Dere Çiftçi (Eds.) *Erken Dönemde Oyun* içinde (s. 2-19). Ankara: Pegem Akademi.
- Al-Jerbie, S. I. ve Jali, M. Z. (2014). *A second look at the information security awareness among secondary school students*. The International Conference on Information Security and Cyber Forensics’de sunuldu, Kuala Terengganu, Malezya.
- Alotaibi, F., Furnell, S., Stengel, I. ve Papadaki, M. (2016, Kasım). *A survey of cyber-security awareness in Saudi Arabia*. 11th International Conference for Internet Technology and Secured Transactions, IEEE’ de sunuldu, Barcelona, Spain.
- Altun, R. (2014). *Belirli kısıtlara göre bilgi güvenliği ihlallerinin tespiti*. Yayınlanmamış yüksek lisans tezi, Beykent Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.
- Altunay, D. (2004). *Oyunla desteklenmiş matematik öğretiminin öğrenci erişimine ve kalıcılığa etkisi*. Yayınlanmamış yüksek lisans tezi, Gazi Üniversitesi, Eğitim Bilimleri Enstitüsü, Ankara.
- Aslan, S. (2019). *Bilişim teknolojileri alanındaki meslek lisesi öğrencilerinin siber güvenliğe yönelik bilgi düzeylerinin belirlenmesi*. Yayınlanmamış yüksek lisans tezi, Necmettin Erbakan Üniversitesi Eğitim Bilimleri Enstitüsü, Konya.
- Bağçecik, M. Ç. (2021). *Pandemi Sürecinde Lise Öğrencilerinin Çevrim İçi Teknolojilere Yönelik Öz Yeterlik Algıları ve Dijital Okuryazarlık Düzeylerinin Akademik Başarıya Etkisi*. Yayınlanmamış yüksek lisans tezi, Gazi Üniversitesi Eğitim Bilimleri Enstitüsü, Ankara.

- Bakar, A., Tüzün, H. ve Çağıltay, K. (2008). Öğrencilerin eğitsel bilgisayar oyunu kullanımına ilişkin görüşleri: sosyal bilgiler dersi örneği, *Hacettepe Üniversitesi Eğitim Fakültesi Dergisi (H. U. Journal of Education)*, 35, 27-37.
- Bayırtepe, E. ve Tüzün, H. (2007). Oyun-tabanlı öğrenme ortamlarının öğrencilerin bilgisayar dersindeki başarıları ve öz-yeterlik algıları üzerine etkileri. *Hacettepe Üniversitesi Eğitim Fakültesi Dergisi*, 33(33), 41-54.
- Bayrakçı, S. (2020). *Dijital Yetkinlikler Bütünü Olarak Dijital Okuryazarlık: Ölçek Geliştirme Çalışması*. Yayımlanmamış doktora tezi, Marmara Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.
- Bilgi Teknolojileri ve İletişim Kurumu. (2018). 1 Milyarın üzerinde insan dijital oyun oynuyor. <https://www.btk.gov.tr/haberler/1-milyarin-uzerinde-insan-dijital-oyun-oynuyor> adresinden alınmıştır.
- Bolstad, R. (2004). The role and potential of ICT in early childhood education: a review of New Zealand and international literature, Wellington: New Zealand Council for Educational Research. <https://www.nzcer.org.nz/system/files/ictinecefinal.pdf> adresinden alınmıştır.
- Büyükbaykal, C. I. ve Cansabuncu, İ. A. (2020). Türkiye’de yeni medya ortamı ve dijital oyun olgusu. *Yeni Medya Elektronik Dergisi*, 4(1), 1-9. DOI: 10.17932/IAU.EJN M.2548020 0.2020.4/1.1-9
- Büyüköztürk, Ş., Kılıç Çakmak, E., Akgün Ö. E., Karadeniz, Ş. ve Demirel, F. (2019). *Eğitimde bilimsel araştırma yöntemleri*. Ankara: Pegem Akademi
- Canbek, G. ve Sağıroğlu, Ş. (2006). Bilgi, bilgi güvenliği ve süreçleri üzerine bir inceleme. *Politeknik Dergisi*, 9(3), 165-174. DOI: 10.2339/2006.9.3.165-174
- Canbek, G. ve Sarıoğlu, Ş. (2007). Çocukların ve gençlerin bilgisayar ve internet güvenliği. *Politeknik Dergisi*, 10(1), 33-39. DOI: 10.2339/2007.10.1.33-39.
- Chen, Y. C., Chen, P., Song, R. ve Korba, L. (2004, Ekim). *Online gaming crime and security issue: Cases and countermeasures from Taiwan*. 2nd Annual Conference on Privacy, Security and Trust’de sunuldu, New Brunswick, Canada.

- Chiong, C. ve Shuler, C. (2010). Investigations of young children's usage and learning with mobile devices and apps. https://clalliance.org/wp-content/uploads/files/learningapps_final_110410.pdf adresinden alınmıştır.
- Cohen, L., Manion, L. ve Morrison, K. (2000). *Research methods in education (5th Edition)*. London: RoutledgeFalmer. DOI: 10.4324/9780203224342
- Cuban, L. (2001) *Oversold and underused: computers in the classroom*. Cambridge, MA: Harvard University Press.
- Çakır, H. (2013). Bilgisayar oyunlarına ilişkin ailelerin görüşleri ve öğrenci üzerindeki etkilerin belirlenmesi. *Mersin Üniversitesi Eğitim Fakültesi Dergisi*, 9(2), 138-150.
- Çalışkan, H. (2019). *Okul öncesi dönemde çalışan öğretmenlerin mahremiyet eğitimi konusunda bilgi düzeylerinin belirlenmesi*. Yayımlanmamış yüksek lisans tezi, Necmettin Erbakan Üniversitesi Eğitim Bilimleri Enstitüsü, Konya.
- Çelen, F. K., Çelik, A. ve Seferoğlu, S. S. (2011). Çocukların internet kullanımları ve onları bekleyen çevrim-içi riskler. *Akademik Bilişim*, 2(4), 645-652.
- Çelik, H. (2021). *Ortaokul Öğrencilerinin Dijital Okuryazarlık Düzeylerinin Belirlenmesi*. Yayımlanmamış yüksek lisans tezi, Gazi Üniversitesi Eğitim Bilimleri Enstitüsü, Ankara.
- Darıcı, S. (2015). Dijital oyunlarda kullanılan subliminal mesajların gerçeklik algısı üzerindeki etkilerine yönelik bir çalışma: Gerçeklik eşiği kavramı, *Turkish Studies International Periodical for the Languages, Literature and History of Turkish or Turki*, 10(14), 181-202. DOI: <http://dx.doi.org/10.7827/TurkishStudies.8778>
- Davison, C. (2012). *Presentation of digital self in everyday life: Towards a theory of Digital Identity*. Yayımlanmamış doktora tezi. RMIT University Graduate School of Business and Law Institute, Melbourne, Australia.
- Derin, M. A. ve Gençoğlu, M. T. (2020). Ortaokul öğrencilerinin bilgi güvenliği farkındalığı. *Savunma Bilimleri Dergisi*, (38), 159-181. DOI: 10.17134.khosbd.813459

- DeVellis, R. (2016). *Ölçek geliştirme: Kuram ve uygulamalar*. Ankara: Nobel Akademik Yayıncılık.
- Dönmez, G. (2019). *Lise öğrencilerinin bilgi güvenliği farkındalığı ile dijital okuryazarlığı arasındaki ilişkinin incelenmesi*. Yayımlanmamış yüksek lisans tezi, Hacettepe Üniversitesi, Eğitim Bilimleri Enstitüsü, Ankara.
- Erboy, E. ve Vural, R. A. (2010). İlköğretim 4 ve 5 sınıf öğrencilerinin bilgisayar oyun bağımlılığını etkileyen faktörler. *Ege Eğitim Dergisi*, 11(1), 39-58.
- Eroğlu, Ş. (2018). Dijital yaşamda mahremiyet (gizlilik) kavramı ve kişisel veriler: Hacettepe Üniversitesi bilgi ve belge yönetimi bölümü öğrencilerinin mahremiyet ve kişisel veri algılarının analizi. *Hacettepe Üniversitesi Edebiyat Fakültesi Dergisi*, 35(2), 130-153. DOI: <https://doi.org/10.32600/huefd.439007>
- Esentaş, M., Güzel, P. ve Vural, M. (2018). Popüler kültürde rekreatif bir etkinlik olarak dijital sporlar. *Beden Eğitimi ve Spor Bilimleri Dergisi*, 20(1), 71-79.
- Fu, J. (2013). Complexity of ICT in education: A critical literature review and its implications. *International Journal of Education and Development Using ICT*, 9(1), 112-125.
- Gülseçen, S. (2021, Ağustos). *Ortaokul Öğrencilerinin Siber Güvenlik Farkındalık Durumu*. 6. Uluslararası Öğrencilik Sempozyumunda sunuldu, Ankara.
- Gaming in Turkey- Oyun ve E-Spor Ajansı. (2020). Türkiye oyun sektörü 2020 raporu. <https://www.gaminginturkey.com/tr/turkiye-oyun-sektoru-raporu-2020/> adresinden alınmıştır.
- Gharieb, M. E. (2021). Knowing the level of information security awareness in the usage of social media among female secondary school students in Eastern Makkah Al-Mukarramah-Saudi Arabia. *International Journal of Computer Science & Network Security*, 21(8), 360-368. <https://doi.org/10.22937/IJCSNS.2021.21.8.45>
- Göldağ, B. (2021). Üniversite öğrencilerinin dijital okuryazarlık düzeyleri ile dijital veri güvenliği farkındalık düzeyleri arasındaki ilişkinin incelenmesi. *E-Uluslararası*

Eğitim Araştırmaları Dergisi, 12(3), 82-100. DOI: <https://doi.org/10.19160/ije-ijer.950635>

- Günay, G. (2011). *Şiddet içerikli online bilgisayar oyunlarının ilköğretim öğrencilerinin saldırganlık tepkileri üzerindeki etkisi*. Yayınlanmamış yüksek lisans tezi, Çanakkale Onsekiz Mart Üniversitesi, Eğitim Bilimleri Enstitüsü, Çanakkale.
- Gür, R. M. (2018). *Çok oyunculu dijital oyunlarda oyun oynama pratikleri: Moba ve mmorpg oyunlar üzerine karşılaştırmalı bir inceleme*. Yayınlanmamış yüksek lisans tezi, İstanbul Arel Üniversitesi, Sosyal Bilimler Enstitüsü, İstanbul.
- Güven, S. (2018). Çocukların oyun tercihleri üzerine bir çalışma. *Electronic Turkish Studies*, 13(27), 795-813. DOI: <http://dx.doi.org/10.7827/TurkishStudies.14335>
- Horzum, M. B. (2011). İlköğretim öğrencilerinin bilgisayar oyunu bağımlılık düzeylerinin çeşitli değişkenlere göre incelenmesi. *Eğitim ve Bilim*, 36(159), 56-68.
- Horzum, M. B., Ayas, T. ve Balta, Ö. Ç. (2012). Çocuklar için bilgisayar bağımlılığı ölçeği. *Türk Psikolojik Danışma ve Rehberlik Dergisi*, 3(30), 76-88.
- Irmak, A. Y. ve Erdoğan, S. (2016). Ergen ve genç erişkinlerde dijital oyun bağımlılığı: Güncel bir bakış. *Türk Psikiyatri Dergisi*, 27(2), 128-137. DOI: 10.5080/u13407
- İzgi, M. C. (2009). *Etik açıdan yaşlı mahremiyeti: Huzurevi örneğinde hizmet alanlar ve verenler açısından bir değerlendirme*. Yayınlanmamış doktora tezi. Ankara Üniversitesi Sağlık Bilimleri Enstitüsü, Ankara, Türkiye.
- Karacı, A., Akyüz, H. İ. ve Bilgici, G. (2017). Üniversite öğrencilerinin siber güvenlik davranışlarının incelenmesi. *Kastamonu Eğitim Dergisi*, 25(6), 2079-2094. <https://doi.org/10.24106/kefdergi.351517>
- Karaduman, M. ve Acıyan, E. P. (2020). Baudrillard'ın simülasyon kuramı bağlamında dijital oyunlar ve bağımlılık üzerine bir değerlendirme. *Trakya Üniversitesi Sosyal Bilimler Dergisi*, 22(1), 453-472. DOI: <https://doi.org/10.26468/trakya-sobed.550935>

- Karaman-Yaşar, S. (2019). *Ortaokul öğrencilerinin gözünden dijital oyun ve dijital oyun bağımlılığı: Kocaeli ili örneği*. Yayımlanmamış yüksek lisans tezi. Atatürk Üniversitesi Eğitim Bilimleri Enstitüsü, Erzurum.
- Kaya, A. (2019). *Üniversite öğrencilerinde sosyal medya kullanımı ile mahremiyet algısı arasındaki ilişkinin incelenmesi*. Yayımlanmamış yüksek lisans tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.
- Kaya, B. A. (2013). *Çevrimiçi oyun bağımlılığı ölçeğinin geliştirilmesi*. Yayımlanmamış yüksek lisans tezi, Gaziosmanpaşa Üniversitesi Eğitim Bilimleri Enstitüsü, Tokat.
- Kaya, M. (2020). *Ortaöğretim öğrencilerinin dijital vatandaşlık ve dijital okuryazarlık düzeyleri arasındaki ilişkinin incelenmesi*. Yayımlanmamış yüksek lisans tezi, Mersin Üniversitesi Eğitim Bilimleri Enstitüsü, Mersin.
- Koçak, H. ve Köse, Z. (2014). Ergenlerin bilgisayar oyunu oynama alışkanlıkları ve sosyalleşme süreçleri üzerine bir araştırma (Kütahya ili örneği). *Dumlupınar Üniversitesi Sosyal Bilimler Dergisi*, Kütahya Özel Sayısı, 21-32.
- Lawshe, C. H. (1975). A quantitative approach to content validity. *Personnel psychology*, 28(4), 563-575.
- Lorenz, B., Sousa, S. ve Tomberg, V. (2012, Temmuz). *Privacy awareness of students and its impact on online learning participation—a case study*. IFIPAICT’de sunuldu, Springer, Berlin, Heidelberg.
- Mıhçı, P. (2016). *Ortaokul öğrencileri, öğretmenleri, okul yöneticileri ve velilerin siber sağlık durumlarının incelenmesi*. Yayımlanmamış doktora tezi. Gazi Üniversitesi Eğitim Bilimleri Enstitüsü, Ankara.
- Mıhçı Türker, P. ve Kılıç Çakmak, E. (2019). An investigation of cyber wellness awareness: Turkey secondary school students, teachers, and parents. *Computers in the Schools*, 36(4), 293-318. DOI: <https://doi.org/10.1080/07380569.2019.1677433>
- Mustafaoğlu, R. ve Yasacı, Z. (2018). Dijital oyun oynamanın çocukların ruhsal ve fiziksel sağlığı üzerine olumsuz etkileri. *Bağımlılık Dergisi*, 19(3), 51-58.

- Mustafaoğlu, R., Zirek, E., Yasacı, Z. ve Özdiñler, A. R. (2018). Dijital teknoloji kullanımının çocukların gelişimi ve sağlığı üzerine olumsuz etkileri. *Addicta: The Turkish Journal on Addictions*, 5(2), 1-21. DOI: 10.15805/addicta.2018.5. 2.0051
- Okumuş, M. ve Atılgan, S. S. (2021). Üniversite öğrencilerinin dijital okuryazarlık becerileri ile dijital mahremiyet kaygısı arasındaki ilişki. *TRT Akademi*, 6(12), 342-363. DOI: <https://doi.org/10.37679/trta.907558>
- Pala, Ş. M. ve Başıbüyük, A. (2020). 10-12 Yaş grubu öğrencileri için dijital okuryazarlık ölçeği geliştirme çalışması. *Akdeniz Eğitim Araştırmaları Dergisi*, 14(33), 542565. DOI: 10.29 329/mjer.2020.272.25
- Pala, Ş. M. (2019). *Ortaokul 5. sınıf öğrencilerinin sosyal bilgiler dersi bilim teknoloji ve toplum öğrenme alanına ilişkin akademik başarı ve becerilerinin incelenmesi*. Yayımlanmamış doktora tezi, Erzincan Binali Yıldırım Üniversitesi Sosyal Bilimler Enstitüsü, Erzincan.
- Öztürk, Y. (2020). *Dijital okuryazarlık hakkında lise öğrencilerinin kendilerine ve anne-babalarına yönelik görüşleri Kırıkkale ili örneği*. Yayımlanmamış yüksek lisans tezi, Gazi Üniversitesi Eğitim Bilimleri Enstitüsü, Ankara.
- Öztürk, A. (2021). Covid-19 Pandemi sürecinde bilişim teknolojileri bağımlılığı. *Ağrı İbrahim Çeçen Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 7(1), 195-219. DOI: 10.31463/aic usbed.903612
- Phillips, D. J. (2004). Privacy policy and PETs: The influence of policy regimes on the development and social implications of privacy enhancing technologies. *New Media & Society*, 6(6), 691-706. DOI: <https://doi.org/10.1177/146144804042523>
- Rideout, V. (2011) Zero to eight: children's media use in america. <https://www.common-sensemedia.org/file/zerotoeightfinal2011pdf-0/download> adresinden alınmıştır.
- Sepetçi, T. (2020). *Avrupa Birliği'nde dijital oyunlara yönelik düzenlemeler ve Türkiye'deki mevcut durum*. 5. International EMI Entrepreneurship and Social Sciences Congress'de sunuldu, Ohri.

- Sezen, A. ve Erden, M. (2018). Mahremiyetin psiko-sosyal yansımaları. *Dicle Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 10(20), 83-92.
- Sığın, İ. (2019). *Sosyal medya kullanan gençlerin mahremiyet algısının incelenmesi*. Yayımlanmamış yüksek lisans tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.
- Sırakaya, M. ve Seferoğlu, S. S. (2018). Çocukların çevrim-içi ortamlarda karşılaştıkları riskler ve güvenli internet kullanımı. B. Akkoyunlu, A. İşman ve H. F. Odabaşı (Ed). *Eğitim teknolojileri okumaları 2018* içinde (s. 185-202). Adapazarı; TOJET ve Sakarya Üniversitesi.
- Simon, M. K. ve Goes, J. (2018). *Dissertation and scholarly research recipes for succes: a practical guide to start and complete your dissertation, thesis, or formal research project*. Seatle: Dissertations Success LLC.
- Söğüt, F. (2020). Dijital ebeveynlerin dijital oyunlar ve şiddet ilişkisine yönelik algıları. *İletişim Kuram ve Araştırma Dergisi*, 2020(51), 79-100.
- Stephen C. ve Plowman L. (2014). Digital play. L. Brooker, M. Blaise ve S. Edwards (Ed), *Sage Handbook of Play and Learning in Early Childhood* içinde (s.330-341). London: Sage.
- Talan, T. ve Aktürk, C. (2021). Orta Öğretim öğrencilerinin dijital okuryazarlık ve bilgi güvenliği farkındalığı seviyelerinin incelenmesi. *Kahramanmaraş Sütçü İmam Üniversitesi Sosyal Bilimler Dergisi*, 18(1), 158-180. DOI: <https://doi.org/10.33437/ksusbd.668255>
- Taştekin, E. (2019). *Ortaokul öğrencilerinin dijital oyun oynama alışkanlıklarının öğrenci ve veli bakış açısından incelenmesi*. Yayımlanmamış yüksek lisans tezi, Balıkesir Üniversitesi Fen Bilimleri Enstitüsü, Balıkesir.
- Tekeli, P. (2018). *Dijital hikâye anlatımı atölyesinde yaşlıların dijital okuryazarlık deneyimlerinin incelenmesi*. Yayımlanmamış yüksek lisans tezi, Hacettepe Üniversitesi Eğitim Bilimleri Enstitüsü, Ankara.

- Tekerek, M. ve Tekerek, A. (2013). Öğrencilerin bilgi güvenliği farkındalığı üzerine bir araştırma. *Turkish Journal of Education*, 2(3), 61-70. DOI: <https://doi.org/10.19128/turje.181065>
- Tirumala, S. S., Sarrafzadeh, A. ve Pang, P. (2016, Kasım). *A survey on Internet usage and cybersecurity awareness in students*. 14th Annual Conference on Privacy, Security and Trust (PST)'da sunuldu, Auckland, New Zealand
- Toran, M., Ulusoy, Z., Aydın, B., Deveci, T. ve Akbulut, A. (2016). Çocukların dijital oyun kullanımına ilişkin annelerin görüşlerinin değerlendirilmesi. *Kastamonu Eğitim Dergisi*, 24(5), 22-63.
- Töngel, E. (2020). *Üniversite öğrencilerinin çevrimiçi mahremiyet farkındalıklarının çeşitli değişkenler açısından incelenmesi*. Yayımlanmamış yüksek lisans tezi, Amasya Üniversitesi Fen Bilimleri Enstitüsü, Amasya.
- Töngel, E. ve Kara, M. (2021). Üniversite öğrencilerinin çevrimiçi mahremiyet farkındalıklarının belirli etkenler açısından incelenmesi. *Türkiye Sosyal Araştırmalar Dergisi*, 25(1), 147-162.
- Trepte, S. ve Reinecke, L. (2011). The social web as a shelter for privacy and authentic living. S. Trepte ve L. Reinecke (Ed.), *Privacy online: perspectives on privacy and self-disclosure in the social web* içinde (s. 61-73). Berlin: Springer. DOI: 10.1007/978-3-642-21521-6_6
- Türkiye Bilişim Derneği. (2020). Türkiye bilişim derneği küresel gelişmeler 2020 raporu. <https://www.tbd.org.tr/tbd-kuresel-gelismeler-2020-raporu/> adresinden alınmıştır
- Türkiye İstatistik Kurumu. (2020). Hane halkı Bilişim Teknolojileri (BT) Kullanım Araştırması. <https://data.tuik.gov.tr/Kategori/GetKategori?p=bilgi-teknolojileri-ve-bilgi-toplumu-102&dil=1> adresinden alınmıştır.
- Uğurlu, T. T., Şengül, C. B. ve Şengül, C. (2012). Bağımlılık psikofarmakolojisi. *Psikiyatride Güncel Yaklaşımlar*, 4(1), 37-50. DOI: <https://doi.org/10.5455/cap.20120403>

- Üstündağ, M. T., Güneş, E. ve Bahçıvan, E. (2017). Dijital okuryazarlık ölçeğinin Türkçe 'ye uyarlanması ve fen bilgisi öğretmen adaylarının dijital okuryazarlık durumları. *Eğitim ve Gelecek Dergisi*, 12, 19-29.
- Üstündağ, A. (2019). 4-6 Yaş arası çocuklar tarafından tercih edilen dijital oyunlar. *Çankırı Karatekin Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 10(2), 1-19.
- Weinberger, M., Bouhnik, D. ve Zhitomirsky-Geffet, M. (2017). Factors affecting students' privacy paradox and privacy protection behavior. *Open Information Science*, 1(1), 3-20.
- Vandewater, E.A. ve Lee, S-J. (2007). Measuring children's media use in the digital age: issues and challenges, *American Behavioral Scientist*, 52(8), 1152-1176. DOI: 10.1177/0002764209331539
- Vangsnes, V., Økland, N. T. G. ve Krumsvik, R. (2012). Computer games in preSchool settings: didactical challenges when commercial computer games are implemented in kindergartens, *Computers and Education*, 58, 1138-1148. DOI: 10.1016/j.compedu.2011.12.018
- Von Solms, R. ve Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97-102. DOI: <http://dx.doi.org/10.1016/j.cose.2013.04.004>
- Vural, Y. (2007). *Kurumsal bilgi güvenliği ve sızma (Penetrasyon) testleri*. Yayımlanmamış yüksek lisans tezi, Gazi Üniversitesi, Fen Bilimleri Enstitüsü. Ankara.
- Yaman, F., Çubukçu, A., Küçükali, M. ve Yurdakul, I. K. (2020). Ortaokul ve lise öğrencilerinin sosyal medya kullanımı ve dijital oyun oynama durumları. *Sakarya Üniversitesi Eğitim Fakültesi Dergisi*, 20(2), 160-174.
- Yaşar, Ç. (2019). *BÖTE öğretmen adaylarının kariyer eğilimlerinin, sosyal medyaya ilişkin görüşlerinin ve dijital okuryazarlık beceri düzeylerinin incelenmesi*. Yayımlanmamış yüksek lisans tezi, Balıkesir Üniversitesi Fen Bilimleri Enstitüsü, Balıkesir.

- Yeşildal, M. (2018). *Yetişkin bireylerde dijital okuryazarlık ve sağlık okuryazarlığı arasındaki ilişki: Konya örneği*. Yayınlanmamış yüksek lisans tezi, Necmettin Erbakan Üniversitesi Sağlık Bilimleri Enstitüsü, Konya.
- Yılmaz, E., Şahin, Y. L. ve Akbulut, Y. (2016). Öğretmenlerin dijital veri güvenliği farkındalığı. *Sakarya University Journal of Education*, 6(2), 26-45. DOI: 10.19126/suje .29650
- Yılmaz, R., Karaoğlu Yılmaz, F. G., Öztürk, H. T. ve Karademir, T. (2017). Lise öğrencilerinin güvenli bilgisayar ve internet kullanım farkındalıklarının incelenmesi: Bartın ili örneği. *Pegem Eğitim ve Öğretim Dergisi*, 7(1), 83-114 DOI: 10.14527/pegegog.2017.004.
- Yiğit, A. (2007). *İlköğretim 2. Sınıf seviyesinde bilgisayar destekli eğitici matematik oyunlarının başarıya ve kalıcılığa etkisi*. Yayınlanmamış yüksek lisans tezi, Çukurova Üniversitesi Sosyal Bilimler Enstitüsü, Adana.
- Young, K. S. (2004). Internet addiction: a new clinical phenomenon and its consequences. *American behavioral scientist*, 48(4), 402-415. DOI: <https://doi.org/10.1177/0002764204270278>
- Yücel, V. (2019). Zararlı dijital oyunlar ve çocuklar. *Avrasya Sosyal ve Ekonomi Araştırmaları Dergisi*, 6(7), 340-353.
- Yüksel, M. (2003). Mahremiyet hakkı ve sosyo-tarihsel gelişimi. *Ankara Üniversitesi SBF Dergisi*, 58(01). DOI: https://doi.org/10.1501/SBFder_0000001619
- Zahri, Y., Ab Hamid, R. S. ve Mustaffa, A. (2017). Cyber security situational awareness among students: a case study in Malaysia. *International Journal of Educational and Pedagogical Sciences*, 11(7), 1704-1710. DOI: doi.org/10.5281/zenodo.1131053
- Zurnacı, B. (2019). *Hedefe dayalı senaryolarla dijital okuryazarlık becerilerinin kazandırılması*. Yayınlanmamış yüksek lisans tezi, Ondokuz Mayıs Üniversitesi Eğitim Bilimleri Enstitüsü, Samsun.

EKLER

Ek 1. Çevrimiçi Oyunlarda Siber Güvenlik Farkındalığı Ölçeği

SORULAR	Hiç Katılmıyorum	Katılmıyorum	Kısmen Katılıyorum	Katılıyorum	Tamamen Katılıyorum
1. Çevrimiçi oyunlarda diğer oyuncuları doğru olmayan bazı davranışları (yalan söyleme, hile yapma vb.) yapmaya zorlarım.					
2. Çevrimiçi oyunlarda rakiplerime onları küçük düşürücü takma isimlerle hitap ederim.					
3. Çevrimiçi oyun oynarken takım arkadaşlarım ve/veya rakip oyuncularla alay ederim.					
4. Çevrimiçi oyun oynarken kazanmak amacıyla doğru olmayan davranışlar (yalan söyleme, hile yapma, zorbalık vb.) yapması için arkadaşlarıma baskı yaparım.					
5. Çevrimiçi oyun oynarken kazanmak için yaptığım doğru olmayan davranışları (yalan söyleme, hile yapma, zorbalık vb.) gerçek hayatta da yapmakta bir sakınca görmem.					
6. Çevrimiçi oyunlarda kullanıcı adı ve şifre bilgilerimi takım arkadaşlarımla paylaşıyorum.					
7. Oynadığım çevrimiçi oyunların her biri için birbirinden farklı giriş şifresi kullanırım.					
8. Çevrimiçi oyun oynarken seviye atlamak için benden istenildiğinde kişisel bilgilerimi paylaşıyorum.					
9. Çevrimiçi oyun oynadığım oyunculara her zaman güvenirim.					
10. Çevrimiçi oyunlarda kredi kartı bilgisini vermeden önce oyun platformlarının (Steam, Valorant, Minecraft vb.) güvenilirliğini kontrol ederim.					
11. Çevrimiçi oyunlarda ödeme yapmam gerektiğinde ailemin bilgisi dahilinde ödeme yaparım.					
12. Çevrimiçi oyunun bölümlerinde ilerleyebilmek için özel yetenek, aksesuar, silah gibi özellikleri satın almam gerektiğinde güvenilir ödeme yöntemlerini (Sanal Kart, Banka Havalesi vb.) tercih ederim.					

13. Çevrimiçi oyunlarda sadece güvenilir oyun platformlarına (Valorant, Minecraft vb.) ödeme yaparım.					
14. Çevrimiçi oyunlarda lisanslı oyunları tercih ederim.					
15. Çevrimiçi oyun oynadığım cihazımda (Bilgisayar, Tablet, Telefon vb.) güncel bir antivirüs yazılımı kullanırım.					
16. Çevrimiçi oyunları güvenilir ortamlardan/sitelerden indiririm.					
17. Çevrimiçi oyun oynarken güvenlik riskleri ile karşılaşabileceğimin farkındayım.					
18. Çevrimiçi oyun oynarken izlenebilirliği önlemek için gerekli olmayan erişim izinlerini (konum, mikrofon, kamera vb.) kapatırım.					



Ek 2. Çevrimiçi Mahremiyet Farkındalığı Ölçeği

Soru No		Kesinlikle Katılmıyorum	Katılmıyorum	Kararsızım	Katılıyorum	Kesinlikle Katılıyorum
1	Kullandığım çevrimiçi platformların gizlilik ayarlarını ve bildirimlerini kontrol ederim.	()	()	()	()	()
2	Kullandığım çevrimiçi ortamlarda (sosyal ağlar, alışveriş siteleri, oyunlar vb.) hesabımın gizlilik ayarlarını yaparım.	()	()	()	()	()
3	Çevrimiçi ortamlarda kullandığım parolaların güçlü olmasına (büyük-küçük harf, rakam, özel karakterler ve en az 8 karakter kullanımıyla) dikkat ederim.	()	()	()	()	()
4	E-posta veya sosyal ağlardan aldığım mesajların içeriğinin güvenilir olup olmadığını anlarım.	()	()	()	()	()
5	Çevrimiçi ortamlarda paylaştığım bilgilerin şirketler, devlet kurumları veya bilgisayar korsanları tarafından kullanılabilirliğinin farkındayım.	()	()	()	()	()
6	Çevrimiçi ortamlarda tanımadığım kişilerden gelen mesaj veya epostaların güvenlik riski oluşturup oluşturmadığını anlarım.	()	()	()	()	()
7	Çevrimiçi platformlarda paylaştığım bilgilerin kötü niyetli kişiler tarafından kullanılabilirliğinin farkındayım.	()	()	()	()	()
8	İnternet sitelerinin kullandığı çerez (cookies) dosyaları hakkında bilgim vardır.	()	()	()	()	()
9	Mobil cihazıma uygulama yüklerken uygulamanın hangi izinleri talep ettiğine dikkat ederim.	()	()	()	()	()
10	İnternet sitelerinin ve mobil uygulamaların güvenlik sertifikalarını ve veri şifreleme yöntemlerini kontrol ederim.	()	()	()	()	()
11	Ziyaret ettiğim web sitelerinin güvenliğini kontrol ederim.	()	()	()	()	()
12	Web tarayıcımdaki eklentilerin hangi bilgilere erişeceğine dikkat ederim.	()	()	()	()	()
13	Çevrimiçi ortamlarda tanımadığım kişilerle kişisel bilgilerimi (adres, doğum tarihi, yaş, iş, telefon vb.) paylaşıyorum.	()	()	()	()	()
14	Arkadaşlarımla veya yakınlarımla yaptığım yazışmaların ekran görüntülerini izin almaya gerek duymadan paylaşıyorum.	()	()	()	()	()
15	Başkalarına ait bilgi, resim, video vb. içerikleri çevrimiçi ortamlarda izin almaya gerek duymadan paylaşıyorum.	()	()	()	()	()
16	Çevrimiçi ortamlarda tanımadığım kişilerin beni takip etmesine veya arkadaş olmasına izin veririm.	()	()	()	()	()
17	Çevrimiçi ortamlarda tanımadığım kişilerle iletişim kurarım.	()	()	()	()	()

Ek 3. Dijital Okuryazarlık Ölçeği

		Her Zaman	Çoğu Zaman	Bazen	Nadiren	Hiçbir Zaman
1	İnternette bilgiye ulaşmak için arama motorlarını kullanabilirim.					
2	Arama yaparken bazı filtreleri kullanabilirim (Örneğin: sadece resimlerde, videolarda, haritalarda arama).					
3	İnternette ulaştığım bilgilerin tamamının güvenilir olmadığını bilirim.					
4	İnternette ulaştığım bilgilerin güvenilirliğini sağlamak için bilgiyi farklı kaynaklarla karşılaştırabilirim.					
5	Dosyaları veya içerikleri (ör: metin, resim, müzik, video, web sayfaları) bilgisayarda, tablette ve telefonda kaydedebilirim.					
6	Kaydettiğim dosya ve içeriklere tekrar ulaşabilirim.					
7	Cep telefonu, internet e-posta ve sohbet etme programlarıyla iletişim kurabilirim.					
8	İnternet siteleri üzerinden dosya ve içerik paylaşabilirim (e-postaya resim ve dosya eklemek, Facebook vb sitelerde fotoğraf paylaşmak gibi).					
9	İnternette başkalarının oluşturduğu/paylaştığı herhangi bir dokümana katkıda bulunabilirim.					
10	Sosyal ağları (Facebook, Twitter, Instagram vb) kullanabilirim.					
11	Dijital araçları kullanırken uyulması gereken kurallar olduğunu bilirim (ör: yorum yaparken, kişisel bilgi paylaşırken).					
12	İnternette bilgi aktarımında/paylaşımında bulunabilirim.					
13	Bilgisayar, akıllı telefon, tablet gibi araçlarımı korumak için şifreler kullanabilirim.					
14	Kimlik bilgilerimin çalınabileceğinin farkında olduğum için kişisel bilgilerimi internette paylaşmamam gerektiğini bilirim.					
15	Dijital teknolojiyi yoğun kullanmanın sağlığını olumsuz etkileyebileceğini bilirim.					
16	Teknolojinin çevreye pozitif ve negatif etkilerini anlayabilirim.					
17	Yeni bir cihaz veya uygulamayı kullanırken teknik bir sorun olduğunda destek ve yardım bulabilirim.					
18	Dijital teknolojileri kullanırken sıkça ortaya çıkan sorunların çoğunu çözebilirim.					
19	Dijital teknolojileri kullanırken teknik olmayan problemleri çözebilirim.					
20	Programlar veya araçların teknolojik problemlerini çözebilirim					
21	Teknoloji ile ilgili bir problem ile karşı karşılaştığımda, problemi çözmek için dijital araçları kullanabilirim.					

Ek 4. Arařtırma İzni



T.C.
TOKAT VALİLİĞİ
İl Millî Eğitim Müdürlüğü

Sayı : E-27001677-44-39934256
Konu : Anket Çalışma İzni

28/12/2021

VALİLİK MAKAMINA

- İlgi : a) Millî Eğitim Bakanlığına Bağlı Okul ve Kurumlarda Yapılacak Araştırma ve Araştırma Desteğine Yönelik İzin ve Uygulama Yönergesi.
b) 10/11/2021 tarihli ve 27001677/44/36577437 sayılı Valilik Makam Onayı.
c) Araştırma İzinleri İnceleme Komisyonunun 24.12.2021 tarihli tutanağı.
d) Tokat Gaziosmanpaşa Üniversitesi Rektörlüğü Öğrenci İşleri Daire Başkanlığının 14.12.2021 tarih ve 108777 sayılı yazısı.

Tokat Gaziosmanpaşa Üniversitesi'nin ilgi (d) talebi gereği okulun Lisansüstü Eğitim Enstitüsü ve Öğretim Teknolojileri Eğitimi Anabilim Dalı yüksek lisans öğrencisi Süleyman VURAL Tokat İl Millî Eğitim Müdürlüğüne bağlı ortaokullarda öğrenim gören öğrencilere yönelik "Ortaokul Öğrencilerinin Çevrimiçi Oyunlardaki Siber Güvenlik Farkındalıkları ile Teknoloji Okuryazarlık Düzeylerinin Dijital Kimlik Mahremiyeti Becerileri Üzerine Etkisi" konu başlıklı anket çalışmasını uygulamak istenmektedir.

Tokat Gaziosmanpaşa Üniversitesi Lisansüstü Eğitim Enstitüsü Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı yüksek lisans öğrencisi Süleyman VURAL Doç. Dr. Kerem KILIÇER danışmanlığında hazırlamış olduğu "Ortaokul Öğrencilerinin Çevrimiçi Oyunlardaki Siber Güvenlik Farkındalıkları ile Teknoloji Okuryazarlık Düzeylerinin Dijital Kimlik Mahremiyeti Becerileri Üzerine Etkisi" konulu bilimsel amaçlı anket çalışmasını Tokat il/ilçe ortaokul öğrencilerine uygulama yapma isteği Müdürlüğümüzce uygun görülmektedir.

Makamınızca da uygun görüldüğü takdirde Olur'unuza arz ederim.

Murat KÜÇÜKALİ
İl Millî Eğitim Müdürü

OLUR

Osman SARI
Vali a.
Vali Yardımcısı

Ek:

- 1-Tutanak
2-Tokat GOP. Üniv. Rektörlüğü yazısı ve yazı ekleri

Adres : Gop Bulvarı 60100 Merkez/TOKAT

Telefon No : 0 (356) 214 10 17
E-Posta: stratejigelistirme60@meb.gov.tr
Kep Adresi : meb@hs01.kep.tr

Bu belge güvenli elektronik imza ile imzalanmıştır.

Belge Doğrulama Adresi : <https://www.turkiye.gov.tr/meb-ebys>

Bilgi için: Güven KOKSAL
Unvan: Büro Hizmetleri
İnternet Adresi: www.mebb.gov.tr Faks: 3562141186

Bu evrak güvenli elektronik imza ile imzalanmıştır. <https://evraksorgu.meb.gov.tr> adresinden 7501-4344-37e5-a751-925b kodu ile teyit edilebilir.



Ek 5. Araştırma Evrenine Ait Öğrenci Sayıları



T.C.
TOKAT VALİLİĞİ
İl Millî Eğitim Müdürlüğü

Sayı : E-27001677-42-36658994
Konu : Veri Talebi

10.11.2021

YEŞİLYURT KAYMAKAMLIĞINA
(İlçe Millî Eğitim Müdürlüğü)

İlgi : 20/10/2021 tarih ve 35125504 sayılı yazı.

İlgi yazı ile, İlçeniz Millî Hakimiyet Ortaokulu'nda Müdür Yardımcısı olarak görev yapan ve Tokat Gazi Osman Paşa Üniversitesi Eğitim Bilimleri Enstitüsü Bilgisayar ve Öğretim Teknolojileri Ana Bilim Dalında Yüksek Lisans Programına devam eden Süleyman VURAL'ın araştırma konusunda kullanılmak üzere veri talebinde bulunmaktadır. Çalışmalarına kaynaklık edebilecek ilkökul ve ortaokul öğrenci sayılarına dair veriler ektedir.

Bilgilerinizi rica ederim.

Murat KÜÇÜKALİ
Vali a.
İl Millî Eğitim Müdürü

Ek:
- İlgi Yazı (1 sayfa)

Bu belge güvenli elektronik imza ile imzalanmıştır.

Adres :

Belge Doğrulama Adresi : <https://www.turkiye.gov.tr/meb-ebys>

Telefon No : 0 (356) 214 10 17

E-Posta: istatistik60@meb.gov.tr

Kep Adresi : meb@hs01.kep.tr

Bilgi için: D.ÇELİK

Unvan : Programcı

İnternet Adresi:

Faks:3562141186

Bu evrak güvenli elektronik imza ile imzalanmıştır. <https://evraksorgu.meb.gov.tr> adresinden 1b8e-43c5-385b-9139-c8b7 kodu ile teyit edilebilir.

2021-2022 Eğitim Öğretim Yılı Öğrenci Sayıları				
Resmi/Özel	İlkokul	Ortaokul	Lise	Genel Toplam
Resmi	27.630	27.841	31.416	86.887
Özel	1.109	1.148	2.517	4.774
Genel Toplam	28.739	28.989	33.933	91.661



Ek 6. Ölçme Araçları Kullanım İzinleri



Ek 7. Özgeçmiş