

T. C.
BAHÇEŞEHİR ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

PROJE ADI

Dijital Güvenlik Bilinci Oluşturmak İçin Eğitsel Oyunların Kullanımı:
Ortaokul Düzeyindeki Öğrencilerinin Bakış Açısı

ÖĞRETİM TEKNOLOJİLERİ PROGRAMI

TEZSİZ YÜKSEK LİSANS

UZMANLIK PROJESİ

Ad SOYAD

Ahmet Polat

İSTANBUL 2023

T. C.
BAHÇEŞEHİR ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

PROJE ADI

**Dijital Güvenlik Bilinci Oluşturmak İçin Eğitsel Oyunların Kullanımı: Ortaokul
Düzeyindeki Öğrencilerinin Bakış Açısı**

ÖĞRETİM TEKNOLOJİLERİ PROGRAMI

TEZSİZ YÜKSEK LİSANS
UZMANLIK PROJESİ

Ad SOYAD

Ahmet Polat

PROJE DANIŞMANI

.....

İSTANBUL 2023

ÖZET

Dijital Güvenlik Bilinci Oluşturmak İçin Eğitsel Oyunların Kullanımı: Ortaokul Düzeyindeki Öğrencilerinin Bakış Açısı

Ahmet Polat

Öğretim Teknolojilerim, Yüksek Lisans Programı

Proje Danışmanı: YRD. DOÇ Dr. ÖZGÜR ERKUT ŞAHİN

Ocak 2024, ... sayfa

Dijital teknolojinin ilerlemesi ve yeni araçların, oyunların, uygulamaların ve sosyal medya sitelerinin gelişmesiyle birlikte çevrimiçi dolandırıcılık, siber zorbalık, kimlik avı gibi tehditlerden ve özellikle bu araçlar, uygulamalar veya web siteleriyle ilişkili güvenlik açıklarından korunmak zorlaşıyor. ortaokul çocukları için. Bu makale ortaokul öğrencilerinin dijital güvenlik bilgilerine genel bir bakış sunmaktadır. Bu araştırmanın amacı, ortaokul öğrencilerinin dijital güvenliğe ilişkin bilgi düzeyini değerlendirmek ve çocuklara dijital güvenliği oyunlar aracılığıyla eğlenceli, ilgi çekici ve motive edici bir şekilde öğretmede yardımcı ve etkili olacak araçları geliştirmektir. Araştırma, görüşmeler ve anketler kullanılarak nitel araştırma yöntemlerini izlemektedir. Araştırmada ortaokul öğrencilerinin bilgi düzeylerinin daha iyi olduğu ve dijital okuryazar bireyler oldukları ortaya çıktı. Öğrenciler siber saldırı, siber zorbalık ve kişisel bilgiler gibi dijital güvenliğin bazı yönlerine ilişkin yeterli düzeyde farkındalık sergilediler. Eğitsel oyunlar ortaokul çocuklarının dijital güvenlik konusunda eğitilmesinde önemli bir rol oynadı. Ayrıca sonuçlar, öğrencilerin internetteki teknik terimleri anlamakta zorlandıklarını, dolayısıyla müfredat ve oyun tasarlamanın siber zorbalık, çevrimiçi dolandırıcılık ve dijital tehditler hakkındaki bilgilerini artırmalarına yardımcı olabileceğini göstermektedir.

Anahtar Kelimeler: Dijital Güvenlik, Siber Zorbalık, Oyunlar, Ortaokul çocukları

ABSTRACT

Using Educational Games to Raise Digital Security Awareness: Middle School Student's Perspective

Ahmet Polat

Instructional Technologies, Masters Program

Project Advisor: YRD. DOÇ. Dr. ÖZGÜR ERKUT ŞAHİN

January 2024, pages

With the advancement of digital technology and the development of new tools, games, applications and social media sites, it is becoming difficult to prevent oneself from threats such as online fraud, cyberbullying, phishing and vulnerabilities associated with these tools, apps or websites, especially for middle school children. This paper provides an overview of digital security knowledge in middle school students. The goal of this research is to assess the level of information in middle school students regarding digital security and further develop tools that will be helpful and effective in teaching the children about digital security through games in a playful, engaging, and motivating manner. The research follows qualitative research methods, using interviews, and questionnaires. The study found that middle school students had a better level of knowledge and they were digitally literate individuals. Students demonstrated a decent level of awareness of some aspects of digital security such as cyber-attack, cyberbullying, and personal information. The educational games played an important role in educating middle school children regarding digital security. Moreover, the results show that students had difficulty in understanding technical terms on the internet, therefore, designing curriculum and games can help them increase their knowledge about cyberbullying, online fraud, and digital threats.

Keywords: Digital Security, Cyberbullying, Games, Middle School children

Önsöz

Öncelikle danışmanım **YRD. DOÇ. DR. ÖZGÜR ERKUT ŞAHİN'e** bu araştırma projesi boyunca verdiği sürekli destek ve rehberlik için son derece minnettarım. Araştırmam boyunca tüm sorularıma iyi yanıtlar verdiği ve hızlı ve olumlu yanıtlar verdiği için kendisine müteşekkirim. Onun engin bilgisi ve engin tecrübesi akademik araştırmalarımnda ve günlük yaşamımda beni cesaretlendirdi.

Röportajlarda benimle işbirliği yapan katılımcılarıma müteşekkirim ve onların işbirliği olmasaydı bu proje mümkün olamazdı. Destekleriyle projemi zamanında tamamlamama yardımcı olan sınıf arkadaşlarıma en derin minnettarlığımı ifade etmek isterim.

İÇİNDEKİLER

ÖZET	i
ABSTRACT	ii
Önsöz	iii
BÖLÜM 1: GİRİŞ	1
1.1 Teorik Çerçeve.....	2
1.2 Problem Durumu	2
1.3 Çalışmanın Amacı.....	2
1.4 Hipotezler	3
1.5 Çalışmanın Önemi	3
1.6 Tanımlar.....	4
BÖLÜM 2: LİTERATÜR İNCELEMESİ	5
2.1 Digital Çağında Eğitsel Oyunların Önemi.....	5
2.2 Digital Oyunların Öğrenciler Üzerine Etkileşimi.....	6
2.3 Online Güvenliliğin Önemi Ve Koruma Mekanizması	8
2.4 Oyun ile Eğitim Ve Sosyalleşme Sağlama Taktik	9
BÖLÜM 3: METODOLOJİ	11
3.1 Veri toplama.....	11
3.2 Veri analizi	11
BÖLÜM 4: VERİ ANALİZİ VE TARTIŞMA	12
4.1 Tematik Analiz Frekans ve Yüzde	12
4.2 Dijital Güvenlik Bilgisi ve Öğrenci Deneyimleri.....	15
4.3 Eğitsel Oyunların Etkililiği.....	16
4.4 Öğrencilerin Öğrenme Tercihleri.....	18
4.5 Dijital Güvenliği Öğrenirken Karşılaşılan Zorluklar.....	19
4.6 Eğitsel Oyunların Etkisi.....	20
4.7 Oyun Tasarımı ve Müfredat Entegrasyonu	21
Sonuç ve Tavsiyeler	25
Kaynakça	28
EK	30

BÖLÜM 1

GİRİŞ

Eğlence sektörü, bilgisayar ve internetin küresel çapta benimsenmesinin bir sonucu olarak kendisine yeni ve büyük bir pazar bulmuştur. "Dijital oyunlar" yeni eğlence pazar payının önemli bir bölümünü oluşturmaktadır. Dijital oyunlar geleneksel oyunların yerini aldıkça, oyun alışkanlıkları, zevkleri ve türlerindeki değişiklikler daha belirgin hale gelmiştir. Ortam değiştiğinde, çocuklar ve gençler sanal dünyada daha fazla zaman geçirmekte, bu da psiko-sosyal ve davranışsal sağlıklarını olumsuz etkilemekte ve kötü davranışlara yol açmaktadır. (Taylan, Kara, & Durğun, 2017). Dijital dünyanın artan önemi, özellikle ortaokul düzeyinde dijital güvenlik farkındalığının geliştirilmesini gerektirmektedir. Eğitsel oyunlar eğlenceli ve interaktif bir öğrenme deneyimi sunarak güvenli çevrimiçi davranışları teşvik eder. Genç yaşta farkındalık yaratmak, öğrencilerin çevrimiçi platformlarda sorumlu davranmalarını sağlamak için çok önemlidir. Eğitsel oyunlar interaktif bir ortam sağlayarak daha iyi anlama ve kalıcı öğrenmeye yol açar. Dijital güvenliğe odaklanan oyunlar, öğrencilerin gerçek dünya senaryolarını simüle etmelerine olanak tanıyarak dijital güvenliğin önemi konusunda daha bilinçli olmalarını sağlar. (Söğüt, 2020) Etkileşimli video ve bilgisayar oyunları son 20-25 yılda özellikle gençler arasında giderek daha popüler hale gelmiştir. Başlangıçta bu oyunlar bilgisayarlara meraklı gençler ve genç yetişkinler tarafından oynanıyordu. Doksanlı yılların başında video ve bilgisayar oyunları, çocuklar da dahil olmak üzere gençler için günlük yaşamın bir parçası haline gelmiştir. Bu gelişme, çocuklar ve gençler medya, moda ve müzik gibi endüstriler için önemli hedef gruplar olduğundan, ekonomik nedenler de dahil olmak üzere çeşitli nedenlere bağlanabilir. Teknik olarak, elektronik oyunlara başlamak ve oynamak son yirmi yılda daha kolay hale gelmiştir. Ancak, informal öğrenme süreçlerini ve bunların arka planını anlamak, "medya kültürlerinin çatışmasını" önlemek için gereklidir. Öğretmenler, ebeveynler ve eğitimciler genellikle çocukların ve gençlerin medya kültürlerini, eğitimsel ve siyasi söylemlerde örtük bir norm olarak temsil ettikleri kuşak perspektiflerinden ele alırlar. (Fromme, 2003). Bu çalışma, ortaokul öğrencileri arasında dijital güvenlik farkındalığını artırmada eğitsel oyunların etkinliğini incelemektedir. Bu oyunların öğrencilerin dijital güvenlik farkındalığını artırmada etkili olup olmadığını ve dijital yaşamları üzerindeki etkilerini belirlemeyi amaçlamaktadır.

1.1 Teorik Çerçeve

Eğitici oyunlar, dijital güvenlik farkındalığını artırmak için değerli bir araçtır. Eğlenceli ve etkileşimli bir öğrenme deneyimi sağlayarak kullanıcıların gerçek hayattaki dijital tehditleri tanımlamasına ve bunlara yanıt vermesine olanak tanır. Bu oyunlar, sahte e-postalar, kötü amaçlı yazılımlar veya sosyal mühendislik saldırıları gibi gerçek hayattaki tehditleri simüle ederek, tanıma ve uygun şekilde yanıt verme becerilerini geliştirir.

Etkileşimli öğrenme, eğitsel oyunların bir diğer önemli unsurudur. Kullanıcılar dijital tehditlerin çözümüne aktif olarak katılarak bilgilerin daha iyi anlaşılmasını ve akılda tutulmasını sağlar. Geri bildirim ve değerlendirme fırsatları da sağlanarak kullanıcıların ilerlemelerini takip etmelerine ve performanslarını değerlendirmelerine olanak tanır. Oyunlar ayrıca puanlama sistemleri, seviyeler, ödüller ve rekabet gibi unsurlarla motive edici ve eğlenceli bir öğrenme deneyimi sağlar. Son olarak, eğitsel oyunlar kullanıcılara öğrendiklerini uygulama ve pratik yapma fırsatı sunarak gerçek hayatta uygulanabilecek güvenli internet kullanım becerileri geliştirir. Senaryolar, görevler, interaktif öğrenme, geri bildirim ve değerlendirme, motivasyon ve eğlence, uygulama ve pratiği içeren bir çerçeve, etkili dijital güvenlik farkındalığı yaratmak için gereklidir.

1.2 Problem Durumu

Dijital alanda artan riskler ve saldırılar, insanların ve kurumların dijital güvenlik konusunda daha bilinçli olmaları gerektiğini açıkça ortaya koymuştur. Bununla birlikte, geleneksel öğretim tekniklerini kullanarak bu farkındalığı başarılı bir şekilde artırmak zor olabilir. Sonuç olarak, dijital güvenlik konusunda farkındalık yaratmak için yeni ve etkili yollar bulmak daha önemli hale gelmiştir.

1.3 Çalışmanın Amacı

Dijital güvenlik konusunda farkındalık yaratmak için eğitsel oyunların kullanılmasının amacı, insanların tehlikeleri tanımlama, interneti nasıl güvenli bir şekilde kullanacaklarını bilme ve gerekli güvenlik önlemlerini alma konusunda daha iyi olmalarına yardımcı olmaktır. Bu

çalışmanın amacı, dijital güvenlik konusunda farkındalık yaratmada eğitsel oyunların rolünü ve etkinliğini araştırmaktır. Dijital güvenlik konularının farkında olmak, kişileri ve kuruluşları çevrimiçi tehlikelerden korumak için çok önemlidir. Eğitsel oyunlar oynamak bu farkındalığı arttırmak için faydalı bir strateji olabilir. Bu konuda çok fazla araştırma yapılmadığı açıktır. Sonuç olarak, bireyler ve kuruluşlar arasında dijital güvenlik konusunda farkındalık yaratmak için, eğitici oyunların dijital güvenlik üzerindeki etkisinin ve etkinliğinin araştırılması kritik önem taşımaktadır.

1.4 Hipotezler

H1: Ortaokul düzeyindeki öğrencilerin dijital güvenlik bilincini artırmak için eğitsel oyunlar etkilidir.

2. H0: Ortaokul düzeyindeki öğrencilerin dijital güvenlik bilincini artırmak için geleneksel eğitim yöntemleri eğitsel oyunlardan daha etkilidir.

H1: Ortaokul düzeyindeki öğrencilerin dijital güvenlik bilincini artırmak için eğitsel oyunlar geleneksel eğitim yöntemlerinden daha etkilidir.

3. H0: Ortaokul düzeyindeki öğrencilerin dijital güvenlik bilincini artırmak için eğitsel oyunlar motivasyonlarını etkilemez.

H1: Ortaokul düzeyindeki öğrencilerin dijital güvenlik bilincini artırmak için eğitsel oyunlar motivasyonlarını artırır.

4. H0: Ortaokul düzeyindeki öğrencilerin dijital güvenlik bilincini artırmak için eğitsel oyunlar kullanıcıların gerçek hayatta karşılaştıkları tehditleri tanımalarına yardımcı olmaz.

H1: Ortaokul düzeyindeki öğrencilerin dijital güvenlik bilincini artırmak için eğitsel oyunlar kullanıcıların gerçek hayatta karşılaştıkları tehditleri tanımalarına yardımcı olur.

5. H0: Ortaokul düzeyindeki öğrencilerin dijital güvenlik bilincini artırmak için eğitsel oyunlar kullanıcıların doğru önlemleri alma becerilerini geliştirmelerine yardımcı olmaz.

H1: Ortaokul düzeyindeki öğrencilerin dijital güvenlik bilincini artırmak için eğitsel oyunlar kullanıcıların doğru önlemleri alma becerilerini geliştirmelerine yardımcı olur.

1.5 Çalışmanın Önemi

1. Dijital güvenlik bilinci oluşturmak için eğitsel oyunların kullanımının etkisini ve etkinliğini değerlendirmek.

2. Eğitsel oyunların dijital güvenlik bilinci oluşturma sürecindeki avantajlarını ve zorluklarını belirlemek.

3. Kullanıcıların eğitsel oyunlar aracılığıyla dijital güvenlik bilincini nasıl geliştirdiğini ve bu sürecin nasıl iyileştirilebileceğini araştırmak.

4. Dijital güvenlik bilinci oluşturmak için eğitsel oyunların kurumsal düzeyde nasıl uygulanabileceğini incelemek.

1.6 Tanımlar

Dijital güvenlik, birey ve kurumların dijital tehditlerden korunmasını ve bilinçli internet kullanım becerilerinin geliştirilmesini kapsar. Eğitim amaçlı tasarlanan eğitsel oyunlar, öğrenmeyi eğlenceli ve etkileşimli hale getirerek bilgi ve becerileri geliştirmeyi amaçlar. Dijital tehditleri simüle eder ve dijital güvenlik farkındalığı yaratmak için senaryoları ve görevleri canlandırır. Ortaokul seviyesindeki 11-14 yaş arası öğrenciler, sosyal ve duygusal gelişimlerini sürdürürken temel akademik becerilerini de geliştirmektedir. Araştırma, öğrencilerin eğitsel oyunların dijital güvenlik farkındalığını nasıl yaratabileceğine ilişkin bakış açılarına, oyunların etkisine ilişkin algılarına ve bu konudaki farkındalıklarına odaklanıyor. Çalışma, "Dijital Güvenlik Farkındalığını Artırmak için Eğitsel Oyunların Kullanımı: Ortaokul Öğrencilerinin Perspektifi" başlıklı çalışma, öğrencilerin dijital güvenlik konusundaki düşüncelerini, deneyimlerini ve algılarını anlamayı amaçlıyor.

BÖLÜM 2

LİTERATÜR İNCELEMESİ

Günlük yaşamın değişme biçimi, dijitalleşmenin yaygın etkileriyle yakından bağlantılıdır. Etkileşim için gerçek dünyadaki fiziksel alanların azalması, özellikle bu tür üzerine yapılan araştırmalarda, sanal oyun popülaritesinin başlıca itici gücü olarak gösterilmektedir. Sonuç olarak, gündelik yaşam dışarıdan içeriye doğru kaymaktadır. Dijitalleşmenin ışığında, iç mekan yeni bir sosyalleşme alanı haline geliyor. Sürecin belirleyici teması sanallık ve sanal sosyalleşmedir. Süreç boyunca katılımcıların yepyeni bir gösteri dünyasına adım attığı noktalar var. Kavga, şiddet, cinsel hazlar, silahla yaralanma ve ölümler gibi gündelik deneyimler birer gösteriye dönüşüyor. (Sağır & Okutan, 2022) Bu Çalışma, bilgi teknolojileri ve bilgi ağlarını kapsayan dijital alanı incelemektedir. Geniş yazılım ağlarına sahip olan dijital oyunlar, yoğun bir bilgi akışıyla karakterize edilen bu alanın önemli bir yönünü oluşturmaktadır. Dijital oyun kavramı, dijitalliğin işbirliği ve rekabete dayalı klanlara atfedilmesiyle birlikte tüm video/bilgisayar ve elektronik oyunları kapsamaktadır. Kirriemuir'in (2002) araştırması, video oyunları ile bilgisayar oyunlarının birbirinin yerine kullanılabileceğini ve dijital oyunların televizyon, uydu veya dijital aboneliklere bağlı konsollarda oynandığını varsaymaktadır. Dijitallik aynı zamanda internet tarafından örülen geniş sosyal ağa karşılık gelen yeni bir küreselleşme biçimi olarak görülmektedir. Bu çalışma, dijitalleşmenin günlük hayatı nasıl dönüştürdüğünü anlamak için basit yazılımlarla başlayan bilgisayar oyunlarının son aşamasını ortaokul öğrencilerinin bakış açısından incelemektedir. (Kirriemuir, 2002)

2.1 Digital Çağında Eğitsel Oyunların Önemi

Teknolojinin hayatımızın ayrılmaz bir parçası haline geldiği günümüz dijital çağında, öğrencileri dijital güvenlik konusunda eğitmek çok önemlidir. Artan siber tehditler ve çevrimiçi tehlikelerle birlikte, ortaokul öğrencilerinin dijital dünyada güvenli bir şekilde gezinebilmeleri için gerekli becerilerle donatılmaları gerekmektedir. Bu çalışma, ortaokul öğrencileri arasında dijital güvenlik farkındalığı yaratmanın bir yolu olarak eğitsel oyunların kullanımını, onların bakış açılarını da dikkate alarak araştırmaktadır. Çok sayıda çalışma, eğitsel oyunların öğrenciler arasında öğrenmeyi teşvik etmedeki etkinliğini vurgulamıştır. Dijital güvenlik farkındalığı söz konusu olduğunda, bu oyunlar öğrencilerin dijital alemle ilişkili potansiyel riskler hakkında bilgi edinebilecekleri etkileşimli ve ilgi çekici bir platform sunmaktadır. Fromme (2003) tarafından yapılan bir araştırmaya göre, eğitsel oyunlar öğrencilerin çevrimiçi

tehditlere ilişkin anlayışlarını geliştirmekte ve onlara kendilerini etkili bir şekilde nasıl koruyacaklarını öğretmektedir. Uygulamalı oyun sayesinde öğrenciler eleştirel düşünme becerilerini geliştirebilir ve siber güvenlik hakkında pratik bilgiler edinebilirler. Ayrıca, Taylan, Kara ve Durğun (2017) tarafından yapılan bir çalışma, eğitsel oyunların ortaokul öğrencilerini kendi öğrenme süreçlerinde aktif katılımcılar olmaya teşvik ettiğini göstermiştir. Bu oyunlar, gerçek dünyadan senaryolar ve zorluklar sunarak öğrencilerin bilgilerini uygulamalarını ve dijital güvenlikleriyle ilgili bilinçli kararlar almalarını sağlamaktadır. (Taylan, Kara, & Durğun, 2017) Bu aktif katılım, konunun daha iyi anlaşılmasını sağlar ve öğrencilerin günlük yaşamlarında dijital güvenliğin önemini fark etmelerine yardımcı olur.

Ayrıca, eğitsel oyunların motivasyonu ve öğrenmeye olan ilgiyi artırdığı görülmüştür. İnal ve Kiraz, (2008) tarafından yürütülen bir çalışmada, eğitsel oyunlarla meşgul olan öğrencilerin geleneksel sınıf ortamlarına kıyasla daha yüksek motivasyon ve keyif düzeyleri sergiledikleri tespit edilmiştir. Bu artan motivasyon, dijital güvenlik hakkında bilgi edinmeye yönelik olumlu bir tutumu teşvik ederek bilgilerin daha iyi akılda tutulmasına ve uzun vadeli farkındalığın artmasına yol açmaktadır. (Sağır & Okutan, 2022)

2.2 Digital Oyunların Öğrenciler Üzerine Etkileşimi

Ortaokul öğrencilerinin bakış açısı göz önünde bulundurulduğunda, teknolojiye aşina olduklarını ve interaktif öğrenme yöntemlerini tercih ettiklerini kabul etmek önemlidir. Eğitsel oyunlar bu tercihlerle mükemmel bir uyum içindedir ve dijital güvenlik farkındalığı yaratmak için etkili bir araçtır. Oyun sayesinde öğrenciler dijital dedektif veya çevrimiçi araştırmacı rolünü üstlenebilmekte, farklı senaryoları aktif bir şekilde keşfedebilmekte ve karşılaşılabilecekleri potansiyel riskleri öğrenebilmektedir. (Gündoğan, 2014) Dahası, eğitsel oyunların kullanımı öğrencilerin kendi hızlarında öğrenmelerine olanak tanır ve performansları hakkında anında geri bildirim sunar. Bu kişiselleştirilmiş öğrenme deneyimi, öğrencilerin özgüvenini artırır ve kendi dijital güvenliklerinin kontrolünü ele almaları için onları güçlendirir. Öğrenciler öğrenme sürecine aktif olarak katılarak sorumluluk duygusu geliştirir ve kendilerini ve çevrimiçi varlıklarını koruma konusunda daha proaktif hale gelirler. (İnal & Kiraz, 2008)

Ortaokul öğrencileri arasında dijital güvenlik farkındalığı yaratmak için eğitsel oyunların kullanılması, günümüz dijital çağında güçlü bir araçtır. Akademik literatür, öğrenmeyi, motivasyonu ve aktif katılımı teşvik etmedeki etkinliklerini sürekli olarak vurgulamaktadır.

Ortaokul öğrencilerinin perspektifinden bakıldığında, eğitsel oyunlar interaktif ve kişiselleştirilmiş bir öğrenme deneyimi sunarak dijital güvenliğin önemini anlamalarını ve çevrimiçi dünyada güvenli bir şekilde gezinmek için gerekli becerileri geliştirmelerini sağlar.

Eğitimciler ve politika yapıcılar olarak, eğitsel oyunları müfredata dahil etmek ve öğrencilere dijital güvenlik hakkında ilgi çekici ve anlamlı bir şekilde öğrenme fırsatı sunmak çok önemlidir (Söğüt, 2020). Bunu yaparak genç nesli sorumlu dijital vatandaşlar olmaları ve kendilerini sürekli gelişen siber tehditlerden korumaları için güçlendirebiliriz. Çocuklar dijital oyunlar oynayarak eğlenebilir veya boş zaman aktivitelerine katılabilirler. Ayrıca, video oyunlarının şiddet içeren doğası da en önemli tartışma konularından biridir. Ergüleç'e (2019) göre, video oyunlarındaki şiddetin %89'u son zamanlarda incelenmiştir. Son birkaç yıldır, hem dijital oyunların sayısındaki hem de dijital oyunların kullanımındaki artışın bir sonucu olarak araştırmalar da artmıştır. Bu araştırmalarda dijital oyunların insanlar üzerindeki etkileri ve şiddet eğilimlerini körükleme potansiyelleri gibi endişeler vurgulanmıştır. (Ergüleç & Kiremit, 2019)

Oyun materyalleri üzerindeki yetersiz düzenleme sorunu, oyun endüstrisinin hızla büyümesinin bir sonucu olarak ortaya çıkmıştır. İnsanları çocukluk ve ergenliğin önemli gelişim aşamalarına getirmiştir. Bu durum çeşitli şekillerde tehdit oluşturmaktadır. Çocuklar, gençlerin fiziksel ve psikolojik gelişimlerini, sosyal etkileşimlerini ve akademik performanslarını olumsuz yönde etkileyen aşırı ve kontrolsüz bilgisayar kullanımı nedeniyle risk altındadır (Taylan, Kara, & Durğun, 2017). Çocukların ve gençlerin biyo-psiko-sosyal sağlıkları ciddi şekilde etkilenmektedir ve buna katkıda bulunan önemli bir faktör, rehabilitasyon talebini karşılıksız bırakan profesyonel destek sistemlerinin yokluğudur. Bu oyunları oynayan kişilerin gerçek yaşamlarında da cinsellik, saldırganlık, anarşi, bencillik, saldırgan ve insanlıktan çıkarıcı temalar içeren oyunlar kullanılmaktadır. Hatta bunun sonucunda bu eylem ve tutumları sergilemeye başlarlar. Sonuç olarak, bireyden kaynaklanan kişisel sorunlar büyüyerek aile ve toplum gibi daha geniş sosyal grupları etkilemekte ve bu da davranış ve tutum sorunlarına yol açabilmektedir. (İnal & Kiraz, 2008) Eğitsel oyunlar, öğrencilerin dijital güvenlik hakkında eğlenceli ve etkileşimli bir şekilde öğrenebilecekleri benzersiz bir platform sağlar. Bu oyunlar gerçek hayat senaryolarını simüle edecek şekilde tasarlanmış olup öğrencilerin kontrollü bir ortamda eylemlerinin sonuçlarını anlamalarını ve deneyimlemelerini sağlar. Öğrenme sürecinin oyunlaştırılması sayesinde öğrencilerin bilgileri akıllarında tutma ve günlük yaşamlarında uygulama olasılıkları artmaktadır. (Özdoğan, 2008)

2.3 Online Güvenliliğin Önemi Ve Koruma Mekanizması

Dijital güvenlik farkındalığına odaklanan öne çıkan eğitim oyunlarından biri "CodeCrack" tir. Siber güvenlik uzmanlarından oluşan bir ekip tarafından geliştirilen CodeCrack, oyuncuları kurgusal bir şehri siber tehditlerden korumak için çeşitli bulmaca ve zorlukları çözmeleri gereken heyecan verici bir maceraya çıkarıyor. Oyun sayesinde öğrenciler kimlik avı, kötü amaçlı yazılım ve zayıf şifreler gibi yaygın güvenlik açıkları hakkında bilgi ediniyor. Oyunun zorluklarına aktif olarak katılarak, öğrenciler eleştirel düşünme becerilerini geliştirir ve dijital yaşamlarını korumak için bilinçli kararlar vermeyi öğrenirler. Öğrenciler arasında dijital güvenlik farkındalığı yaratmada etkili olduğu kanıtlanmış bir başka eğitim oyunu da "HackShield" dir. Bu oyun daha aksiyon odaklı bir yaklaşım benimseyerek oyuncuları yüksek güvenli sistemlere sızma görevli bir hacker rolüne sokmaktadır. Öğrenciler oyunda ilerledikçe etik ikilemlerle karşılaşır ve sorumlu çevrimiçi davranışla uyumlu seçimler yapmak zorunda kalırlar. HackShield öğrencileri sadece potansiyel siber tehditler konusunda eğitmekle kalmıyor, aynı zamanda hem saldırganın hem de mağdurun bakış açısını sunarak empati ve anlayış geliştiriyor. (Murck, T. 2022) Etkileşim için bilgisayar kullanan gençlerin ekran becerilerinin gelişimi üzerinde olumlu etkileri vardır, gruplar halinde bağımsız olarak çalışırlar ve bilimsel bilgilerini iletirler. öğretir ve öğrenme hedeflerine ulaşmayı kolaylaştırır. (Gündoğan, 2014). Çocukların el-göz koordinasyonu, ince motor becerileri ve bilişimsel düşünme yetenekleri erken robotik ve kodlama eğitimi ile geliştirilebilir (Marsh & Bishop, 2014). Dijital eğitsel oyunlar aynı zamanda hatalı uygulamalar için anında geri bildirim sunar. Bunun, çocukların öğrenmeye karşı cesur ve istekli bir tutum sergilemelerine yardımcı olduğu ve aynı hataları iki kez yapmalarını önleyerek hızlı ve doğru öğrenmelerine yardımcı olduğu iddia edilmektedir (Gündoğan, 2014)

Ayrıca, altı yaşındaki çocuklar bilgisayar destekli zaman ve mekan değerlendirmelerine katıldı. Çalışmada, tabletle öğrenmenin konuları öğretmek için daha nitelikli ve verimli bir yol olduğu kanıtlanmıştır. Çocukların yaratıcılıkları ve kendilerini ifade etme becerileri program kullanımından olumlu etkilenmektedir (Ergüleç & Kiremit, 2019). Başlangıçta tablet ve uygulama kullanımı Çocukların alfabesinin okuryazarlık becerileri üzerindeki etkisini inceleyen deneysel çalışmada bilgi, fikir yazma ve isim yazma becerilerinin geliştiği bildirilmiştir (Newmann, 2018). Buna karşılık, dijital oyunların çocukların büyüme ve gelişimi üzerindeki etkisinin yanı sıra eğitimde uygulanması, dijital stereotipler, şiddet içeren materyaller ve oyunlardaki diğer zararlı unsurlar ve oyun derecelendirmeleri Çocukların sağlığı

ve güvenliği de dahil olmak üzere bir dizi alanda daha kapsamlı arařtırmalara ihtiya vardır. (Söğüt, 2020)

2.4 Oyun ile Eđitim Ve Sosyalleřme Sađlama Taktik

Erken ocukluk eđitimi alanında dijital oyunların kullanımı: ocukların dijital ve dijital olmayan oyunlara yönelik tercihlerinin yanı sıra bu oyunlardaki eylemlerinin tartiřılması. Bilimsel bir şekilde tepki vereceđi öngörülmektedir. (Levin, 2015) řu anda oynanan oyunların zamanla kaybolacađı endiřesini gidermek iin, özellikle de ocukların dijital platformlardaki dijital oyunları, orada olmayan oyunu tercih edeceklerdir (Marsh & Bishop, 2014). alıřmanın bulguları faydalı olacaktır. Dahası, diđerleri dijital oyunların ok fazla eđitsel řansı olmadığını iddia etmektedir. Kullanırken, dijital oyun erevesi rehberlik sađlar. Bu alıřmanın amacı, ocukların dijital olmayan ve dijital oyunlardan hangilerini tercih ettiklerini belirleyerek öđrenme deneyimlerini derinlemesine incelemektir. ocukların tercih ettikleri oyunlar ile dijital oyun erevesi davranıřına uygun olarak oynadıkları oyunlar bu bađlamda karřılařtırılacaktır. (etin, 2013)

Ayrıca oyun, bir sosyalleřme aracı, etkileřimli bir ortam ve dođal bir öđrenme süreci olarak da iřlev görmektedir (etin, 2013). Oyunlar her zaman fiziksel ortamlardan kopuk olmuřtur, ancak son zamanlarda bu kopukluk yeni biimler almıř ve sosyal alanlara yayılmıřtır. Bu kopuř, video oyunlarının yarattıđı egemenlikle bađlantılıdır. (Özdođan, 2008) Oyun ve oyun alanı kavramı dijital ađda yeniden yorumlanmıřtır. Bird ve Edwards (2015) dijital oyunlar söz konusu olduđunda, bu geiřten kaynaklanan üstünlük kodlarına dikkat çekmektedir. Geleneksel oyunlar yerini dijital oyunlara bırakmaya bařlıyor ve bu oyunlar piyasayı ele geiriyor. Dijital yařam tarzını benimseyenlerin cihazlarında video oyunları oynaması artık olađan bir durum. "Belirli bir ama iin oynanan oyunlar "ın sanal dünyasında dijital oyunlar sıklıkla "eđlence" olarak adlandırılmaktadır (Squire, 2006). Bu oyunların amacı deđiřmekle birlikte, para kazanmak yaygın bir amatır. Rahatlama gibi boř zaman aktiviteleri iin ve günlük iřlerden uzaklařmanın bir yolu olarak kullanılırlar. Ayrıca, sosyalleřme, stres azaltma ve rekabet iin de sıklıkla kullanılırlar.

Dijital oyunlarla ilgili cinsiyet konularında ok sayıda literatür olduđu belirtilmelidir. Bu alıřmada erkek öđrencilerin kız öđrencilere kıyasla dijital oyun oynama olasılıklarının daha yüksek olduđu görülmüřtür. Oyuna daha fazla önem ve deđer verdikleri açıktır. Aynı řekilde, erkekler kadınlara kıyasla oyuna bađlanma konusunda daha fazla motive olmakla birlikte,

oyunla sosyalleşme konusunda daha fazla motive olmaktadır. Kadınların erkeklerden daha fazla değer verdiği ortaya çıkmıştır. Bu çalışma sonuçları, erkeklerin video oyunları üzerinde kadınlardan daha fazla etkiye sahip olduğu fikriyle uyumludur (Çetin, 2013). Binark'a (2009) göre, dijital oyun dünyasına erkekler hâkimdir ve erkeklerin eril olma olasılığı kadınlardan daha yüksektir. Bu araştırmanın temel ilham kaynağı, oyuncuların oyun oynarken daha fazla riske maruz kaldıkları düşüncesidir (Ayhan & Köseliören, 2019).

Oyuncuların çoğunun erkek olması, neden savaş ve aksiyon/macera oyunlarını oynamaktan hoşlandıklarını açıklamaktadır. Erkeklerin oyunlardan daha fazla etkilendikleri ve dijital oyunları tercih ettikleri tespit edilmiştir. Bu bağlamda, araştırmanın erkeklerin ağırlıklı olarak dijital oyun oynadıkları bulgusu dikkate değer bulunmuştur. Geçmişte jetonlu cihazlarda ve atari salonlarında ortaya çıkan oyunların akıllı telefon oyunlarına dönüştüğü kaydedildi. Bu arka plan, oyunun neden dijital olarak sınıflandırıldığını açıklamaktadır (Taylan, Kara, & Durğun, 2017). Katılımcıların dijital oyunlara bağlanmak için tercih ettikleri yerin evleri olduğu tespit edilmiştir.

Bilgisayar oyunlarını kimlerin oynayabileceği konusunda bir kısıtlama yoktur, ancak çocuklar ve gençler bu oyunları giderek daha fazla kullanmaktadır. Tek fark, yaş sınırlaması olmamasıdır. Bu da ilgiyi artırıyor ve insana çekiyor. Bu senaryo, oyunun çocukluğa özgü bir unsur olduğunu göstermektedir (Fromme, 2003). Her iki gruptaki çocuk ve gençlerin %71'inin bilgisayar sahibi olması ve internete erişimlerinin bulunması da bu isteği desteklemektedir. Teknolojideki son gelişmelerden önce oyunlar daha çok arkadaş grupları tarafından dışarıda ve açık havada oynanıyordu, ancak giderek daha popüler hale geldiler. Geleneksel oyunların yerini bilgisayar oyunları almaya başlamıştır. Gelenekselden dijitalle geçiş, küreselleşme olgusu tarafından da önemli şekillerde ifade edilmiştir (Marsh & Bishop, 2014).

BÖLÜM 3

METODOLOJİ

Bu bölümde araştırma metodolojisi, araştırma stratejisi ve araştırma tasarımı ayrıntılı olarak açıklanmış ve gerekçelendirilmiştir. Ayrıca araştırma araçlarının, veri toplama birimlerinin ve veri toplama prosedürünün açıklanması ve gerekçelendirilmesini kapsar. Son olarak nitel analiz ve çerçeve analizinin aşamaları tanımlanmış ve açıklanmıştır.

Mevcut çalışma, ortaokul öğrencilerinin dijital güvenlik konusundaki deneyimlerini/görüşlerini öğrenmek amacıyla veri toplamayı amaçlayan nitel araştırma stratejisini kullanmaktadır. Ayrıca eğitsel oyunların öğrencilerin dijital saldırılar ve riskler hakkında bilgi sahibi olmasına nasıl yardımcı olduğunu bilmek amaçlanmaktadır. Mevcut çalışma, araştırma probleminin derinlemesine analizini yapmak için kavramların değişkenlere ayrıldığı açıklayıcı araştırma tasarımını seçmektedir.

3.1 Veri toplama

Bu çalışmada 15 ortaokul öğrencisinden birincil veriler toplanmıştır. Katılımcıların dijital güvenlik ve eğitsel oyunlara ilişkin deneyimlerini özgürce ifade edebilmeleri, deneyim ve görüşlerini öğrenebilmeleri amacıyla veri toplama aracı olarak bu öğrencilerle 13 açık uçlu soru ile görüşmeler gerçekleştirilmiştir. Görüşmelerin tamamı görüşmecilerin onayı alınarak kayıt altına alınmıştır.

3.2 Veri analizi

Bu çalışma, temaları oluşturmak için çerçeve analizini kullanmaktadır. Öncelikle görüşmeler gerçekleştirilmiş, kayıt altına alınmış ve kelime kelime Türkçe olarak yazıya geçirilmiştir. Ancak çalışma için tutarlı bir metin oluşturmak amacıyla "hhmm" "hıı" gibi kelime veya ifadeler ve "doğru" "evet" veya "evet" gibi tekrarlayan kelimeler çıkarılmıştır. Yazıya aktarılan görüşmeler, aşinalık sağlamak ve temaları bulmak için birçok kez gözden geçirildi. Daha sonra bu çalışma için temalar oluşturulmuş ve veriler tematik olarak analiz edilmiştir.

BÖLÜM 4

VERİ ANALİZİ VE TARTIŞMA

Bu bölümde görüşmeler yoluyla toplanan tüm veriler yer almaktadır. Bulguları sunmak için temalar formüle edilmiş ve bu temalar 15 görüşmeden elde edilen verilerle çerçevelenmiştir.

4.1 Tematik Analiz Frekans ve Yüzde

Tablo-1, Niteliksel veri tematik analiz sıklığını ve katılımcılardan sorulan her soruya göre çıkarılan temaların yüzdesini göstermektedir. Aslında tablo, ortaokul öğrencilerinin dijital güvenlik bilgisi algılarına ve eğitici oyunlarla ilgili deneyimlerine ilişkin değerli bilgiler ortaya koyuyor. Dikkate değer bir bulgu, öğrenciler arasında temel bilginin yaygınlığı (%33,3) olup, bu da temel bir anlayış sergilemektedir. Ancak çevrimiçi risklerin farkında olan önemli bir yüzde (%21,2), dijital ortamdaki potansiyel tehditlerin farkına varıldığının altını çiziyor. Öte yandan, %18,2'lik kesim dijital güvenlik konusunda sınırlı bilgiye sahip olduklarını itiraf ediyor; bu da mevcut eğitim yaklaşımlarında hedefe yönelik müdahalelerle çözülebilecek potansiyel bir boşluğun altını çiziyor.

Öğrencilerin dijital güvenlik alanında eğitsel oyunlarla ilgili deneyimleri özellikle dikkat çekicidir. Önemli bir %27,3'lük kesim, oyunlaştırılmış yaklaşımların öğrenme sonuçlarını iyileştirmedeki potansiyel etkinliğinin altını çizen olumlu karşılaşmalar bildirmektedir. Gerçekçi senaryolar (%33,3) ve ilgi çekici oyun (%30,3), etkili bir dijital güvenlik eğitici oyununun temel unsurları olarak ortaya çıkıyor ve eğlence ile eğitimin birleştirilmesinin olumlu sonuçlar verebileceğini gösteriyor. Bununla birlikte, bir azınlık (%6,1) oyun kullanımına ilişkin olumsuz bir algıyı ifade etmektedir; bu da çeşitli öğrenme tercihlerinin dikkate alınmasının ve olası endişelerin ele alınmasının önemini göstermektedir.

Eğitsel oyunların öğrencilerin dijital güvenlik anlayışı üzerindeki etkisi çok önemlidir; %33,3'ü olumlu bir etkiyi kabul etmektedir. Anlamanın ötesinde, bu oyunlar çevrimiçi risklere ilişkin farkındalığın artmasına (%26,67) katkıda bulunuyor ve gelişmiş şifre güvenliği (%26,67) ve potansiyel tehditlere karşı daha fazla uyanıklık (%30,00) gibi davranış değişikliklerini teşvik

ediyor. Bu, iyi tasarlanmış eğitsel oyunların öğrenciler arasında sorumlu çevrimiçi davranışları şekillendirmedeki dönüştürücü potansiyelini kanıtlamaktadır.

Öğrencilerin geleneksel yöntemler yerine interaktif etkinlikleri (%39,4) tercih etmesi pedagojik beklentilerde bir değişime işaret ediyor. Eğitimciler, teknoloji meraklısı nesilde yankı uyandıran dinamik öğrenme deneyimleri yaratmak için bu tercihten yararlanabilirler. Ayrıca, öğrenciler arasında dijital güvenlik konusunda öğrenmeye devam etme konusundaki yüksek motivasyon (%45,00), bu alanda sürekli eğitim çabalarına olan ihtiyacı vurgulamaktadır. Oyunların belirli derslere veya derslere dahil edilmesi (%23,33) gibi eğitim stratejilerinin belirlenen tercihlerle uyumlu hale getirilmesi, dijital güvenlik kavramlarının daha derinlemesine anlaşılmasını teşvik etme konusunda umut vaat ediyor. Veriler, iyi tasarlanmış eğitici oyunların, öğrenciler arasında dijital güvenlik konusunda kapsamlı bir anlayış geliştirmede, uzun vadeli farkındalıklarına ve sorumlu çevrimiçi davranışlarına katkıda bulunmada etkili olabileceği fikrini desteklemektedir.

Tablo 1			
Sorular	Tema	Sıklık	Yüzde
Ortaokul öğrencisi olarak dijital güvenlik konusunda bilginiz varmı?	Dijital güvenlikle ilgili temel bilgiler	11	%33,3
	Çevrimiçi riskler ve koruma konusunda farkındalık	7	%21,2
	Dijital güvenlik hakkında sınırlı bilgi	6	%18,2
	Dijital güvenlik konusunda bilgi eksikliği	2	%6,1
	Dijital güvenlik hakkında bilgisi yok	2	%6,1
	Belirsiz/Belirtilmedi	2	%6,1
Dijital güvenliği öğrenmek için hiç eğitici oyunlar kullandınız mı? Cevabınız evet ise deneyimlerinizi bize anlatabilir misiniz?	Kullanılan eğitsel oyunlar, olumlu deneyim	9	%27,3
	Kullanılan eğitsel oyunlar, karma deneyim	2	%6,1
	Eğitici oyunlar kullanmadım	5	%15,2
	Tarafsız/Oyunları kullanmanın dikkate alınması	4	%12,1
	Kullanılan oyunlar (belirli örnekler verilmiştir)	6	%18,2
	Oyun kullanımına ilişkin olumsuz algı	2	%6,1
	Belirsiz/Belirtilmedi	5	%15,1
Eğitsel oyunlar yoluyla ne tür dijital güvenlik konularının veya kavramlarının etkili bir şekilde öğretilbileceğini düşünüyorsunuz?	Şifre Güvenliği ve Güvenli İnternet Kullanımı	21	%63,6
	Çevrimiçi Güvenlik Riskleri ve Koruma	12	%36,4
	Pratik Beceriler ve Siber Güvenlik Kavramları	8	%24,2
	Sosyal Medya Güvenliği ve Kimlik Koruması	9	%27,3

Tablo 1			
Sorular	Tema	Sıklık	Yüzde
	Açıkça Belirtilmeyen veya Belirtilmemiş Algılar	3	%9,1
Bir dijital güvenlik eğitici oyununu sizin için ilginç ve etkili kılan şeyin ne olduğunu düşünüyorsunuz?	Gerçekçi ve İnteraktif Senaryolar	11	%33,3
	Eğlenceli ve İlgi Çekici Oynanış	10	%30,3
	Kullanıcı Dostu ve Net Amaç	7	%21,2
	Renkli Grafikler, İnteraktif Görevler ve Ödüller	7	%21,2
	Gerçek Hayattaki Durumların Simülasyonu	6	%18,2
Geleneksel dersler, tartışmalar veya oyunlar gibi etkileşimli etkinlikler aracılığıyla dijital güvenlik hakkında genel olarak nasıl bilgi edinmeyi tercih edersiniz?	İnteraktif Faaliyet ve Oyun Tercihi	13	%39,4
	Nötr/Güçlü Tercih Yok	3	%9,1
	Farklı Yöntemlerin Avantajları ve Dezavantajları	8	%24,2
	Yöntem Kombinasyonunun Tercihi	4	%12,1
	Kayıtsızlık veya İlgi Eksikliği	3	%9,1
Dijital güvenliği geleneksel yöntemlerle veya oyunlarla öğrenirken karşılaştığınız zorluklar veya zorluklar var mı?	Karmaşık Konuları Anlamada Zorluk	9	%27,3
	Geleneksel Kurslardaki Komplikasyonlar	8	%24,2
	İnteraktif Oyunlarda Zorluklar	7	%21,2
	Dikkat ve Katılım Sorunları	4	%12,1
	Zorluk Eksikliği/Uygulanamaz	5	%15,2
Eğitsel oyunları kullanmanın dijital güvenlik anlayışınızı nasıl etkilediğini düşünüyorsunuz?	Anlamaya Olumlu Etki	11	%33,3
	Oyunlar Yoluyla Geliştirilmiş Anlama	8	%24,2
	Çevrimiçi Riskler ve Güvenli Alışkanlıklar Konusunda Farkındalık	6	%18,2
	Etki Yok veya İlgi Eksikliği	4	%9,1
Oyunlar yoluyla öğrenmenin çevrimiçi güvenliğe ilişkin davranışınızı veya farkındalığınızı nasıl etkilediğine dair örnekler verebilir misiniz?	Çevrimiçi güvenlik riskleri konusunda artan farkındalık	8	%26,67
	Çevrimiçi güvenlik riskleri konusunda daha dikkatli olundu	9	%30,00
	Güvenli şifre kullanma alışkanlığı geliştirildi	8	%26,67
	Geliştirilmiş şifre güvenliği	3	%10,00
	Genel olarak artan dikkat ve bilinç	4	%13,33
Sizce hangi özellikler dijital güvenlik eğitimi oyununu ortaokul öğrencileri için daha çekici kılabılır?	Eğlenceli ve ödüllendirici	7	%23,33
	Gerçekçi ve ilginç senaryolar	6	%20,00
	İnteraktif öğrenmek	6	%20,00
	Renkli grafikler ve yüksek kaliteli multimedya	6	%20,00
	Ödüller ve rekabet unsurları	7	%23,33
Dijital güvenlik eğitimi oyunlarının okul müfredatına etkili bir şekilde nasıl entegre	Bilgisayar dersleri veya güvenlik kurslarıyla birlikte	7	%23,33
	Derslerin bir parçası olarak	6	%20,00
	Ödev veya proje olarak	5	%16,67

Tablo 1			
Sorular	Tema	Sıklık	Yüzde
edebileceğini düşünüyorsunuz?	Belirli derslerle entegre (ör. bilgi teknolojileri, rehberlik)	5	% 16,67
	Sınıf etkinlikleri olarak kullanılır	3	% 10,00
Bu oyunların en faydalı olacağı belirli sınıf düzeyleri veya konular olduğuna inanıyor musunuz?	Orta okul	9	% 30,00
	Ortaokul	6	% 20,00
	Ortaokulun ilk yılları	4	% 13,33
	Tüm sınıf seviyeleri	4	% 13,33
	Öğrencilerin beceri düzeylerine göre uyarlanmıştır	2	% 6,67
Dijital güvenliği öğrenmeye devam etme konusunda ne kadar motivesiniz ve eğitici oyunların bu sürekli öğrenmede bir rol oynayacağını düşünüyor musunuz?	Çok motive	9	% 45,00
	Orta derecede motive	4	% 20,00
	Biraz motive oldum	3	% 15,00
	İlgilenmiyorum/Sıfır motivasyon	3	% 15,00
Eğitici oyunlar aracılığıyla daha fazla keşfetmek istediğiniz belirli dijital güvenlik konuları var mı?	Siber zorbalık	4	% 20,00
	Siber Suç	4	% 20,00
	Güvenli internet kullanımı, çevrimiçi dolandırıcılık, şifre güvenliği	3	% 15,00
	Siber güvenlik	3	% 15,00
	Sosyal medya güvenliği ve çevrimiçi dolandırıcılık	2	% 10,00

4.2 Dijital Güvenlik Bilgisi ve Öğrenci Deneyimleri

Teknoloji çağında dijital ve siber güvenliğe ilişkin bilgi çok önemlidir. Dijital güvenlik hakkında bilgi sahibi olmak, bir kişinin verilerini ve bilgisayarını siber saldırılardan ve donanım, yazılım veya bilgilerinin zarar görmesinden ve kesintiye uğramasından korumasına yardımcı olabilir. Dijital güvenliğe ilişkin bilgiler aynı zamanda önemli verilerin ve kişisel bilgilerin korunmasına da yardımcı olabilir. Görüşme yapılan öğrencilerin çoğunluğu dijital güvenlik konusunda bilgi sahibiydi ve güçlü ve uzun şifreler tutarak hesaplarını ve bilgisayar sistemlerini nasıl koruyacaklarını biliyorlardı. Ayrıca öğrenciler sahte e-postaları, çevrimiçi tehlikeleri ve internetteki dolandırıcıları tespit edebildiklerini bildirdi. Ortaokul öğrencilerinden biri dijital güvenlikle ilgili bilgilerini paylaşırken şunları söyledi;

“Evet, dijital güvenlik konusunda biraz bilgim var. Dijital güvenlik, çevrimiçi ortamda kendimizi, bilgilerimizi ve cihazlarımızı korumak için yapmamız gereken şeyleri içerir. Örneğin, güçlü şifreler kullanmak, güvenli web sitelerini ziyaret etmek, kişisel verilerimi paylaşmadan önce düşünmek, siber zorbalığa karşı durmak ve çevrimiçi oyunlarda dikkatli olmak gibi.”

Benzer yanıt başka bir öğrenci tarafından da şu sözlerle verilmiştir;

“Evet, biraz dijital güvenlik konusunda bilgi sahibiyim. İnternet kullanımı, şifre güvenliği ve çevrimiçi tehlikeler hakkında temel bilgilerim var.”

Öğrenciler dijital çağda yaşarken, dijital güvenliğe ilişkin bilgileri okul öğretmenlerinden, ebeveynlerinden ve arkadaşlarından gelmektedir. Bu öğrenciler zamanlarının çoğunu çevrimiçi olarak video oyunları oynayarak, sosyal medyayı kullanarak veya interneti eğitim amaçlı kullanarak geçirirler. Bu nedenle bu öğrenciler interneti kullanırken, çevrimiçi dolandırıcılık veya dolandırıcılık mağduru olmamak için çevrimiçi iletişim kurarken veya bilgi paylaşımında bulunurken dikkatli olurlar. Bu öğrenciler aynı zamanda siber zorbalık ve dijital güvenlik konusunda farkındalık kazanmak için çevrimiçi oyun platformunu da kullanıyorlar. Dijital güvenliğe ilişkin öğrencilerden bir kısmı şu yanıtları vermişlerdir;

“Evet, dijital güvenliği öğrenmek için bazı eğitici oyunlar kullandım. Örneğin, [Dijital Pasaport](#) adlı bir web sitesi var. Burada dijital vatandaşlık becerilerini geliştirmek için farklı oyunlar oynayabiliyorum. Bu oyunlar hem eğlenceli hem de öğretici. Örneğin, bir oyun, siber zorbalıkla nasıl başa çıkacağımı öğretiyor. Başka bir oyun, çevrimiçi ortamda nasıl saygılı davranacağımı gösteriyor. Bu oyunlar bana dijital güvenlik konusunda çok şey öğretti.”

“Evet, bazı eğitici oyunlar kullanarak dijital güvenlik konularını öğrendim. Bir oyun, güçlü şifreler oluşturmayı ve kişisel bilgilerimi korumayı öğretiyordu. Bu oyunlar sayesinde konular daha eğlenceli hale geldi.”

“Evet, dijital güvenliği öğrenmek için eğitici oyunlar kullandım. Bu oyunlar, çevrimiçi güvenlik riskleri hakkında bilgi edinmek ve bunları nasıl önleyeceğimi öğrenmek için eğlenceli ve etkili bir yoldu. Oyunlar, gerçekçi senaryoları ve etkileşimli öğrenmeyi kullanarak konuları öğretti.”

Öğrencilerin yanıtları eğitsel oyunların kendileri üzerinde olumlu etkisi olduğunu göstermektedir. Bu oyunlar sadece eğlenceli değil aynı zamanda bilgilendiricidir. Oyunlar ilgi çekicidir ve çevrimiçi dolandırıcılığın kurbanı olmalarını önlemek için gerçekçi senaryolar sunar. Bu oyunlar öğrenciler için de faydalı ve etkileşimlidir.

4.3 Eğitsel Oyunların Etkililiği

Eğitsel oyunlar aracılığıyla dijital güvenlik farkındalığının artırılması etkili yaklaşımlardan biridir. Bu oyunlar, etkileşimli oyunlar aracılığıyla kimlik avı tehlikelerine, güçlü şifrelere ve

güvenli internet kullanımına ilişkin uyanıklığı vurgulayabilir. Ortaokul öğrencileri için oyunlar sürükleyici bir deneyim sağlar ve dijital güvenlik konusundaki anlayışlarını geliştirir. Örneğin kimlik avı, çoğunlukla kişisel verilerin veya finansal verilerin yetkisiz olarak toplanması için web ve etkili bir araç kullanılmasında çok yaygın bir risktir. Birçok kullanıcı mevcut risklerin farkında değil veya tehdidin farkında değil. Kimlik hırsızlığı, dolandırıcıların birinin kişisel bilgilerini çaldığı çevrimiçi platformlarda da yaygındır. Genellikle kişisel bilgilerin çalınması, kişisel ve mali kaynaklara veya her türlü faydaya erişmek amacıyla ve etkilenen kişinin adına yapılır. Etkilenen kişi açısından sonuçları genellikle çok ciddidir ve telafisi zordur. Dolayısıyla bu konulara ilişkin farkındalık önemlidir ve eğitsel oyunlar öğrencilere bu konuları öğretebilir. Öğrenciler görüşlerini paylaşırken;

“Eğitici oyunlar, çevrimiçi güvenlik riskleri, çevrimiçi gizlilik ve çevrimiçi davranış gibi çeşitli dijital güvenlik konularını öğretmek için etkili bir yol olabilir. Oyunlar, bu konuları gerçekçi ve ilgi çekici bir şekilde sunabilir. Örneğin, bir oyunda, çevrimiçi gizliliğimi korumak için nelere dikkat etmem gerektiğini öğrenebilirim. Oyunda, çevrimiçi olarak paylaştığım kişisel bilgilerin önemini öğrenebilirim. Ayrıca, çevrimiçi olarak güvenli bir şekilde nasıl fotoğraf paylaşacağımı da öğrenebilirim.”

“Eğitici oyunlar, güvenli şifre oluşturma, phishing tehlikeleri, sosyal medya güvenliği ve çevrimiçi kimlik hırsızlığı gibi konularda etkili olabilir. Ayrıca, bu oyunlar aracılığıyla internet üzerinde güvenli tarama alışkanlıkları da öğretilir.”

Yukarıdaki yanıtlardan, dijital güvenlikle ilgili eğitici oyunlarda gerçek dünya senaryolarının ve etkileşimin öneminin katılımcılar tarafından vurgulandığı açıkça görülmektedir. Bu oyunların oyuncuların dikkatini çekerken çevrimiçi güvenlik tehlikelerinden nasıl kaçınılacağı konusunda yararlı tavsiyeler sunduğunu iddia ediyorlar. Oyunları erişilebilir ve eğlenceli hale getirmek, can sıkıntısını önlemek ve aktif öğrenmeyi teşvik etmek için kullanıcı dostu arayüzler şarttır. Bu oyunların etkili olabilmesi için eğlenceli ve öğretici içeriklerin bir arada olması gerekmektedir. Parlak görseller, teşvikler ve etkileşimli etkinliklerin tümü, oyuncuları dijital güvenlik konusunda eğitmek ile motivasyonlarını sürdürmek arasında bir denge kurulmasına katkıda bulunur. Etkili eğitsel oyunlar uygulanabilir becerileri içermeli ve gerçek hayattaki durumlarla alakalı olmalıdır. Oyuncu katılımını sürdürmek aynı zamanda çekici grafikler ve sesler, net bir hedef ve uygun zorluk seviyeleri gerektirir. Dolayısıyla, dijital güvenlik eğitiminin temel bilgi ve becerilerin kazandırılmasında umut verici bir araç olduğu sonucuna varılabilir. İyi tasarlanmış bir eğitici oyun, kullanıcıları çevrimiçi tehlikeler konusunda

eğitmenin yanı sıra öğrenmeyi ilgi çekici, eğlenceli ve günlük senaryolara uygulanabilir hale getirmelidir. Teknoloji daha da geliştikçe, ilgi çekici eğitici oyunların dijital güvenlik müfredatına dahil edilmesi, daha güvenli ve siber farkındalığı yüksek bir küresel topluluk oluşturmanın güçlü bir yolu olabilir.

4.4 Öğrencilerin Öğrenme Tercihleri

Öğrenciler dijital güvenliği etkileşimli etkinlikler veya oyunlar aracılığıyla öğrenmeyi tercih ediyor ve gerçek hayattan örnekler yoluyla öğrenmeyi daha ilginç ve ilgi çekici buluyorlar. Öğrenme tercihlerine ek olarak, öğrenciler dijital güvenlik hakkında bilgi edinmek için geleneksel dersleri ve etkileşimli etkinlikleri daha ilgi çekici buluyorlar. Öğrencinin öğrenme tercihlerine ilişkin şu yanıtları verilmiştir;

“Etkileşimli etkinlikler ve oyunlar benim için daha ilgi çekici ve öğretici olabilir. Dijital güvenliği gerçek yaşam örnekleriyle öğrenmek daha anlamlı oluyor.”

“Genellikle etkileşimli etkinlikleri tercih ederim, bu nedenle dijital güvenlik konusunu öğrenirken oyunları daha cazip bulabilirim. Ancak bazen geleneksel derslerin de detaylı bilgiler sağlamada faydalı olabileceğini düşünüyorum.”

“Geleneksel dersler, tartışmalar ve oyunlar gibi çeşitli öğrenme yöntemlerini tercih ederim. Her yöntemin kendi avantajları ve dezavantajları vardır. Geleneksel dersler, temel bilgileri öğrenmek için iyidir. Ancak, dersler bazen sıkıcı olabilir ve öğrenciler dikkatlerini kaybedebilir. Tartışmalar, öğrencilerin farklı bakış açılarını öğrenmeleri için iyidir. Ancak, tartışmalar kontrolsüz hale gelebilir ve öğrenciler konuyu dağıtabilir. Oyunlar, bilginin eğlenceli ve ilgi çekici bir şekilde öğrenilmesini sağlar. Ancak, oyunlar her zaman kapsamlı bir eğitim sağlamaz. En iyi öğrenme yöntemi, konuya ve öğrencilerin ilgilerine bağlıdır.”

Öğrenciler geleneksel anlatım, oyun ve tartışmalara ilişkin çelişkili görüşler sunmuş ve bu yöntemlerin avantaj ve dezavantajlarına dikkat çekmişlerdir. Öğrencilere göre, geleneksel dersler ve kurslar dijital güvenliğe ilişkin temel bilgileri sağlıyor ve sıkıcı olabiliyor ancak derinlemesine tartışmalar bilgilendirici ancak düzensiz olabiliyor. Ancak geleneksel dersler, tartışmalar ve etkileşimli etkinlikler veya oyunlar gibi farklı yöntemleri birleştirmek, öğrenciler için kapsamlı ve etkili bir öğrenme deneyimi yaratabilir.

4.5 Dijital Güvenliđi Öğrenirken Karşılaşılan Zorluklar

Öğrenciler dijital güvenliđi oyunlarla öğrenirken teknik terimleri anlamada sorunlarla karşılaşmaktadırlar. Teknik terimler oyunlarda belirli konuların tam olarak anlaşılmasına engel teşkil etmektedir. Bu nedenle oyunlar, dersler ve interaktif aktiviteler yoluyla dijital güvenlik eğitiminin basitleştirilmesi ve herkesin anlayabileceđi şekilde anlatılması gerekmektedir. Ayrıca öğrenciler konuyu sıkıcı ve karmaşık buldukları ve ders esnasında dikkatlerini kayb ettikleri için ilgi çekici ve interaktif bir ders anlatımı tercih etmektedirler. Öğrenciler zorluklara ve zorluklara ilişkin görüşlerini belirtirken şu yanıtları verdiler;

“Bazı konular daha karmaşık olduğunda, oyunlar belirli konuları daha derinlemesine anlamamda yardımcı olamayabilir. Bu durumda, öğretmenin rehberliđi önemli olabilir.”

“Bazen konular karmaşık hale gelebilir. Oyunlarla öğrenirken bazı detayları atlayabiliyorum, bu da anlamamı zorlaştırabilir.”

“Geleneksel derslerde karşılaşabildiğim zorluklardan biri, dikkatimi korumaktır. Dersler bazen sıkıcı olabilir ve ben dikkatimi kaybedebilirim. Tartışmalarda karşılaşabildiğim zorluklardan biri, konuyu takip etmek olabilir. Tartışmalar hızlı ilerleyebilir ve ben konuyu kaçırabilirim. Oyunlarda karşılaşabildiğim zorluklardan biri, oyunun zorluđudur. Oyun çok zorsa, sıkılabilir veya pes edebilirim.”

Geleneksel derslerin sıkıcı veya aşırı karmaşık görülmesi, dikkatin dağılması ve takip edilmesinin zor olması gibi dezavantajları vardır. Katılımcıların oyunların çok kolay ya da çok zor olması ya da doğru bilgi vermemesi konusundaki kaygıları, eğitsel oyunların doğruluk ve zorluk düzeylerinin eleştirilmesine yol açmıştır. Bu, katılımcıların ilgisini ve anlayışını canlı tutmak için etkili bir öğretim tasarımına sahip olmanın ne kadar önemli olduğunu vurgulamaktadır. Oyunlar bazı durumlarda derin bir anlayış sağlayamasa da tamamlayıcı öğretim yaklaşımları da önerilmektedir. Öğrenme deneyimleri öznel olduğundan, eğitim stratejileri farklı öğrenme stillerinin ihtiyaçlarını karşılayacak şekilde özelleştirilmelidir. İlgisizlik ve hayal kırıklığı, öğrenilen materyalin algılanan faydası ve uygunluğu konusunda şüphe uyandırır. Dijital okuryazarlığı garanti altına almak için müfredat tasarımı dikkatle düşünölmelidir.

4.6 Eğitsel Oyunların Etkisi

Öğrencilerden eğitim oyunlarının etkisine ilişkin alınan yanıtlar, öğrencilerin dijital güvenlik anlayışına ilişkin olumlu düşünceleri ortaya koydu. Eğitsel oyunlar daha keyifli bir deneyim sunarak dijital güvenlik ve buna bağlı risklerin anlaşılmasına ve internette daha bilinçli olmaya katkıda bulunur. Bir öğrenci görüşünü paylaşırken şunları söyledi;

“Bence eğitici oyunları kullanmak dijital güvenlik anlayışımı olumlu yönde etkiledi. Eğitici oyunlar sayesinde, dijital güvenlik konularını daha iyi kavrayabildim, daha fazla ilgi duydum ve daha fazla pratik yapabildim. Eğitici oyunlar, dijital güvenlik konularını daha eğlenceli, daha anlaşılır ve daha uygulanabilir hale getirdi.”

“Eğitici oyunları kullanmak, dijital güvenlik anlayışımı önemli ölçüde etkiledi. Bu oyunlar, çevrimiçi güvenlik risklerini ve bunların nasıl önlenebileceğini daha iyi anlamama yardımcı oldu. Ayrıca, güvenli internet kullanımı ve kişisel bilgilerin korunması konusundaki farkındalığımı artırdı.”

Gerçek hayattan senaryolar ve eğlenceli hikayeler içeren etkileşimli oyunlar, kullanıcıların dijital güvenlik kavramlarını anlamalarına yardımcı olma konusundaki kullanışlılıkları nedeniyle beğeniliyor. Bu oyunlar internet konusunda farkındalık yaratır, güvenli davranışlar geliştirir ve karar verme becerilerini geliştirir. Bazı öğrenciler çevrimiçi güvenlik gibi gelişmiş bilgiler ve çevrimiçi dolandırıcılık, hırsızlık ve zorbalığa karşı gelişmiş bilinç gibi avantajlardan bahsetti. Buna karşılık bazı öğrenciler ise eğitsel oyunların dijital güvenlik anlayışını etkilemediğini, bunun da farklı yaklaşımlar ve bireysel tercih davranışları gerektirdiğini öne sürmüştür. Başka bir öğrenci ise şunları söyledi;

“Oyunlar, güvenli internet alışkanlıkları oluşturmamda etkili oldu. Şifreleri güncel tutma, güvenli bağlantılar kullanma ve kişisel bilgileri paylaşma konularında daha dikkatli olmaya başladım.”

Başka bir yanıtta katılımcı şunları söyledi;

“Oyunlar yoluyla öğrenme, çevrimiçi güvenliğe ilişkin davranışımı ve farkındalığımı şu şekilde etkiledi: Çevrimiçi güvenlik riskleri hakkında daha fazla farkında oldum. Oyunlar, çevrimiçi güvenlik risklerinin gerçekliğini ve bunların nasıl ortaya çıkabileceğini anlamama yardımcı oldu. Çevrimiçi güvenlik risklerine karşı daha dikkatli oldum. Oyunlar, çevrimiçi güvenlik risklerine karşı dikkatimi artırmama yardımcı oldu. Çevrimiçi olarak daha güvenli davranmaya başladım. Oyunlar, çevrimiçi olarak daha güvenli davranmama yardımcı oldu. Örneğin, bir oyunda, çevrimiçi bir sahtekarlık kurbanı olmamak

için nelere dikkat etmem gerektiğini öğrendim. Bu oyundan sonra, çevrimiçi olarak gelen e-postalara daha dikkatli olmaya başladım. E-postanın gerçek olup olmadığını belirlemek için e-postanın içeriğini ve gönderenin adresini kontrol etmeye başladım.”

Öğrencilerin verdikleri yanıtlardan oyunların onlara güçlü şifreler oluşturmayı, şifrelerini düzenli olarak değiştirmeyi ve şifreyi başkalarıyla paylaşmamayı öğrettiği analiz edilmiştir. Bu davranış, öğrencilerin çevrimiçi güvenliklerini oyun oynayarak geliştirmeyi öğrendiklerini göstermektedir. Ayrıca öğrenciler tanımadıkları kişilerle olan etkileşimlerinde daha dikkatli ve temkinli hale gelmişlerdir. Oyunların çevrimiçi dolandırıcılıkların önlenmesinde etkili olduğu kanıtlandı. Ayrıca öğrenciler internette hangi bilgileri paylaşacaklarını öğrenmişlerdir ve bu yaklaşım eğitsel oyunların yarattığı anlayışı göstermektedir.

4.7 Oyun Tasarımı ve Müfredata Entegrasyonu

Yüksek ve renkli grafikler içeren oyunlar ortaokul öğrencilerinin ilgisini çekecektir. Ayrıca kullanıcı dostu, etkileşimli tasarım, ödül, rekabet ve gerçek hayat senaryoları da oyunların öğrenciler için ilgi çekici ve çekici olmasını sağlayacaktır. Göz alıcı grafikler, iyi müzik ve ses ile dikkat çeker. Bu estetikler öğrencilerin oyuna olan ilgisini sürdürmek açısından önemlidir. Öğrencinin ifadesiyle;

“Dijital güvenlik eğitim oyunlarını çekici kılacak özellikler arasında ödüller, seviyeler, ve sürükleyici senaryolar bulunabilir.”

“Renkli ve dikkat çekici grafikler, basit ve anlaşılır görevler, ödüller ve rekabetçi unsurlar çocukları motive edebilir. Ayrıca, oyunun eğlenceli ve interaktif olması önemli.”

Ortaokul öğrencileri için etkileşimli öğrenme önemlidir çünkü onların materyale aktif olarak katılmalarını ve etkileşimde bulunmalarını sağlar. Etkileşimli görevler, büyüleyici görevler ve gerçekçi senaryo simülasyonları temel bileşenlerdir. Öğrenciler rekabetçi unsurlar, ödüller ve ilgi çekici karakterler gibi oyunlaştırma unsurlarıyla motive edilebilir. Oyunlar oyuncuların beceri düzeylerine göre tasarlanmalı, net bir hedefe sahip olmalı ve uygun zorluk seviyelerine sahip olmalıdır. Dijital güvenlik kavramlarının uygulanabilirliği ve geçerliliği gerçekçi senaryolar kullanılarak geliştirilebilir. Ancak bazı öğrenciler oyunlaştırılmış bileşenlere hiç ilgi göstermiyor; bu da kişisel tercihleri ve itici güçleri anlamının önemini vurguluyor. Genel olarak ortaokul öğrencilerine yönelik görsel olarak çekici, etkileşimli ve ödüllendirici oyunlar

geliştirmek, dijital güvenlik farkındalığında sağlam bir temel oluşturmak açısından çok önemlidir.

Ayrıca bu oyunlar okul müfredatına dahil edilebilir, çünkü bunlar dijital güvenlik konusunda öğrencilerde bilgi birikiminin artırılması ve farkındalık yaratılması açısından çok değerlidir. Öğrencilere dijital güvenlik konusunda pratik bilgi ve ilk elden deneyim kazandırmak amacıyla bu oyunlar bilgisayar derslerine eklenebilir. Bu oyunlar, geçmişteki siber saldırıları, dolandırıcılıkları veya zorbalıkları keşfetmek için tarih gibi farklı derslere dahil edilebilir. Bu sayede dijital güvenlik farkındalık oyunlarına diğer ders planlarında da yer verilebilir veya öğretmenlere ödev veya ödev verilebilir. Öğrenci şunları söyledi;

“Dijital güvenlik oyunları, bilgisayar dersleri veya özel güvenlik dersleri kapsamında okul müfredatına entegre edilebilir. Bu, öğrencilere teorik bilgileri uygulama fırsatı tanıyabilir.”

“Oyunlar, bilgisayar dersleri veya etik bilgi teknolojileri dersleri içinde düzenli olarak kullanılabilir. Ayrıca, diğer derslerle ilişkilendirilerek, öğrencilere dijital güvenlik konularını farklı bağlamlarda öğretme şansı verilebilir.”

Katılımcıların önerileri arasında dijital güvenlik oyunlarının proje veya ödev olarak müfredata dahil edilmesi, öğrencilerin bu türle ilgilenmeye teşvik edilmesi ve ardından öğrendiklerine dayalı olarak raporlar yazmaları veya sunumlar oluşturmaları yer alıyor. Öğrenmeyi güçlendirmek için oyundan yararlanan bu yaklaşım, dijital güvenlik kavramlarının anlaşılması üzerine düşünmeyi teşvik eder. İlgi çekici bir öğrenme ortamı yaratmak amacıyla öğretmenler, öğretmen eğitimi için dijital güvenlik oyunlarını da kullanabilirler. Dahası, katılımcıların çoğu dijital güvenlik oyunlarını müfredata dahil etmenin faydalarını vurguluyor, bazıları buna katılmıyor, dikkatli planlamanın gerekliliğini vurguluyor ve bu oyunların daha geleneksel öğretim yöntemlerini nasıl geliştirip tamamlayabileceğini düşünüyor.

Motivasyon ve Öğrenme İçgörülleri

Öğrenciler yüksek düzeyde motivasyon gösterdiler ve dijital güvenlik hakkında bilgi edinme konusunda istekli olduklarını ifade ettiler. Teknoloji çok hızlı bir şekilde geliştiğinden, öğrenciler çevrimiçi güvenliğin sağlanması için güncel kalmanın önemli olduğunu kabul etmektedirler. Öğrenciler oyunların öğrenmeyi daha eğlenceli hale getirerek kendilerini motive ettiğini ifade etti.

“Evet, dijital güvenlik konusunda öğrenmeye devam etme konusunda çok motivesiyim. Çünkü dijital güvenlik, günümüzde çok önemli bir konu. Çevrimiçi ortamda güvenli ve sorumlu bir şekilde davranmak,

hem kendim hem de başkaları için faydalıdır. Eğitici oyunların bu sürekli öğrenmede bir rol oynayacağını düşünüyorum. Çünkü eğitici oyunlar, dijital güvenlik konularını daha eğlenceli, daha anlaşılır ve daha uygulanabilir hale getiriyor. Eğitici oyunlar sayesinde, dijital güvenlik konusunda hem öğrenebilir hem de eğlenebilirim.”

“Dijital güvenlik konusunda öğrenmeye devam etmeye oldukça motive olduğumu düşünüyorum. Eğitici oyunlar, bu konuda sürekli öğrenmeye ve güncel kalma konusunda bana yardımcı olabilir.”

Yanıtlara göre, bazı öğrencilerin dijital güvenlik konusunda bilgi edinme konusunda güçlü bir isteği varken bazılarının ise orta düzeyde bir ilgisi var. Eğitsel oyunların, öğrenmeyi geliştiren ve dijital güvenlik kavramlarının uygulamalı olarak anlaşılmasını sağlayan paha biçilmez kaynaklar olduğu düşünülmektedir. Buna rağmen çoğu katılımcı eğitici oyunların motivasyonu geliştirme ve sürdürme yeteneğine sahip olduğunun farkındadır. Dijital güvenlik eğitiminde oyunlaştırılmış yaklaşımların algılanan değerini vurgulayan tekrarlanan bir tema, oyunlar, eğlence ve sürekli öğrenme arasındaki pozitif korelasyondur. Öğrencilerin dijital güvenlik alanında motivasyonunu korumak ve arttırmak için oyun stratejilerini benimsemenin oldukça önemli olduğu söylenebilir.

Konuyla ilgili derinlemesine bilgi edinmek amacıyla öğrencilerin çoğu, çevrimiçi güvenlikle ilgili bilgilerini geliştirmek için dijital güvenliğe ilişkin belirli konular hakkında daha fazla bilgi edinmeye ilgi gösterdi. Öğrencilerin ilgi duyduğu konular arasında çevrimiçi dolandırıcılık, sosyal medya güvenliği, şifre güvenliği, internetin güvenli kullanımı, çevrimiçi gizlilik ve güvenli çevrimiçi alışveriş yer alıyor. Katılımcılar, eğitici oyunların dijital güvenlik konusunda derinlemesine bilgi edinmede etkili olduğunun farkındaydı. Buna ek olarak öğrenciler siber zorbalık ve siber suçlar gibi siber güvenlikle ilgili konuları daha fazla keşfetmeye ilgi gösterdiler ve eğitsel oyunlar oynayarak bu konulardaki bilgilerini artırma konusunda isteklilik gösterdiler.

Katılımcılardan biri şunları söyledi;

“Daha fazla araştırmak istediğim konular arasında çevrimiçi dolandırıcılık ve kişisel veri koruma stratejileri yer alıyor. Eğitici oyunlar aracılığıyla daha fazla araştırmak istediğim belirli dijital güvenlik konuları arasında şunlar yer almaktadır: Çevrimiçi zorbalık, Çevrimiçi dolandırıcılık, Çevrimiçi uygunsuz içerik, Çevrimiçi gizlilik”

Cevaplar, katılımcıların çevrimiçi güvenliğe yönelik yeni tehditler, kişisel verileri koruma yolları, güvenli internet kullanımının yönleri ve siber zorbalığı durdurma taktikleri hakkında

daha fazla bilgi edinme konusundaki istekliliđini açıkça gösteriyor. Bu insanlar için eđitici oyunlar oynamak, dijital gvenlikteki en son sorunları ve czmleri takip etmenin harika bir yoludur.

Sonuç ve Tavsiyeler

Günümüzde ortaokul çocukları günde birkaç saatini internette geçiriyor ve birçok çevrimiçi oyun oynuyor. İnterneti kullanırken pek çok fırsat ve riskle karşılaşılıyorlar, ancak gerekli bilgi eksikliği nedeniyle dijital sistemleri ve interneti kullanmanın getirdiği riskleri veya tehditleri değerlendirmeyi zor buluyorlar. Risklerin zarar verme potansiyelinin farkında olmadıkları anlar vardır. Çocuklar çeşitli şekillerde istemeden kendilerini tehlikeye atabilir veya ebeveynlerinin bilgisi olmadan özel veya hassas bilgileri sızdırabilirler. Arama motorları, çevrimiçi reklamlar ve Facebook, Twitter gibi sosyal ağ siteleri ve diğer birçok web sitesi aracılığıyla, sosyal mühendislik, siber zorbalık, bilgisayar korsanlığı, virüsler ve zararlı kötü amaçlı yazılımlar, siber taciz vb. gibi siber güvenlik tehditlerinin de kurbanı olabilirler.

Bu çalışmada öğrencilerin çoğunluğunun dijital güvenliğe ilişkin bilgi düzeyinin iyi düzeyde olduğu tespit edilmiştir. İnternetteki hesapları için güçlü şifreler kullanmayı öğrendiler ve çevrimiçi olarak hangi bilgileri paylaşacaklarını biliyorlardı. Ortaokul çocukları tarafından çocuklara dijital ve siber güvenlik eğitimi verilmesinde yardımcı olan, halihazırda çevrimiçi olarak erişilebilen çeşitli eğitici oyun platformları ve uygulamaları kullanıldı. Ancak çocuklar hâlâ internette kullanılan teknik terimlerden habersizdi ve bu konular hakkında araştırma yapıp daha fazlasını öğrenmeye istekli olduklarını gösterdiler.

Sonuç olarak, öğrencilere dijital güvenliği daha etkili bir şekilde öğretmek için yaratıcı eğitici oyunlar oluşturma fırsatı vardır. Bu çalışmanın sonuçları göz önünde bulundurularak ortaokul çocukları arasında dijital güvenliğin artırılmasına yönelik aşağıdaki önerilerde bulunulmuştur.

Öncelikle öğrencilerin ilgisini çekecek yüksek ve renkli grafiklere sahip eğitsel oyunlar geliştirilmelidir. İkinci olarak, oyunların öğrencilerin ilgisinin yüksek kalması için seviyeleri, ödülleri ve rekabeti içermesi gerekir. Okullar, müfredatlarına dijital güvenlik farkındalığı derslerini dahil etmeli ve öğretmenler, öğrencilerin çevrimiçi dolandırıcılık, kimlik avı, siber zorbalık vb. mağduriyetlerini önlemek için öğrencilere teknik terimler ve stratejiler öğretmelidir. Ayrıca öğrencilere dijital güvenlik konusunda etkileşimli ve ilgi çekici bir şekilde eğitim verilmelidir. ilgi ve motivasyonlarını yüksek tutacak etkinlikler. Sonuçlara göre, öğrenciler geleneksel dersleri sıkıcı bulmakta ve odaklanmalarını kaybetmelerine neden olmakta, bu nedenle geleneksel ders anlatımı, tartışmalar ve etkileşimli etkinlikler veya oyunlar gibi farklı yöntemlerin birleştirilmesi, öğrenciler için kapsamlı ve etkili bir öğrenme deneyimi yaratabilmektedir. Bu çalışmanın sonuçları, ortaokul çocuklarına yönelik dijital farkındalığı ve

yüksek düzeyde bilgiyi geliştirmeye yönelik öğrenme materyalleri hazırlamak için memnuniyetle karşılanan bir kılavuzdur. Burada yetkin öğretmenin rolü çok önemlidir. Bulgular ışığında öğretmen adaylarının öğrenme sürecinin dijital güvenlik alanına daha fazla odaklanması gerekiyor. Hem aktif öğretmen hem de geleceğin öğretmeni, dijital güvenliği öğrencilere aktarmadan önce gerekli miktarda uzmanlık, odaklanma ve bilgi edinmelidir.

Ayrıca öğretmen ve öğrencilerin görüşlerini öğrenmek ve okuldaki dijital güvenlik programının geliştirilmesine ve iyileştirilmesine yardımcı olmak için geri bildirim mekanizması oluşturulmalıdır. Dijital güvenlik farkındalığını destekleyen Digital Passport veya Google Interland gibi çevrimiçi platformların iyileştirilmesi gerekiyor. Bu oyunlar çoğunlukla örneklerden ve teknik prosedürlerden yoksundur. Öğrencilerin sadece kavramları anlamalarını değil aynı zamanda bunları gerçek hayatta nasıl uygulayacaklarını da inceleyen oyunlara ihtiyaçları var. Örneğin çoğu oyun, öğrencilerin şifreleriyle nasıl başa çıktıklarına dair açılır ipuçları sağlar. Öğrencilerden oyunlar aracılığıyla güç seviyelerini test etmek için şifre vermeleri istenmelidir. Ayrıca bu oyunlar iyi grafiklere ve özelliklere sahip değil. İlginç özelliklere sahip oyunlar geliştirerek öğrencilerin ilgisini çekecektir.

Sonuçlar öğrencilerin dijital risklere ilişkin farkındalığının yüksek olduğunu gösterse de şifre paylaşma, kimliği belirsiz web sitelerini ziyaret etme, kişisel bilgilerini veya güvenliklerini koruyamama gibi güvenlik risklerine maruz kalabilmektedirler. Öğrenciler hâlâ gizliliklerini ve verilerini nasıl koruyacaklarını bilmiyorlar. Öğrenciler internete sık sık maruz kaldıkları için siber saldırı riski altındadırlar. Bu sorun öğrencinin sık sık bilgi aktarımı ve uygun yönlendirme almasıyla çözülebilir. Öğrencilerin siber güvenlik konusundaki anlayışlarını artıracak bir program şu anda mevcut değil. Ustalıkta katkı sağlayan tek şey dijital güvenlik ve bilgisayar üzerine çalışmaktır. Öğrenciler ayrıca dış siber güvenlik ve farkındalık programlarına da katılabilirler. Ayrıca, farkındalığı tüm düzeylere yaymak için hükümet, ortaokul öğrencilerinin okullarda daha iyi eğitilmesini sağlamak amacıyla özel kuruluşlarla işbirliği yapmalıdır.

Bu çalışmanın bazı sınırlılıkları da bulunmaktadır. Öncelikle zaman ve maddi kısıtlılıklardan dolayı veriler sadece 15 öğrenciyle gerçekleştirilmiştir. Bu nedenle bu çalışmanın sonuçları genellenemez. Ayrıca 15 öğrenciden toplanan veriler yeterli bilgi içermediği gibi öğretmen ve okul müdürlerinin görüşlerini de içermemektedir. Daha fazla araştırma, öğrenciler arasındaki dijital güvenlik düzeyi hakkında daha fazla bilgi edinmek için okullardan ve öğretmenlerden

temsilcileri içermelidir. Gelecek çalışmalarda örneklem büyüklüğü artırılabilir ve öğrencilerin çevrimiçi ortamda mağdur olup olmadığı sorulabilir.

Kaynakça

- Ayhan, B. ve Köseliören, M. (2019). İnternet, Online Oyun ve Bağımlılık. *Online Journal of Technology Addiction Cyberbullying*, 6(1), 1-30.
- Bauman, Z. (2015). *Akışkan Modern Dünyada Kültür*, (Çev: İ. Çapçioğlu ve F. Örnek). İstanbul: Atıf Yayınları.
- Cicchirillo, V. J. (2019). Digital Game Adversiting (IGA and Advergemes): Not All Fun and Games. *Journal of Interactive Adversiting*, 19(3), 202-203
- Çetin, E. (2013). Temel Tanımlar ve Kavramlar, (iç) Eğitsel Dijital Oyunlar, Kuram, Tasarım ve Uygulama (ed. M. Akif Ocak), Ankara: Pegem Yayınları, 2-6.
- Ergulec, F. & Kiremit, R. (2019). Tablet Bilgisayarların Okul Öncesi Dönemde Resim Çiziminde Kullanılması. *Eğitimde Kuram ve Uygulama*, 15(1), 17-36.
- Fromme, J. (2003). Computer Games as a Part of Children's Culture. *Game Studies*, 3(1). Erişim Adresi: <http://www.gamestudies.org/0301/fromme/>, 2 Haziran 2020.
- Gündoğan, A. (2014). Okul Öncesi Dönemde Bilgisayar Destekli Eğitim Projeleri, *GEFAD/GUJGEF* 34(3), 437-449.
- Güdüm, S. (2016). Sanal Yaklaşımlar ve Bilgisayar Oyunlarında Pazarlanan Şiddet. *Uluslararası Sosyal Araştırmalar Dergisi*, 9(42), 1986-1992.
- İnal, Y., & Kiraz, E. (2008). Bilgisayar Oyunları İdeoloji İçerir Mi? Eğitsel ve Ticari Oyunlara Bakış. *Türk Eğitim Bilimleri Dergisi*, 6(3), 523-544. (İnal & Kiraz, 2008)
- Işıkoğlu, N., Bayraktaroğlu, E. ve Ayekin Dülger, D. N. (2021). Çocukların Dijital veya Dijital Olmayan Oyun Tercihleri ve Davranışları. *Pamukkale Üniversitesi Eğitim Fakültesi Dergisi*.
- Kirriemuir, J. (2002). Video Gaming, Education and Digital Learning Technologies, *D-Lib Magazine*, 8(2).
- Levin, D.E. (2015). Technology Play Concerns. In D. P. Fromberg & D. Bergen (Eds.), *Play from Birth to Twelve: Contexts, Perspectives, and Meanings* (pp.225-232). New York: Routledge.
- Marsh, J., & Bishop. J.C. (2014). *Changing play: Play, Media and Commercial Culture from the 1950s to the Present Day*. Maidenhead: Open University Press/McGrawHill.

Neumann, M.M. (2018), Using Tablets and Apps to Enhance Emergent Literacy Skills in Young Children. *Early Childhood Research Quarterly*, 42, 239-246.

Özdoğan, B. (2008). *Çocuk ve Oyun: Çocuğa Oyunla Yardım*. Ankara: Anı Yayıncılık.

Ritzer, G. (2010). *Küresel Dünya*, (çev:M. Pekdemir). İstanbul: Ayrıntı Yayınları.

Squire, K. (2006). Games as ideological worlds. <http://www.academiccolab.org/resources>

Söğüt, Fatih. (2020). Dijital Ebeveynlerin Dijital Oyunlar ve Şiddet İlişkisine Yönelik Algıları. *İletişim Kuram ve Araştırma Dergisi - Sayı 51 / Güz 2020*.

Taylan, H. H., Kara, H. Z., & Durğun, A. (2017). Ortaokul ve Lise Öğrencilerinin Bilgisayar Oyunu Oynama Alışkanlıkları ve Oyun Tercihleri Üzerine Bir Araştırma. *PESA Uluslararası Sosyal Araştırmalar Dergisi*, 3(1), 78-87.

T.C. Sağlık Bakanlığı, (2018). Dijital oyun bağımlılığı çalıştayı. (Sonuç Raporu.) Erişim adresi: <https://www.guvenlioyna.org.tr/dosya/YVWJq.pdf>

Toran, M., Ulusoy, Z., Aydın, B., Deveci, T. & Akbulut, A. (2016). Çocukların dijital oyun kullanımına ilişkin annelerin görüşlerinin değerlendirilmesi. *Kastamonu Eğitim Dergisi*, 24(5), 2263-2278.

Tuğrul, B. (2017). Dünya oyunun gücünde uzlaştı şimdi bu gücü çocukların yararına kullanma zamanı: Hadi Türkiye. *Erken Çocukluk Çalışmaları Dergisi*, 1(2), 259-266.

Yıldırım, A. & Şimşek, H. (2013). *Sosyal bilimlerde nitel araştırma yöntemleri*. Ankara: Seçkin Yayıncılık

Yücelyigit, S., & Aral, N. (2020). Dijital Teknolojiyi Üretim ve Tüketim Amacıyla Kullanan Çocukların ve Ebeveynlerinin Tercihlerinin İncelenmesi. *İnönü Üniversitesi Eğitim Fakültesi Dergisi*, 21 (2), 1071-1084. DOI: 10.17679/inuefd.739564.

EK

Görüşme soruları

S:1 Ortaokul öğrencisi olarak dijital güvenlik konusunda herhangi bir bilginiz var mı?

Eğitsel Oyunlar ile ilgili olarak katılımcılara aşağıdaki sorular sorulacaktır:

S:2 Dijital güvenliği öğrenmek için hiç eğitici oyunlar kullandınız mı? Cevabınız evet ise deneyiminizi anlatabilir misiniz?

S:3 Eğitici oyunlar yoluyla ne tür dijital güvenlik konularının veya kavramlarının etkili bir şekilde öğretilbileceğini düşünüyorsunuz?

S:4 Sizce bir dijital güvenlik eğitici oyununu sizin için ilgi çekici ve etkili kılan şey nedir?

Öğrenme Tercihleri ile ilgili olarak katılımcılara aşağıdaki sorular sorulacaktır:

S:5 Geleneksel dersler, tartışmalar veya oyunlar gibi etkileşimli etkinlikler yoluyla dijital güvenlik hakkında genel olarak nasıl bilgi edinmeyi tercih edersiniz?

Zorlukları ve Endişeleri anlamak için şu soru sorulacaktır:

S: 6 Dijital güvenliği geleneksel yöntemlerle veya oyunlarla öğrenirken karşılaştığınız zorluklar veya zorluklar var mı?

Eğitsel Oyunların Etkisini değerlendirmek için bu soru sorulacaktır.

S:7 Sizce eğitici oyunları kullanmak dijital güvenlik anlayışınızı nasıl etkiledi?

S: 8 Oyunlar yoluyla öğrenmenin çevrimiçi güvenliğe ilişkin davranışınızı veya farkındalığınızı nasıl etkilediğine dair örnekler verebilir misiniz?

Oyun Tasarımı ve Özellikleri:

S: 9 Sizce bir dijital güvenlik eğitim oyununu ortaokul öğrencileri için daha çekici hale getirecek özellikler nelerdir?

Okul Müfredatına Entegrasyon:

S: 10 Dijital güvenlik eğitim oyunlarının okul müfredatına etkili bir şekilde nasıl entegre edilebileceğini düşünüyorsunuz?

S: 11 Bu oyunların en faydalı olabileceği belirli sınıf düzeyleri veya konular olduğuna inanıyor musunuz?

Gelecekteki Öğrenme stratejilerini bilmek ve önermek için aşağıdaki sorular sorulacaktır:

S: 12 Dijital güvenlik konusunda öğrenmeye devam etme konusunda ne kadar motivesiniz ve eğitici oyunların bu sürekli öğrenmede bir rol oynayacağını düşünüyor musunuz?

S: 13 Eğitici oyunlar aracılığıyla daha fazla araştırmak istediğiniz belirli dijital güvenlik konuları var mı?